1. OBJETIVO

Realizar el soporte y actualización de las redes de cómputo para agilizar los procesos administrativos en la operación de los servicios de red que proporciona la ADR, garantizándole al personal un fácil acceso a los aplicativos y servicios como correo electrónico, Internet, bases de datos, entre otros.

2. ALCANCE

Inicia con el evaluar el estado inicial de las redes y finaliza con la publicación de servicios en el Firewall.

3. BASE LEGAL

Decreto 1078 de 2015, Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. Título 9, Capítulo 1, Sección 1.

Decreto 1499 de 2017. Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015

4. DEFINICIONES

CPU (unidad central de procesamiento): Es la parte del ordenador o dispositivo que se encarga interpretar las instrucciones del sofware para realizar las operaciones básicas aritméticas, lógicas y de entrada y salida de un sistema.

Dirección IP: Es un número que identifica de manera lógica a un equipo en una red de computadores o en el internet.

DNS (Sistema de nombre de dominio): Se encarga de traducir el número de las direcciones IPv4 o IPv6 en nombres URLs que las personas puedan utilizar.

Firewall: Es una aplicación de seguridad diseñada para bloquear las conexiones en determinados puertos del sistema, independientemente de si el tráfico es benigno o maligno. Un firewall debería formar parte de una estrategia de seguridad estándar de múltiples niveles.

Incidente de seguridad de la información: El incidente, por su parte, requiere de la conjunción de eventos de seguridad de la información de modo que tengan la posibilidad de comprometer la seguridad y debilitar y afectar en la capacidad del negocio para alcanzar sus objetivos.

LAN: Red de área local, la cual se encarga de agrupar una o varias redes de computadoras en un área específica como un edificio, con el fin de transferir información entre los usuarios.

Pachcord: Nombre que se asigna al cable que se conecta entre la toma de red y el computador, con el fin de poder acceder a los servicios de red.

PING: Utilidad de los sistemas operativos, para poder diagnosticar fallos de red

Traceroute: Utilidad de los sistemas operativos para verificar los tiempos de respuesta de los paquetes en una red, desde un origen a un destino.

Switch: Dispositivo de red que permite segmentar, comunicar y transportar información de los equipos en las redes de computadores.

URL (Localizador Uniforme de Recursos): Es el nombre que se le asigna a la dirección específica que se asigna a cada uno de los recursos disponibles en la red con la finalidad de que estos puedan ser localizados o identificados, de esta forma, hay una URL para cada uno de los recursos como páginas, sitios, documentos, archivos, carpetas) que hay en la internet.

WAN: Red de área amplia, se encarga de agrupar una o varias redes LAN separadas geográficamente para poder transmitir información entre los usuarios.

5. CONDICIONES ESPECIALES

Para todas los incidentes o requerimientos asociados a la línea de redes de infraestructura se deben gestionar por medios dispuesto en la mesa de servicios.

Para el desbloqueo de sitios restringidos, debe dirigirse a la política de navegación web literal 8 que se encuentra publicada ISOLUCION y verifica en que categoría se encuentra el usuario, se solicita el desbloqueo con la categoría respectiva y el permiso del jefe de área, se evaluará el sitio con el oficial de seguridad y se indicará si es autorizado el desbloqueo, en el cual será configurado.

Para la publicación de nuevos servicios de internet, se debe tener en cuenta un tiempo de 8 horas aproximadamente, a partir de la configuración realizada por el proveedor, para que el servicio entre en producción, ya que se debe esperar a que los DNS autoritativos de internet tomen el cambio realizado.

El guardado de logs de los equipos de infraestructura de red está limitado a la capacidad del hardware de cada uno de los equipos, los cuales serán sobrescritos una vez se acabe el tamaño de espacio de guardado.

6. DESARROLLO

N°	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO
1	Evalué el estado inicial de las redes	Supervisa el software de monitoreo de los enlaces de comunicaciones WAN ingresando a la siguiente URL http://200.110.171.101/cacti Supervisa la herramienta de monitoreo de los servicios en la siguiente URL http://192.168.1.51/nagios/ Valida las configuraciones de los equipos activos de red. Verifica la segmentación de la red Verifica las actualizaciones de firmware de los equipos activos de la red. Verifica la asignación adecuada de IPs. En caso de presentar alertas en el monitoreo, se evalúa la alarma por medio de un ping al equipo que corresponda, si el ping no es satisfactorio se procede a crear el incidente, en la mesa de servicios, de acuerdo con el procedimiento de gestión de incidentes y requerimientos tecnológicos.	Administrador de redes	Log de los equipos activos Correo electrónico reportado por NAGIOS Mesa de servicios
2	Verifique Firewall	Ingresa al sitio de monitoreo del firewall, donde: Verifica el estado de la memoria y CPU del firewall. Verifica el número de sesiones concurrentes. Verifica el consumo del canal en el firewall que no supere lo contratado (500MB), si se llega a superar la capacidad máxima se presentara intermitencia en los servicios de navegación. Se procede a desarrollar los siguientes pasos: a. Genera caso en la mesa de servicios. b. Identifica las IPs que consumen el ancho de banda y procede a bloquearlas.	Administrador de redes	Mesa de servicio Log del firewall Correo electrónico

		c. Identifica las URLs de mayor consumo y se procede a desarrollar los cerrar las sesiones. d. Seguimiento y cierre del caso. Cuando se presenten alarmas no categorizadas, se escalan con el proveedor del servicio y se crea el caso en la herramienta de mesa de servicio, de acuerdo con el procedimiento de gestión de incidentes y requerimientos tecnológicos.		
3	Verifique Swicth Core	Ingresa al sitio de verificación del Switch Core, donde: Verifica el estado de la memoria y CPU. Verifica el estado de las interfaces Verifica alarmas presentadas, si las hay se procede a desarrollar los siguientes pasos: a. Genera caso en la mesa de servicios b. Identifica la interface donde se presenta el error y se procede a reiniciar la interface. c. Identifica que proceso está consumiendo la CPU o memoria y se procede a reiniciar el proceso d. Identifica si es posible acceder al switch core por medio de consola, si no es posible se debe apagar en el siguiente orden – Primero el SW3, segundo el SW2, tercero SW1. Dejar 30 segundos sin energía y luego prender en el siguiente orden – Primero SW1, segundo SW2, tercero SW3. Verifica el funcionamiento de la red. e. Seguimiento y cierre del caso en mesa de servicios.	Administrador de redes	Log del switch core Mesa de servicio
		Realiza soporte de primer nivel. (Mesa de servicio) de acuerdo con el procedimiento de gestión de incidentes y requerimientos tecnológicos. En caso de ser necesario se escala el requerimiento al		

4	Atender las fallas reportadas en la red LAN	administrador de red. Ingresa por SSH a las IP de gestión de los dispositivos o switches de piso. Valida las alertas reflejadas en los logs. Verifica estado y funcionamiento de los equipos activos de red. Hace seguimiento a la solución del incidente o ticket, según el procedimiento de gestión de incidentes y requerimientos tecnológicos.	Mesa de servicios Administrador de red	Mesa de servicios. Logs switchs de pisos
5	Atender las fallas reportadas en la red WAN	Valida las alertas visuales reflejadas por el monitoreo. Identifica el tipo de falla para categorizarla. Realizar soporte de primer nivel. (Administrador de redes) a. Verifica si hay fluido eléctrico. b. Verifica si los equipos activos y de cómputo se encuentran encendidos. c. Verifica las conexiones eléctricas y de red. En caso de ser necesario se escala el requerimiento o incidente al proveedor respectivo y se genera el caso en la mesa de servicios según el procedimiento de gestión de incidentes y requerimientos tecnológicos. Hace seguimiento al incidente reportado por el funcionario encargado ó proveedor. Aprueba el cierre del incidente del proveedor de acuerdo con los ANS. Soluciona el incidente en la mesa de servicios.	Mesa de servicio Administrador de red	Mesa de servicios Correo electrónico
		Realiza soporte el nivel uno. (Mesa de servicio) de acuerdo con el procedimiento de gestión de incidentes y requerimientos tecnológicos. El responsable del incidente o requerimiento deberá ejecutar como mínimo las siguientes tareas:		

6	Falla de acceso a la RED	a. Identifica si es solo un usuario o es un grupo donde se presenta la falla. b. Realiza desde uno de los equipos afectados ping 127.0.0.1, con el fin de descartar problemas en la tarjeta de red del equipo, sino es satisfactoria la prueba, se debe reinstalar la tarjeta de red o en su defecto cambiar el equipo. c. Realizar desde uno de los equipos afectados ping a la ip de default Gateway de red del piso, sino es satisfactoria la prueba se debe cambiar los pachcord del equipo y verificar los puertos del switch de piso, que estén encendidos para el respectivo puesto de trabajo. d. Realizar desde uno de los equipos afectados traceroute 8.8.8.8 con el fin de determinar en qué equipo de red se quedan los datos. e. Si los datos se quedan en un equipo interno se procederá a verificar la configuración del equipo y dar la solución. Si se evidencia que los datos salen, pero no se completa la traza, se devuelve con lo descrito en la actividad 4	Mesa de servicios Administrador de redes	Mesa de servicios Correo electrónico
7	Crea VPN Site to Site	Crea el requerimiento según el procedimiento de gestión de incidentes y requerimientos tecnológicos. Verifica si el requerimiento es viable. Solicita el respectivo permiso del jefe de la Oficina de tecnologías de la información. Identifica los servicios que se prestaran por medio de la VPN site to site Solicita al cliente remoto la documentación para la creación de la VPN site to site con los siguientes datos mínimos: a. IP del Gateway remoto b. Dominio de encripción	Administrador de redes	Mesa de servicios

		remoto c. Puertos lógicos remotos d. Tipo de dispositivo remoto e. IP del Gateway local f. Dominio de encripción local g. Puertos lógicos locales h. PSK de la VPN i. Tipo de dispositivo local Crea la VPN site to site con la información enviada en el firewall. Crea la respectiva política de navegación para la VPN site to site e el firewall. Establece la VPN site to site y realiza pruebas de funcionamiento.		Correo electrónico
8	Crea VPN SSL trabajo remoto	Verifica que el requerimiento esté en el aplicativo de mesa de servicios. Verifica que se encuentre la aprobación del jefe de área y el jefe de la OTI en el aplicativo de mesa de servicios. Otorga permiso a la VPN SSL al usuario en el directorio activo. Realiza la documentación y solución de acuerdo con el procedimiento de gestión de incidentes y requerimientos tecnológicos.	Administrador de redes	Mesa de servicios Correo electrónico
9	Publica servicios en el Firewall	Verifica que el requerimiento se encuentre creado en el aplicativo de mesa de servicios. Verifica los respectivos permisos de publicación del jefe de la OTI y del oficial de seguridad de la información. Asigna IP publica y puerto para el nuevo servicio Asigna IP interna y puerto para el nuevo servicio. Gestiona con el proveedor de servicio la publicación del DNS en internet. Realiza el seguimiento y solución de acuerdo con el procedimiento de gestión de incidentes y requerimientos tecnológicos.	Administrador de redes	mesa de servicios Correo electrónico
		Se genera informe mensual		

10	Genera informe de eventos	que consolida los incidentes y requerimientos gestionados en la Mesa de servicios.	Administrador de redes	Correo Electrónico

7. DOCUMENTOS ASOCIADOS

Procedimiento Gestión del cambio de Tecnologías de la Información

Procedimiento de gestión de incidentes y requerimientos tecnológicos

Política de navegación web

Log de los equipos activos

Log del firewall

Log del switch core

Logs switchs de pisos

Formato de requerimiento de cambio (FRC

VERSIÓN	FECHA	RAZÓN DE LA ACTUALIZACIÓN

ELABORÓ	REVISÓ	APROBÓ
Nombre: CATALINA SANABRIA **Cargo:** 2.4. Oficina de Tecnologías de la Información **Fecha:** 30/Jun/2020	**Nombre:** Leonardo Alfonso Murillo Corrales **Cargo:** 2.4. Oficina de Tecnologías de la Información **Fecha:** 06/Jul/2020 **Nombre:** Harold Steaben Reyes Bernal **Cargo:** 2.4. Oficina de Tecnologías de la Información **Fecha:** 06/Jul/2020	**Nombre:** Victor Manuel Mondragon Maca **Cargo:** 2.4. Oficina de Tecnologías de la Información **Fecha:** 07/Jul/2020