CONTROL DE CAMBIOS		
VERSIÓN[1]	**FECHA**	**DESCRIPCIÓN DE LA MODIFICACIÓN**
1	14 de Junio de 2011	Primera versión del documento, vincula y elimina los procedimientos de administración de plataforma de voz P-116301-07,
2	14 de Marzo de 2013	Segunda versión del documento, se actualizan los servicios e instrucciones.
01	28 de noviembre de 2017	Se realiza ajuste de normalización como consecuencia de la entrada en vigencia de la resolución 162 de 2017, que crea el proceso Gerencia de TIC como parte del mapa de procesos de la entidad, y en cumplimiento de lo establecido en la circular 16 del 1 de noviembre de 2017. Los lineamientos operativos descritos en este documento, corresponden íntegramente a los aprobados en la versión 2 de fecha 14 de marzo de 2013, la cual fue aprobada por Martha Patricia Jiménez Rodríguez – Subsecretaría de Planeación y Gestión como líder del proceso Gestión y Adquisición de Recursos, vigente en ese momento.

[1] ***Nota:*** *"Si este documento se encuentra impreso no se garantiza su vigencia, por lo tanto se considera "Copia no Controlada. La versión vigente se encuentra publicada en la intranet de la Secretaría Distrital de Gobierno"*

1. INFORMACIÓN GENERAL

Propósito del Instructivo:

Brindar soporte técnico especializado sobre la Infraestructura Tecnológica de la Secretaria Distrital de Gobierno de manera eficiente, a través de recurso humano calificado y teniendo en cuenta los estándares nacionales e internacionales que apliquen, con el fin de garantizar la disponibilidad de los servicios de la Entidad.

Responsable:

Director (a) de Planeación y Sistemas de Información.

2. INSTRUCCIONES:

Para el cumplimiento del propósito del presente Instructivo, es necesario tener en cuenta los siguientes lineamientos en cada uno de los componentes de Infraestructura Tecnológica a los que se les brindará soporte técnico, así:

2.1. EMISIÓN DE CONCEPTOS TÉCNICOS DE DIAGNÓSTICO ELÉCTRICO Y DE CABLEADO ESTRUCTURADO.

Para la emisión de conceptos técnicos de diagnóstico eléctrico y de cableado estructurado, es necesario tener en cuenta los siguientes lineamientos de operación:

- Toda solicitud debe ser dirigida a la Dirección de Planeación y Sistemas de Información, a través de la mesa de servicios o por medio de memorando u oficio radicado por el aplicativo Orfeo.

- La realización de la visita técnica se programará en conjunto con Planta Física de Dirección Administrativa y se debe contar con el acompañamiento del solicitante, el administrador de red o del enlace de sistemas en dicha sede.

- Durante la visita técnica, se realizarán las siguientes actividades teniendo en cuenta lo establecido en el Reglamento Técnico de las Instalaciones Eléctricas, RETIE, el Código Eléctrico Colombiano, la NTC2050 y las demás normas vigentes relacionadas con la actividad a realizar:

  - ✓ Revisión de la acometida eléctrica, identificación de la carga eléctrica contratada del predio, capacidad, si corresponde a una acometida monofásica, bifásica o trifásica y si cumple con los requerimientos de carga eléctrica requerida.
  - ✓ Revisión de los tableros eléctricos de distribución principal y secundaria, verificando que se que se encuentran debidamente normalizados acorde con la normatividad técnica vigente.
  - ✓ Medición de voltajes fase-fase, fase-tierra, fase-neutro y tierra-neutro en los tableros de distribución normal y regulado y verificación de que se encuentran dentro de los valores normales de operación.

  - ✓ Verificación del estado de la UPS instalada en el cuarto eléctrico, su capacidad y la cantidad de equipos conectados a ella.
  - ✓ Revisión de los aires acondicionados instalados en los cuartos de equipos, su estado, su capacidad y si están

dimensionados acorde con los requerimientos de los cuartos de equipos.
- ✓ Revisión del estado de la planta eléctrica, capacidad y características, en los casos que aplique.
- ✓ Revisión de las características técnicas de las protecciones eléctricas internas, como transformadores de aislamiento y supresores de picos clase B y clase C, en los casos que aplique.
- ✓ Revisión de la existencia de un sistema de protección contra rayos, adecuadamente dimensionado acorde con las características técnicas de la sede, en los casos que aplique.
- ✓ Revisión del sistema de puesta a tierra y si se encuentra instalado acorde con lo descrito en la normatividad técnica vigente.
- ✓ Inspección técnica para la adecuación y/o instalación de cableado estructurado.

- Realizar el informe técnico, el cual debe contener:

  - ✓ La solicitud realizada, con el número de caso registrado en Aranda o el número del oficio o memorando con su respectiva fecha.
  - ✓ La fecha de la visita técnica y el profesional que realizó dicha actividad.
  - ✓ La evaluación del estado actual de la sede en lo referente a la red eléctrica y de cableado estructurado.
  - ✓ Las recomendaciones técnicas.
  - ✓ El informe técnico deberá emitirse por medio de memorando u oficio radicado en el aplicativo Orfeo, dentro de los 10 días hábiles siguientes a la realización de la visita técnica.

2.2. SOPORTE TÉCNICO PLATAFORMA DE VOZ

En este aparte se determinan los diferentes pasos que deben realizarse cuando se requiera la prestación de un servicio destinado a solucionar inconvenientes con la plataforma de voz de la Entidad.

El requerimiento del servicio debe ingresar por el aplicativo existente para la Gestión de Servicios de Tecnología de la Información, mediante la cual se registra la eventualidad presentada, que dará lugar a un incidente o solicitud de servicio según las características de dicha eventualidad.

Esta solicitud de servicio es documentada por el primer nivel de atención de la Gestión de Servicios de TI. Luego es transferida al segundo nivel de atención, con el fin de que la persona asignada al apoyo de esta actividad proceda a verificar la causa de la novedad presentada.

Los incidentes o solicitudes de servicio pueden ser originados por diferentes causas, las cuales se describen a continuación, estableciendo las pautas que se deben seguir.

- **Generación de una nueva extensión**

El primer nivel escala el caso al segundo nivel de atención, quien verifica la disponibilidad de aparato telefónico, para habilitar la nueva extensión, en caso positivo, abre un incidente ante el tercer nivel de atención: proveedor de servicios de mantenimiento de la plataforma de voz, quien se encargará de

verificar la disponibilidad de licencias existentes en la planta telefónica, para la creación de una nueva extensión.

En caso de existir la disponibilidad tanto de software como de hardware, la extensión es creada por el tercer nivel de atención, quien le asignará el código de la dependencia donde se ubica el usuario solicitante, con el apoyo de la información brindada por el segundo nivel de atención.

Una vez terminado el servicio por el tercer nivel de atención, este se encarga de documentar el incidente abierto y posteriormente lo cierra, comunicándolo vía correo electrónico, al funcionario de segundo nivel de atención.

El segundo nivel de atención habilita la nueva extensión conectando el aparato telefónico y da la instrucción respectiva de su uso a la persona solicitante. Luego documenta el caso abierto en el aplicativo de Gestión de Servicios de TI y lo da como solucionado.

- **Falla en el servicio de una extensión**

El primer nivel de atención recibe del usuario la solicitud de la falla presentada, para escalarla inmediatamente al segundo nivel de atención, quien realiza una verificación del funcionamiento de la extensión. Inicialmente, se comunica con el usuario que requirió el servicio con el fin de determinar el origen de la falla presentada. Realizada esta primera evaluación, el segundo nivel de atención, determina si el viable resolverla mediante asistencia remota, indicándole al usuario el procedimiento que debe seguir para solucionarla; o si es necesario realizar asistencia técnica en el sitio. Para este último caso, el segundo nivel de atención realiza una revisión física del aparato y sus conexiones, estableciendo el origen de la falla y, si es viable solucionarla mediante el conocimiento adquirido, procede a solucionarla. En caso contrario, si la falla requiere de una revisión minuciosa por daño físico del aparato o configuración de la extensión en la planta telefónica, el segundo nivel de atención, escala el caso al tercer nivel de atención (proveedor de servicios de mantenimiento preventivo y correctivo), quien genera un número de incidente y realiza las revisiones respectivas para la eliminación de la falla). El tiempo que tarda el tercer nivel en atender la falla depende de las características de la misma y los tiempos de respuesta SLA (Acuerdos de Nivel de Servicio) establecidos en el contrato de prestación de servicios.

Realizada la reparación a la falla presentada, el tercer nivel de atención remite un correo electrónico al segundo nivel de atención, indicando el cierre del incidente, donde describe la solución aplicada. El segundo nivel de atención procede a documentar el caso abierto en el aplicativo de Gestión de Servicios de TI y luego lo da por solucionado.

- **Cambio de aparato telefónico por daño físico**

Cuando se presenta un daño del aparato telefónico, el proveedor de servicios de mantenimiento preventivo y correctivo, entrega uno de iguales características al que presenta la falla. Como este nuevo aparato reemplaza al existente, el segundo nivel de atención adelanta el trámite interno de cambio por garantía del equipo, el cual debe ser diligenciado por el funcionario de segundo nivel de atención y firmado por el usuario a cargo del aparato telefónico, para que se registre dicho cambio en el aplicativo de inventarios de la Entidad.

2.3. MANTENIMIENTO CORRECTIVO DE UPS´s

Para la realización de un mantenimiento correctivo de las UPS's de la Secretaría Distrital de Gobierno, es necesario tener en cuenta los siguientes lineamientos de operación:

- Toda solicitud de mantenimiento correctivo por fallas en las UPS's, debe ser dirigida a la Dirección de Planeación y Sistemas de Información, a través de la mesa de servicios.
- Debe realizarse la revisión de las alarmas a través del display frontal de la máquina, por parte del profesional encargado de la red eléctrica en las sedes de nivel central y por parte de los administradores de red o los enlaces de sistemas en las demás sedes.
- La revisión de dichas alarmas debe quedar debidamente documentada en el histórico del aplicativo de gestión de servicios de TI.
- El profesional encargado de la red eléctrica en las sedes de nivel central y/o los administradores de red o los

enlaces de sistemas en las demás sedes, deben realizar las actividades de encendido, apagado o bypass descritas en cada una de las UPS´s de la Secretaria Distrital de Gobierno, de acuerdo al tipo de alarma.

- Se debe verificar que la UPS se encuentre en estado normal, de lo contrario se procede a escalar el servicio a soporte Nivel III, para que el proveedor encargado del mantenimiento de las UPS´s asigne los técnicos que realizarán el mantenimiento correctivo de la máquina, acorde con los tiempos y especificaciones establecidas en las obligaciones contractuales.
- Finalmente, el proveedor encargado del mantenimiento de las UPS deberá entregar el Reporte Técnico de Mantenimiento Correctivo de la máquina, debidamente diligenciado.

2.4. MANTENIMIENTO CORRECTIVO DE AIRES ACONDICIONADOS

En este aparte se determinan los diferentes pasos que deben realizarse cuando se requiera la prestación de un servicio destinado a solucionar inconvenientes con los equipos de aires acondicionados de la Entidad.

El requerimiento del servicio debe ingresar por el aplicativo existente para la Gestión de Servicios de Tecnología de la Información, mediante la cual se registra la eventualidad presentada, que dará lugar a un incidente o solicitud de servicio según las características de dicha eventualidad. Esta solicitud de servicio es documentada por el primer nivel de atención de la Gestión de Servicios de TI. Luego es transferida al segundo nivel de atención, con el fin de que la persona asignada al apoyo de esta actividad proceda a gestionar la solución a la novedad presentada.

El segundo nivel de atención, escala el servicio al tercer nivel de atención (proveedor de servicios de mantenimiento preventivo y correctivo), quien realiza visita técnica de inspección y reparación de la falla presentada. En caso de requerirse el cambio de algún elemento del equipo, el proveedor pide su aprobación al segundo nivel de atención, quien una vez analizada su viabilidad, lo autoriza. El tercer nivel de atención entrega un informe técnico escrito, describiendo la novedad presentada y las acciones tomadas para su solución. Con esta información, el segundo nivel de atención, procede a documentar el incidente o llamada de servicio generada mediante la Gestión de Servicios de TI y lo da por solucionado.

2.5 GESTIÓN DEL DIRECTORIO ACTIVO

En este aparte se determinan los diferentes pasos que deben realizarse cuando se requiera la prestación de un servicio relacionado con la gestión del directorio activo:

- **Creación de un nuevo usuario**

  - ✓ Verificar la solicitud realizada, con el número de caso registrado en la herramienta de gestión institucional.
  - ✓ Comprobar que los documentos de solicitud de cuenta se encuentren en el Formato 015, Nombre completo de usuario, dependencia, vigencia de la cuenta.
  - ✓ Confirmar si el nombre del usuario existe o está inactivo.
  - ✓ Crear la cuenta de usuario en la unidad organizativa correspondiente.
  - ✓ Asignar un nombre de cuenta acorde al estándar de creación de cuentas.
  - ✓ Asignar una contraseña alfanumérica y se activa la casilla la opción de cambio de contraseña al inicio de sesión.
  - ✓ Realizar el perfilamiento de la cuenta, como grupos a los que se deben asociar, y accesos compartidos que debe tener dependiendo la unidad organizativa o funciones a realizar el usuario.
  - ✓ Verificar el ingreso al dominio de la máquina, que debe ser igual al nombre de la cuenta y con las características de cada sede o localidad.

- ✓ Agregar la máquina a la unidad organizativa perteneciente.
- ✓ Asociar la máquina a la cuenta del usuario correspondiente.
- ✓ Perfilar los permisos correspondientes de navegación o acceso.
- ✓ Solucionar el caso y documentar la respuesta correspondiente

- **Otras solicitudes**

  - ✓ Traslado de cuentas a las unidades organizativas correspondientes dentro del dominio gobiernobogota.gov.co.
  - ✓ Desvinculación de las máquinas de los usuarios y de los grupos donde se encuentra la cuenta, según el traslado de estos de las localidades o unidades organizativas.
  - ✓ Eliminación de máquinas de sede, localidades y nivel central dependiendo la solicitud.
  - ✓ Creación de unidades organizativas según solicitud.
  - ✓ Administración de permisos temporales o permanentes a las cuentas de los usuarios.
  - ✓ Reinicio de contraseñas de usuarios especiales.
  - ✓ Soporte técnico de segundo nivel a los administradores de red de las Alcaldías Locales.

2.6 GESTIÓN A LA PLATAFORMA DE SERVIDORES LINUX

A continuación se establecen los pasos que deben realizarse cuando se requiera la prestación de un servicio destinado a solucionar los siguientes inconvenientes relacionados con los servidores Linux de la Entidad:

- Instalación y configuración
- Conexión a red
- Aplicativos

- Aseguramiento
- Afinamiento

El requerimiento del servicio debe ingresar por el aplicativo existente para la Gestión de Servicios de Tecnología de la Información, mediante la cual se registra la eventualidad presentada, que dará lugar a un incidente o solicitud de servicio según las características de dicha eventualidad.

Esta solicitud de servicio es documentada por el primer nivel de la Gestión de Servicios de TI. Luego es transferida al segundo nivel, con el fin de que la persona asignada al apoyo de esta actividad proceda a verificar la causa de la novedad presentada, en caso de no poder solucionar el inconveniente se escala al nivel 3 de atención que es el proveedor de servicios de suscripción de los sistemas operativos, con el fin de tramitar la solución definitiva.

2.7 GESTIÓN DE LA PLATAFORMA DE SERVIDORES WINDOWS

El presente documento determina los diferentes pasos que deben realizarse cuando se requiera la prestación de un servicio destinado a realizar las siguientes actividades relacionadas con la gestión de la plataforma de servidores Windows de la Entidad:

- Instalación y Configuración
- Dimensionamiento Servidor
- Versión de Windows Server

- Función a Cumplir
- Requerimientos Técnicos
- Aseguramiento
- Afinamiento

El requerimiento del servicio debe ingresar por el aplicativo existente para la Gestión de Servicios de Tecnología de la Información, mediante la cual se registra la eventualidad presentada, que dará lugar a un incidente o solicitud de servicio según las características de dicha eventualidad.

Esta solicitud de servicio es documentada por el primer nivel de la Gestión de Servicios de TI. Luego es transferida al segundo nivel, con el fin de que la persona asignada al apoyo de esta actividad proceda a verificar la causa de la novedad presentada, en caso de no poder solucionar el inconveniente se escala al nivel 3 de atención que es el proveedor de servicios de suscripción de los sistemas operativos, con el fin de tramitar la solución definitiva.

Dentro de los requerimientos que se atienden por la plataforma de Gestión de Servicios de la Entidad relacionada con la administración de servidores se encuentran:

- ✓ Realizar tareas de administración asociadas al ciclo de vida operativo del servidor, como iniciar o detener servicios y administrar cuentas de usuario locales.
- ✓ Realizar tareas de administración asociadas al ciclo de vida operativo de las funciones instaladas en el servidor.
- ✓ Determinar el estado del servidor, identificar eventos críticos, y analizar y solucionar problemas o errores de configuración.
- ✓ Instalar o quitar funciones, servicios de función y características desde la línea de comandos de Windows.

2.8 GESTIÓN DE LA PLATAFORMA DE CORREO ELECTRÓNICO ZIMBRA

En este aparte se determinan los diferentes pasos que se realizan cuando se requiere hacer la gestión del correo electrónico implementado utilizando la plataforma de correo zimbra, dicha gestión consiste en el manejo de los servidores de correo y sus respectivas tareas administrativas, y el manejo de usuarios de correo electrónico.

La plataforma de correo electrónico está implementada en tres servidores de correo, cada uno de ellos cumplen las siguientes tareas:

MTA (Envió y recepción de correo)
STORE (Almacenamiento de los archivos y correo de los usuarios)
LDAP (Gestión de Usuarios, Agenda y Directorio, entre otros)

Cabe anotar, que la gestión que se realiza actualmente sobre la plataforma de correo electrónico Lotus se realiza por parte de la mesa de servicios.

2.8.1 Administración de Servidores

- **Ingresar a la consola administrativa de cada uno de los servidores ssh y realizar las siguientes tareas:**

- ✓ Verificar que el sistema este actualizado.
- ✓ Instalar las actualizaciones de seguridad requerida
- ✓ Revisar y limpiar de ser necesario los logs y verificar la correcta operación de dicho sistema.
- ✓ Revisar el estado del almacenamiento de cada uno de los servidores y asegurarse que tenga espacio e inodos

disponibles para la correcta operación del sistema.

- **Ingresar a la consola administrativa web del sistema:**

  - ✓ Revisar la cola de correo, entrante y saliente, se debe poner en cola los correos que quedan en la bandeja de diferido.
  - ✓ Eliminar la cola de correo que lleve más de dos días.
  - ✓ Verificar el correcto funcionamiento de cada uno de los servicios de correo.

2.8.2 Manejo de usuarios de correo electrónico

En este aparte se determinan los diferentes pasos que deben realizarse cuando se requiera la prestación de un servicio relacionado con la creación o eliminación o usuarios del sistema:

- ✓ Verificar la solicitud realizada, con el número de caso registrado en la herramienta de gestión institucional.
- ✓ De acuerdo a la solicitud, se debe ingresar a la plataforma administrativa e ingresar al menú "Administrar" donde el sistema permite gestionar, las cuentas de correo, los alias, las listas de correo y los recursos.

2.9 GESTIÓN DE LOS FIREWALLS DE LA ENTIDAD

Con el fin de brindar lineamientos generales en la administración y/o operación de los firewalls de la Entidad y garantizar una atención oportuna a las solicitudes generadas por la mesa de servicios a través de la herramienta de gestión, o a los posibles incidentes de seguridad tanto a nivel interno como externo, se contemplan los siguientes pasos:

- Recibir la solicitud realizada a través de la herramienta de gestión de incidentes, con el respectivo número de caso registrado ó la verificación de los diferentes eventos y/o evidenciadas reportadas en el firewall.
- Realizar la autenticación con el usuario y contraseña destinada a cada administrador para la gestión de dichos dispositivos, evaluar y aplicar los cambios solicitados con previa autorización del Director(a) de Planeación y Sistemas de Información o Coordinador(a) del grupo de Infraestructura Tecnológica.
- Realizar las pruebas de funcionamiento con el usuario que realizo la solicitud.
- Cerrar la conexión con el dispositivo.
- Solucionar y documentar el caso registrado con la descripción del cambio realizado.

2.10 GESTIÓN DE LOS EQUIPOS ACTIVOS DE RED DE LA ENTIDAD

El presente ítem determina los diferentes pasos que deben realizarse cuando se requiera la prestación de un servicio destinado a solucionar inconvenientes con los equipos activos de la Entidad, clasificados en:

2.10.1 Gestión Física de los Equipos Activos

El requerimiento del servicio debe ingresar por el aplicativo existente para la Gestión de Servicios de la Entidad, mediante la cual se registra la eventualidad presentada, que dará lugar a un incidente o solicitud de servicio según las características de este.

Esta solicitud de servicio es documentada por el primer nivel de la Gestión de Servicios de TI, luego es transferida al segundo nivel con el fin de que la persona asignada al apoyo de esta actividad proceda a verificar la causa de la novedad presentada, en el caso de no poder solucionar el inconveniente se escala al nivel 3 que es el proveedor del servicio de mantenimiento el cual evaluara y dará la solución correspondiente.

Los incidentes o solicitudes de servicio pueden ser originados por diferentes causas, las cuales se describen a

continuación:

- **Validar conectividad equipos activos:** se realiza un ping constante con la herramienta de monitoreo de la Entidad, la cual nos genera la alerta de la disponibilidad del servicio. Cuando en equipo activo presenta una caída del servicio se genera una alerta o incidente que es comunicado al administrador de la herramienta y este comunica al supervisor del contrato de equipos activos el cual registra el incidente al proveedor correspondiente.
- **Validación de primer nivel:** por parte de la Secretaria Distrital de Gobierno, Proveedor de canal de comunicación y/o soporte y mantenimiento de equipos activos, se valida por parte de la SGD que los equipos activos estén prendidos, que no se presenten problemas eléctricos en determinada sede y que las conexiones físicas estén debidamente conectadas, una vez realizadas las pruebas anteriores se detecta que se sigue presentado problemas de disponibilidad del servicio se escala al

segundo nivel.
- **Validación de segundo nivel:** Se valida por parte de la SGD que los puertos no presenten bloqueo y las configuraciones de los equipos activos estén de acuerdo con los parámetros establecidos para determinada sede, en caso de seguir presentando inconvenientes el soporte de segundo nivel determina la causa y escala el servicio a la empresa encargada del mantenimiento de equipos activos o al proveedor del servicio del canal de comunicaciones WAN.

2.10.2 Gestión Lógica de los Equipos Activos

A continuación, se describen los pasos para realizar la gestión lógica de los equipos de red (switch, router, AP, etc.) de la Secretaria Distrital de Gobierno:

- Recibir la solicitud a través de la herramienta de gestión de la Entidad, con el respectivo número de caso registrado.
- Verificar la conectividad del dispositivo que se requiere intervenir. Si existe comunicación, se realiza la autenticación con el usuario y contraseña destinada para la administración de dichos dispositivos y se aplican los cambios solicitados. Si no existe comunicación con el dispositivo a intervenir se hace verificación en sitio, se detecta y soluciona la falla de comunicación y se aplican los cambios solicitados. En caso de detectar falla física sobre el equipo, debe remitirse a lo relacionado en el punto No 2.10.1 Gestión Física de los Equipos Activos.
- Guardar los cambios de la configuración realizada.
- Cerrar la conexión con el dispositivo intervenido.
- Solucionar y documentar el caso registrado con la descripción del cambio realizado.

2.11 GESTIÓN DE PERMISOS DE ACCESO A INTERNET

A continuación, se describen los pasos que deben realizarse cuando se requiera generar permisos de acceso a internet en el nivel central y local:

• NIVEL CENTRAL

Teniendo en cuenta que el control de la navegación se realiza por nombre y no por IP a través de la cuenta de dominio asignada a cada usuario, la asignación de dichos permisos se debe realizar de la siguiente manera:

- ✓ Recibir la solicitud a través de la mesa de servicios.
- ✓ Crear la cuenta de usuario en el directorio activo (si el usuario es nuevo), en la unidad organizativa

correspondiente a la dependencia a la que pertenezca, así mismo es debe verificar que el equipo de cómputo asignado debe estar debidamente unido al dominio de la Entidad. Lo anterior, acorde a lo establecido en el ítem 2.5 Gestión del Directorio Activo.

- ✓ Se asocia la cuenta de determinado usuario al grupo de navegación correspondiente "teniendo en cuenta las labores a ejecutar" y de acuerdo con los grupos creados en el directorio activo para tal fin (perfil de navegación Usuario Normal – perfil de navegación VIP – perfil de navegación Invitados – perfil de navegación Periodistas – Administradores de la plataforma de Infraestructura).
- ✓ Asociar el punto de red donde se ubique el equipo del usuario a la VLAN correspondiente al área en la cual ejecute las labores propias de su cargo.

- ✓ Si el usuario solicita elevación y/o cambios en los privilegios de navegación, se debe realizar la respectiva solicitud a través de la mesa de servicios, justificando debidamente su requerimiento.
- ✓ Validar que el equipo quede correctamente configurado con los parámetros de red propios de cada VLAN.

Nota: Es de aclarar que a los equipos de personas visitantes les aplica el perfil de navegación de invitados de manera instantánea.

- **NIVEL LOCAL**

Teniendo en cuenta que el control de la navegación en las localidades se realiza por IP, la asignación de dichos permisos se debe realizar de la siguiente manera.

- ✓ Realizar la solicitud a través de la mesa de servicios, indicando el nombre completo del solicitante, dirección IP, Dirección MAC con el fin de dar trámite a la solicitud.
- ✓ Crear el objeto en el firewall principal de acuerdo con los datos suministrados y se asocia al grupo correspondiente definido en el firewall para el control de la navegación.
- ✓ Tramitar la reserva en el DHCP de la dirección IP del equipo del usuario solicitante al especialista competente, por parte de la mesa de servicios.

2.12 GESTIÓN DE LA SEGURIDAD INFORMÁTICA

El objetivo del siguiente paso a paso es adoptar una metodología basada en el OSSTMM (Manual de metodología abierta para el testeo de la seguridad) para ejecutar las pruebas de seguridad externas e internas sin tener en cuenta el grado de importancia de las mismas, para ello se tratara las tomas de muestras de seguridad como únicas e independientes y se definirán políticas preventivas, detectivas y correctivas sobre los servicios que presta la Entidad.

- Realizar la fase de reconocimiento, en la cual se hará análisis caja blanca para el reconocimiento interno y análisis caja gris y caja negra para el reconocimiento externo.
- Continuar con la fase de escaneo a partir de la información obtenida de la fase anterior, con el fin de encontrar vectores de ataque, como servicios provistos por versiones desactualizadas, sin parches y con vulnerabilidades conocidas y se verificara en busca de falsos positivos.
- Realizar la fase de enumeración, mediante la cual se obtiene información importante que puede ser sensible de ataque, como nombres de máquinas, nombres de usuarios, recursos compartidos y demás servicios.
- Iniciar con la fase de acceso (programada, anunciada y autorizada), se aplicaran distintas técnicas de acceso a los servicios o recursos, estos accesos podrán realizarse por fuerza bruta o por exploits conocidos. En esta fase se puede solicitar un snapshot del servicio y hacer un ataque a la aplicación offline sin afectar la producción, con este método se podrá tratar de llegar a escalar privilegios y tomar el control total del sistema.
- Entregar los reportes y recomendaciones para corregir los problemas en caso de encontrarse.

- Repetir todas las fases desde el inicio, para verificar si las vulnerabilidades mencionadas en el reporte anterior fueron solucionadas y para buscar nuevos exploits o fallas de seguridad en los sistemas y se volverá a reportar y recomendar soluciones.
- Durante todo el proceso se deben socializar los problemas de seguridad para que se vayan aplicando correctivos.

Glosario

1. **Concepto:** Su estructura jerárquica permite mantener una serie de objetos relacionados con componentes de una red, como usuarios, grupos de usuarios, permisos y asignación de recursos y políticas de acceso.
2. **Servicio de directorio:** Es uno de los componentes más importantes de una red, ya que organiza la información de los recursos de la red para que los usuarios puedan encontrarla con mayor facilidad.
3. **Administración Centralizada:** Tener toda la información centralizada en un equipo, permite una mejor administración.
4. **Dominio:** Se trata de las unidades centrales en la estructura lógica del Directorio activo que son un conjunto de objetos organizados de forma jerárquica y que comparten una base de datos.
5. **Controlador de Dominio:** Es un servidor que se encarga de la seguridad de un dominio, es decir administra toda la información correspondiente a usuarios y recursos de su dominio.
6. **Unidades Organizativas:** Es una especie de objeto organizativo que contiene objetos del dominio con ciertas características. Si se desea denegar o permitir algo a un grupo de objetos dentro de una unidad organizativa, simplemente se harían los cambios a la unidad organizativa y los objetos la heredarían de éste.
7. **UPS (Uninterruptible Power Supply):** Una UPS es un equipo de suministro de energía eléctrica regulada, con baterías que brindar soporte en el caso de una interrupción eléctrica.
8. **Firewalls:** Son los equipos que permiten garantizar y proteger las comunicaciones internas y externas de la entidad.
9. **Administración Centralizada:** La administración centralizada de los firewalls, permite la seguridad perimetral y local a través de una estandarización en las configuraciones propias de dichos dispositivos.
10. **Equipos Activos:** son los equipos que permiten unificar y/o concentrar las conexiones de los diferentes dispositivos de cómputo que utilizan los usuarios (computadores, impresoras, teléfonos, etc.), para acceder de manera centralizada a los servicios de red.
11. **Administración Centralizada:** La gestión centralizada sobre los equipos de red (switch, routers, AP, etc.), permite una mejor administración y control de cambios sobre la configuración de dichos equipos.

3. DOCUMENTOS DEL SIG RELACIONADOS

CÓDIGO	DOCUMENTO
N/A	No aplica

3.3. Documentos externos

NOMBRE	FECHA DE PUBLICACIÓN O VERSIÓN	ENTIDAD QUE LO EMITE	MEDIO DE CONSULTA
Administración copias de respaldo (Backups)	3 de octubre de 2014	Secretaría General	Intranet de la SDG