PROCESO		
TECNOLOGIAS DE INFORMACIÓN Y COMUNICACIÓN		
CÓDIGO	PROCEDIMIENTO	VERSIÓN
PR-TI-23	GESTION DE TELECOMUNICACIONES	2

PRTI23-Gestión de Telecomunicaciones

Control de Versiones

Versión	Fecha	Descripción Modificación	Folios
2	2020-11-26	Es actualizado el Formato del proceso, marco normativo, términos y definiciones; se ajusta la actividad de gestión de usuarios en la Wifi; se elimina la mención al procedimiento PR-TI-09; se elimina la mención al formato FO-TI-08 por estar derogado.	44
1.0	16/12/2015	Versión inicial	51

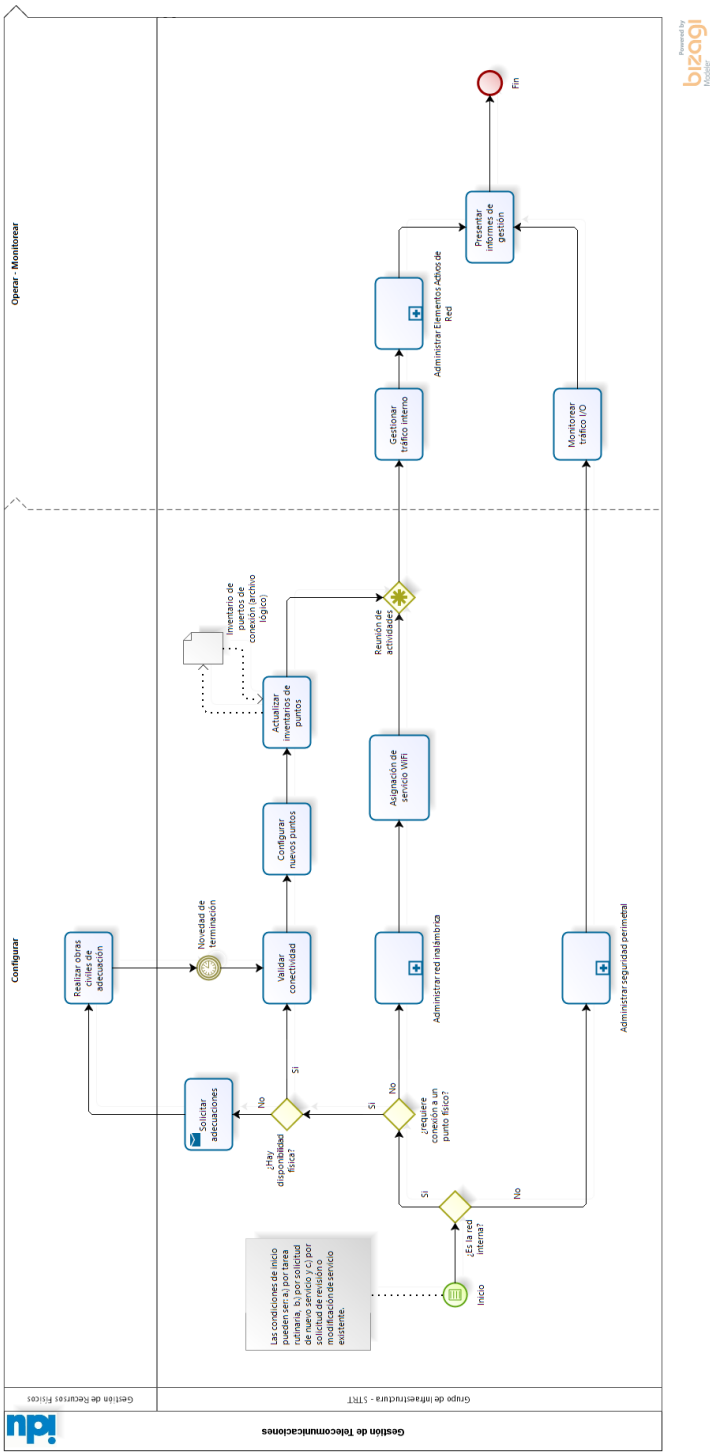
El documento original ha sido aprobado mediante el SID (Sistema Información Documentada del IDU). La autenticidad puede ser verificada a través del código

Participaron en la elaboración[1]	Carlos Fernando Campos Sosa, OAP / Hector Pulido Moreno, STRT / Marco Fidel Guerrero Parada, STRT / Raul Augusto Rodriguez Olaya, STRT /
Validado por	Sandra Milena Del Pilar Rueda Ochoa, OAP Validado el 2020-11-24
Revisado por	Julio Cesar Pinto Villamizar, STRT Revisado el 2020-11-26
Aprobado por	Julio Cesar Pinto Villamizar, STRT Aprobado el 2020-11-26

[1]El alcance de participación en la elaboración de este documento corresponde a las funciones del área que representan

Tabla de Contenidos

GESTIÓN DE TELECOMUNICACIONES



1.GESTIÓN DE TELECOMUNICACIONES

Descripción

Participaron en la elaboración: Héctor Pulido, Profesional STRT y Carlos Fernando Campos Sosa, Oficina Asesora de Planeación

1.1. OBJETIVO

Realizar las actividades administrativas y operativas relacionadas con las redes de datos físicas y lógicas internas y la conectividad hacia el exterior que requiere el Instituto para el manejo y transmisión segura de datos.

1.2. ALCANCE

Este procedimiento abarca de la etapa de configuración de los dispositivos teniendo en cuenta los prerrequisitos y condiciones necesarias para poder brindar el servicio de conectividad a la red local y de acceso a internet, hasta la operación y control de los dispositivos de red interna y externa.

1.3. MARCO NORMATIVO

· Ley 1273 de 05 de enero de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado de la protección de la información y de los datos - y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

· Ley Estatutaria 1581 de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales.

· Ley 1712 de 2014, Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones.

· Decreto 1078 de 2015, Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".

· Resolución Distrital 305 de 2008, Por la cual se expiden políticas públicas para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, caridad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre

· Resolución 004 de 2017, Por la cual se modifica la Resolución 305 de 2008 de la CDS.

· Documento CONPES 3701 de 2011 - Lineamientos de Políticas sobre ciberseguridad y ciberdefensa.

· Documento CONPES 3854 de 2016 - Política Nacional de Seguridad Digital.

· Documento CONPES 3975 de 2019 - Política Nacional para la Transformación Digital e Inteligencia Artificial

· Documento CONPES 3995 de 2020 - Política Nacional De Confianza y Seguridad Digital

· Norma Técnica Colombiana NTC/ISO 27001 versión 2013, Sistemas de Gestión de Seguridad de la Información (SGSI). Requisitos. Anexo A. Control A.13.1. “Gestión de la sefuridad de las redes”

Nota: Las normas de aplicación general y documentos internos (circulares, resoluciones, memorandos) que son parte de este documento, están relacionadas en el normograma del proceso Tecnologías de Información y comunicación publicado en el mapa de procesos.

1.4. TERMINOS Y DEFINICIONES

Los términos y definiciones aplicables al procedimiento pueden ser consultados en el micro sitio Diccionario de términos IDU (https://www.idu.gov.co/page/transparencia/informacion-de-interes/glosario)

- Access Point
- Cableado estructurado
- Face plate
- Firewall
- Login
- IDS
- IP o Internet Protocol
- IPS
- Patch cord
- Patch panel
- PETI
- Proxy Server
- Router
- Seguridad perimetral
- Switch
- STRT
- TIC
- Tráfico I/O
- URL

- VPN
- WiFi

1.5. POLÍTICA OPERACIONAL

1. El tiempo de este procedimiento esta dado en horas.
2. Algunas actividades, tanto de diagnóstico como se atención de solicitudes y/o de configuración dependen de variables específicas de cada situación y de la disponibilidad de recursos, por lo cual los tiempos del procedimiento pueden variar. Para efecto de documentación, se incluyen tiempos promedio por actividades globales.

1.6. ELEMENTOS DEL PROCESO

1.6.1. Inicio

Descripción

Describe las actividades propias de la administración de las telecomunicaciones del Instituto.

Este inicio puede presentarse por:

a.) por tarea rutinaria,

b.) por solicitud de nuevo servicio y/o

c.) por solicitud de revisión o modificación de servicio existente.

1.6.2. ¿Es la red interna?

Descripción

Se evalúa si las actividades a realizar corresponden a la red interna o si por el contrario es para los servicios de la red externa.

Flujos

Si

Condición

Validar... ¿se requiere conexión a un punto físico?

No

Condición

Administrar Seguridad Perimetral

1.6.3. ¿requiere conexión a un punto físico?

Descripción

Se valida si la actividad o servicio a prestar requiere de conexión física, es decir un punto de red en un puesto de trabajo que tiene identificación y se conecta mediante un cable de red (patch cord) o es una conexión totalmente inalámbrica.

Flujos

No

Condición

Ir a Administrar red inalámbrica

Si

Condición

Validar... ¿hay disponibilidad física?

1.6.4. ¿Hay disponibilidad física?

Descripción

Se valida si el puesto de trabajo en donde se prestará el servicio cuenta con la adecuada disposición de conexión (face plate) o si por el contrario será necesario solicitar la adecuación correspondiente al proceso de Gestión de Recursos Físicos.

Flujos

No

Condición

Solicitar adecuaciones

Si

Condición

Validar conectividad

1.6.5. Solicitar adecuaciones

Descripción

Mediante la realización de esta actividad se realiza una solicitud formal proceso de gestión de recursos físicos, de la adecuación o instalación física de los puntos de red en el puesto o puestos de trabajo indicados. En esta solicitud, se deben suministrar detalladamente los datos de Sede, Piso, Área, Puesto o localización en donde se deben adelantar dichos trabajos.

Ejecutantes

Profesional Universitario, Técnico

Implementación

Servicio Web

1.6.6. Realizar obras civiles de adecuación

Descripción

Esta actividad no está bajo el control de procedimiento, pero invita al lector a tener en cuenta que se deben adelantar trabajos de adecuación probablemente locativos y en algunos casos de obra civil, en la estructura física del área, para llevar cables de red (cableado estructurado) desde el punto más próximo de conexión del piso en que se encuentra hasta el puesto de trabajo. A diferencia del tendido de cableado eléctrico, los cables de red requieren condiciones específicas de manejo e instalación a fin de evitar posibles daños en su estructura física, razón por la cual este tipo de trabajos no pueden ser considerados como actividades triviales.

Algunas de las tareas que se cumplen en esta actividad, pueden requerir de la participación activa de personal de la Subdirección Técnica de Recursos Tecnológicos, a fin de validar y asegurar la calidad y completitud de la labor a realizar.

Ejecutantes

Profesional Universitario, Técnico

Punto de Control

El tiempo promedio de tender un nuevo cable de red para un puesto de trabajo (tendido horizontal), puede requerir desde tres (3) horas hasta cinco (5) días, razón por la cual se incluye este tiempo máximo como parámetro de control.

Duración

40.00

1.6.7. Novedad de terminación

Descripción

Esperar la notificación de terminación de las tareas de instalación y adecuación de los puntos físicos de red. Se estima como máximo tiempo cinco (5) días o su equivalente en horas (40).

Ciclo

R1/P5D

1.6.8. Validar conectividad

Descripción

El paso a seguir es validar la conectividad, que consiste en tomar los datos de identificación del externo del usuario (marcación del face plate) y compararlo contra el mismo identificador en el tablero de distribución (patch panel) del centro de cableado del piso correspondiente y posteriormente mediante un dispositivo de generación de tonos o mediante la ubicación de equipos de cómputo que permiten validar la transmisión adecuada de dos entre dichos extremos.

Ejecutantes

Profesional Universitario, Técnico

Duración

2.00

1.6.9. Configurar nuevos puntos

Descripción

Mediante esta actividad se atiende la solicitud de habilitación de un nuevo punto de red (para voz y/o datos), tomando como base la existencia física de una toma identificada y certificada en el nuevo puesto de trabajo con un externo en el centro de cableado correspondiente igualmente identificado y certificado.

En esta actividad se realizan las siguientes tareas puntuales:

Validar contra el inventario de puertos de conexión disponibles de los switches del centro cableado correspondiente.

Luego, se debe conectar físicamente un cable de red entre el panel de conexiones y el puerto del switch previamente identificado.

El siguiente paso es informar al administrador de la red, acerca de las tareas físicas terminadas.

A continuación, se debe ingresar a la consola de administración de los dispositivos activos de red (switch core), para activar la transmisión de datos a través del puerto asignado en el switch del centro de cableado correspondiente.

Luego se vincula dicho puerto del switch con el segmento lógico de red al cual pertenece el usuario que usará el punto de red.

Posteriormente se deben realizar pruebas de conectividad.

Si los resultados son satisfactorios, se procede a informar al usuario solicitante.

Por último, se debe actualizar el inventario de puertos disponibles.

Ejecutantes

Profesional Especializado, Profesional Universitario, Técnico

Duración

4.00

1.6.10. Actualizar inventarios de puntos

Descripción

En este punto se actualiza el documento del inventario de puntos de red con el fin de mantener un control adecuado de la capacidad de conexión del piso que se está afectando y los controles necesarios para determinar necesidades de ampliación o instalación de elementos de red adicionales.

Ejecutantes

Profesional Universitario, Técnico

1.6.11. Administrar red inalámbrica

Ver detalles

Descripción

En esta actividad se describen las tareas necesarias para lleva a cabo la administración de la red inalámbrica o red WiFi.

Ejecutantes

Profesional Especializado

1.6.12. Asignación de servicio WiFi

Descripción

La administración de la Wifi está gestionada por el Clear Pass, que se encuentra vinculada con el Directorio Activo y conceden el acceso, independiente si es usuario visitante o del IDU.

Si el usuario es visitante, al hacer la conexión con el punto Wifi, se despliega un Portal Cautivo, donde le solicita los datos para el ingreso (Nombre de la Empresa, correo electrónico, correo del usuario que acompaña por parte del IDU, a quien le debe aceptar la petición. Acto seguido al visitante le llegan las credenciales de ingreso; las credenciales tienen una vigencia de 2 horas, renovables.

Duración

1.00

1.6.13. Reunión de actividades

Descripción

Se centralizan los diversos flujos de trabajo que se presentan en la Gestión de Telecomunicaciones

Flujos

Gestionar tráfico interno

1.6.14. Gestionar tráfico interno

Descripción

Esta actividad comprende las tareas del administrador de la red interna que están encaminadas a revisar las consolas de monitoreo de los dispositivos de red, para determinar su adecuado funcionamiento y validación respecto a las condiciones esperadas de intercambio de datos.

Estas tareas incluyen:

- Revisar el tráfico entre compuertas lógicas de la red interna.
- Validar el uso de ancho de banda entre redes lógicas.
- Analizar posibles colisiones (A medida que aumenta el número de nodos que pueden transmitir en un segmento de red, aumentan las posibilidades de que dos de ellos transmitan a la vez. Esta transmisión simultánea ocasiona una interferencia entre las señales de ambos nodos, que se conoce como colisión. Conforme aumenta el número de colisiones disminuye el rendimiento de la red.)
- Control de difusión de datos por segmento lógico de red.
- Identificación de uso excesivo (abuso) de los recursos de red (transmisión de archivos no autorizados)
- Validar el estado actual de transmisión de los diferentes elementos activos de red (switches, bridges, routers, concentradores, puntos de acceso).
- Determinar medidas de cancelación de procesos, elevación de consultas o apertura de casos de seguridad de la información asociados al análisis de los datos de tráfico de red.

Ejecutantes

Profesional Universitario, Técnico

Duración

2.00

1.6.15. Administrar Elementos Activos de Red

Ver detalles

Descripción

Esta actividad, describe el conjunto de tareas relacionadas con configuración y gestión los elementos activos de red de la institución.

Ejecutantes

Profesional Especializado

1.6.16. Administrar seguridad perimetral

Ver detalles

Descripción

En esta actividad se describen las tareas necesarias para administrar los dispositivos y servicios que protegen las comunicaciones de datos entrantes y salientes del Instituto de posibles ataques o intrusiones no autorizadas.

1.6.17. Monitorear tráfico I/O

Descripción

El Administrador de la seguridad perimetral, debe monitorear constantemente el uso de los servicios entrantes y salientes.

En estas labores de monitoreo se deben analizar los registros de eventos que los dispositivos de seguridad perimetral reporten como anormales o intentos de ataque, con el fin de determinar posibles incidentes de seguridad de la información. Todo el tráfico entrante que se compruebe como un "ataque" informático deberá ser inmediatamente bloqueado, y se procederá a reportar a los funcionarios y entidades competentes acerca del suceso.

De igual forma, será necesario que se controlen las actividades de intercambio de información que se efectúen por medio del correo electrónico, las VPN y los servicios de FTP, con el fin de analizar posibles usos indebidos o fugas de información de la institución.

Ejecutantes

Técnico, Profesional Universitario

Duración

2.00

1.6.18. Presentar informes de gestión

Descripción

En esta actividad se unifican los resultados de las actividades realizadas en el periodo y se presenta un informe de la gestión de telecomunicaciones.

Ejecutantes

Profesional Universitario, Técnico

Duración

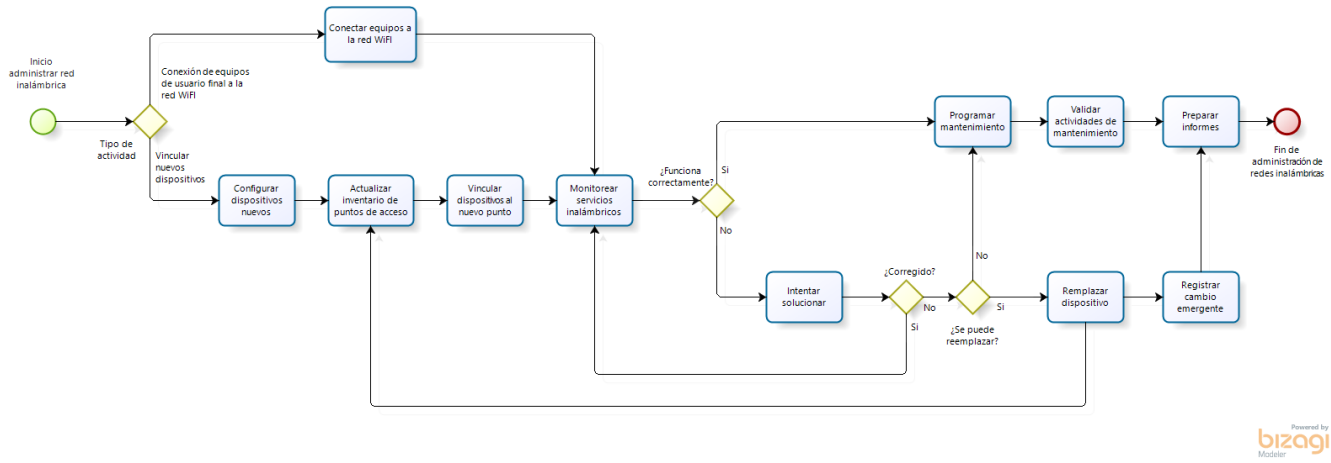
16.00

1.6.19. Fin

Descripción

Terminación del procedimiento de administración de Telecomunicaciones.

2.ADMINISTRAR RED INALÁMBRICA



2.1. ELEMENTOS DEL PROCESO

2.1.1. Inicio administrar red inalámbrica

Descripción

Se marca el inicio de actividades para gestionar la red inalámbrica del Instituto.

2.1.2. Tipo de actividad

Descripción

Se hace la validación acerca del tipo de acción a realizar que puede ser: atender solicitudes o configurar dispositivos.

Flujos

Vincular nuevos dispositivos

Condición

Configurar dispositivos nuevos

Conexión de equipos de usuario final a la red WiFI

2.1.3. Configurar dispositivos nuevos

Descripción

En esta actividad se realiza la adecuación lógica de los nuevos dispositivos que son recibidos para permitir la conexión inalámbrica de dispositivos a la red de datos y servicios ofrecidos a través de ella.

Los pasos mínimos que se deben realizar son:

- Asignar la dirección IP del dispositivo
- Establecer credenciales de administración del dispositivo
- Asignación de nombre de red (SSID)
- Definición de los protocolos de red aceptados (p.e. 802.11 a/b/g)
- Definición del canal y la frecuencia válida de emisión de datos (Channel 11, 2462 MHz)
- Definir método de aislamiento del dispositivo
- Definir el protocolo de seguridad y la contraseña de vinculación (WAP 2)

Ejecutantes

Profesional Universitario, Técnico

Duración

3.00

2.1.4. ☐ Actualizar inventario de puntos de acceso

Descripción

Esta actividad consiste en actualizar el archivo de la Subdirección Técnica de Recursos Tecnológicos los con los datos del nuevo dispositivo de acceso inalámbrico.

Ejecutantes

Profesional Universitario, Técnico

Duración

1.00

2.1.5. ☐ Vincular dispositivos al nuevo punto

Descripción

Una vez el dispositivo de acceso ha sido instalado en la zona a la cual debe brindar servicio de conexión, se deben vincular o registrar los dispositivos que pueden acceder a la red a través de dicho dispositivo.

Ejecutantes

Profesional Universitario, Técnico

Duración

2.00

2.1.6. Monitorear servicios inalámbricos

Descripción

Esta actividad consiste en revisar el normal funcionamiento de los diferentes access point del Instituto y de paso confrontar el adecuado uso que le dan los usuarios, ante la verificación de los registros automáticos de cada uno de estos dispositivos.

Ejecutantes

Profesional Universitario, Técnico

Duración

1.00

2.1.7. ¿Funciona correctamente?

Descripción

Se valida si el dispositivo operar de manera adecuada.

Flujos

Si

Condición

Programar mantenimiento

No

Condición

Intentar solucionar

2.1.8. Intentar solucionar

Descripción

En esta actividad el administrador de los access point, mediante los instructivos del fabricante procederá a realizar los diagnósticos y taras de ajuste y reconfiguración con el propósito de solucionar las advertencias, alertas o errores que están reportándose.

Ejecutantes

Profesional Universitario, Técnico

Duración

4.00

2.1.9. ¿Corregido?

Descripción

Se valida la efectividad de las acciones de solución realizadas por el responsable de administrar estos dispositivos.

Flujos

No

Condición

Validar ... ¿se puede remplazar?

Si

Condición

Monitorear servicios inalámbricos

2.1.10. ¿Se puede reemplazar?

Descripción

Se valida la disponibilidad de dispositivos en almacén o cuyo reporte de uso indique que es poco utilizado.

Flujos

No

Condición

Programar mantenimiento

Si

Condición

Reemplazar dispositivo

2.1.11. ☐ Remplazar dispositivo

Descripción

Esta actividad consiste en retirar de la ubicación física actual el dispositivo que presenta fallas o advertencias de funcionamiento y colocar un dispositivo de remplazo, tomado del inventario de equipos disponibles o por traslado de un dispositivo de poco uso en otra área o sede del Instituto.

El retiro implica que se deban realizar las actualizaciones de registros en el inventario correspondiente.

Por último, se deben validar los plazos y condiciones de garantías vigentes respecto al access point retirado, para determinar si se puede remplazar o dar de baja definitivamente.

Ejecutantes

Profesional Universitario, Técnico

Duración

3.00

2.1.12. ☐ Registrar cambio emergente

Descripción

Una vez realizado el remplazo y confirmada su adecuada operatividad se debe registrar el suceso como un cambio emergente que se debe presentar a la mesa de trabajo de gestión de cambios de TI, para que se lleve un control sobre los elementos de configuración y sobre los componentes de infraestructura asociados.

Ejecutantes

Profesional Universitario, Técnico

Duración

0.30

2.1.13. ☐Programar mantenimiento

Descripción

Para los access point que estén cubiertos con garantías de funcionamiento vigentes o contratos de mantenimiento, se debe programar un mantenimiento preventivo periódico el cual incluya las tareas de limpieza física y actualizaciones lógicas que correspondan.

Cuando se presentan eventos de falla, advertencia o error no superados con actividades internas, se debe programar una visita de mantenimiento correctivo, a fin de coordinar con el proveedor las actividades de reparación o sustitución que sean adecuadas para volver a disponer de los dispositivos en operación normal.

Ejecutantes

Profesional Universitario, Técnico

Duración

8.00

2.1.14. ☐Validar actividades de mantenimiento

Descripción

En esta actividad el responsable de la administración de los access point y de los servicios de la red inalámbrica revisará los resultados de las tareas y actividades realizadas por el proveedor, respecto a los mantenimientos (preventivos o correctivos) realizados, con el fin de aceptar o rechazar los resultados derivados de dichas tareas.

Ejecutantes

Profesional Universitario, Técnico

Duración

8.00

2.1.15. ☐Preparar informes

Descripción

En esta actividad que se debe realizar mensualmente, se reúnen los registros de las actividades ejecutadas en el periodo para administrar los servicios de red inalámbrica ofrecidos al Instituto, para crear informe que contenga los resultados de los eventos más significativos, los cambios efectuados, la disponibilidad y el uso de estos servicios y posibles recomendaciones que se deriven de esta gestión.

Ejecutantes

Profesional Universitario, Técnico

Duración

16.00

2.1.16. Fin de administración de redes inalámbricas

Descripción

Se marca el fin de las actividades de la gestión de la red inalámbrica y los servicios ofrecidos a través de ella.

2.1.17. Conectar equipos a la red WiFI

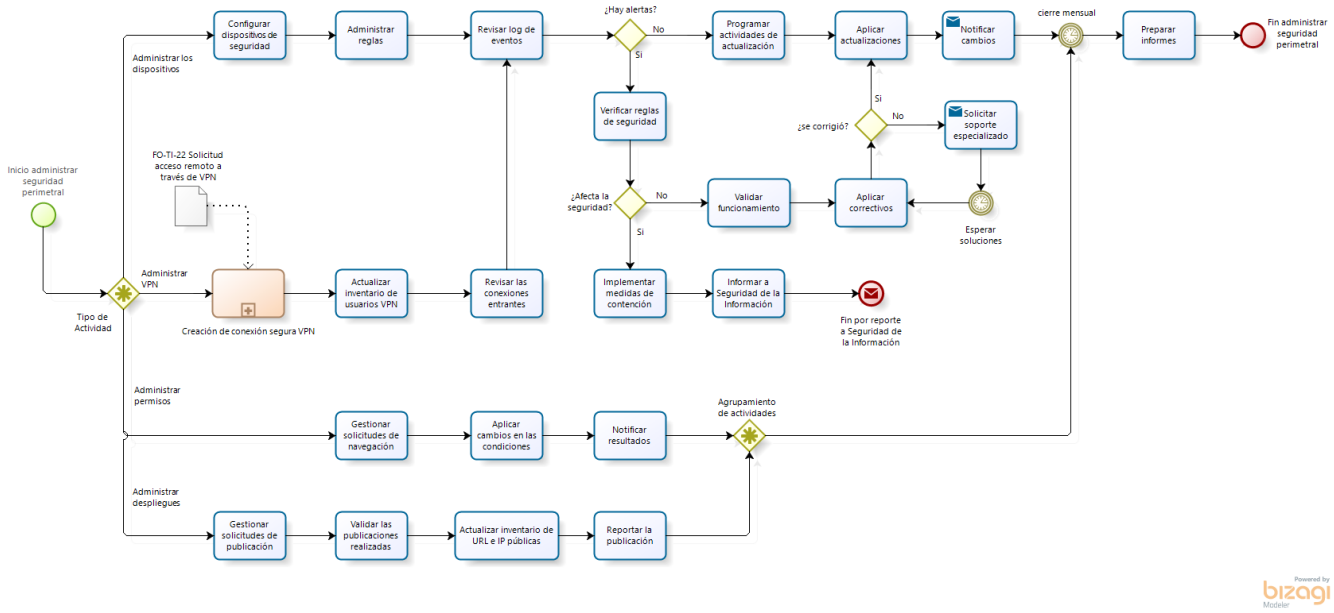
Descripción

Realizar tareas de soporte de segundo nivel de atención a usuarios, relacionados con la conexión de los dispositivos a la red WIFI, una vez cumplidas las condiciones de prestación del servicio.

Duración

1.00

3.ADMINISTRAR SEGURIDAD PERIMETRAL



3.1. ELEMENTOS DEL PROCESO

3.1.1. Inicio administrar seguridad perimetral

Descripción

Este procedimiento contiene las actividades principales de la gestión de la seguridad lógica perimetral. Se puede iniciar por ingreso de nuevos dispositivos, por gestión de las conexiones entrantes, por la administración de permisos o por la colaboración en la publicación de nuevos servicios.

Tipo de Actividad

Descripción

Dependiendo del tipo de actividad se elige alguna de las rutas de acción para la gestión de la seguridad perimetral.

Flujos

Administrar permisos

Condición

Gestionar solicitudes de navegación

Administrar VPN

Condición

Gestionar solicitudes de acceso remoto

Administrar los dispositivos

Condición

Configurar dispositivos de seguridad

Administrar despliegues

Condición

Gestionar solicitudes de publicación

3.1.2. Creación de conexión segura VPN

Descripción

Esta es una actividad de soporte de segundo nivel, que consiste en recibir los datos de la solicitud que se soporta en el formato de solicitud de acceso remoto a través de VPN. Todas las tareas que implican esta gestión se describen el procedimiento PR-TI-10 Creación de conexión segura VPN.

Por definición este acceso remoto se otorga a los funcionarios de planta del Instituto que están autorizados a realizar TELETRABAJO, que deben surtir todo el trámite previo dispuesto por el proceso de Gestión del Talento Humano para tal fin.

También se puede conceder acceso remoto a colaboradores (de planta o contratistas) que deben realizar tareas puntuales de a través de este tipo de conexión, la cual debe contar con las justificaciones y autorizaciones indicadas en el formato de soporte, así como la definición de las fechas desde ya hasta cuándo está vigente dicha autorización.

Ejecutantes

Técnico, Profesional Universitario

3.1.3. Actualizar inventario de usuarios VPN

Descripción

Esta es una actividad de control administrativo, que consiste en registrar en el control de conexiones remotas, los usuarios autorizados para ingresar a través de VPN.

Ejecutantes

Profesional Universitario, Técnico

Duración

1.00

3.1.4. Revisar las conexiones entrantes

Descripción

Una vez se han establecido las conexiones, se deben realizar un control preventivo o monitoreo del uso de estos servicios, con el fin de controlar el uso adecuado de permisos y privilegios otorgados, así como para validar los niveles de uso del ancho de banda y transmisión de datos asociados a estos servicios. Este control debe realizarse al menos una vez a la semana.

Ejecutantes

Profesional Universitario, Técnico

Duración

2.00

3.1.5. Configurar dispositivos de seguridad

Descripción

Esta actividad consiste en recibir los dispositivos que se deben ingresar a la administración de seguridad perimetral del Instituto. Por definición la estrategia de seguridad perimetral lógica, está centrada en el principio de control de uso (entrante y saliente) de las redes públicas y para cumplir con este objetivo puede disponer de varios elementos físicos y/o lógicos que le permiten cumplir esta labor.

Entre los dispositivos de seguridad perimetral que se pueden encontrar, como son el Firewall, el IDS, el ISP y el Proxy server, se deben coordinar procesos de configuración inicial antes de ser incorporados y desplegados en el ambiente de producción. Esta configuración debe estar acorde con las necesidades de conexión definidas por el Instituto, los niveles de riesgos que se hayan identificado y valorado y por las buenas prácticas de la industria de las telecomunicaciones.

Las condiciones o pasos de configuración de cada dispositivo de seguridad perimetral son particulares a cada elemento, sin embargo, se deben contemplar al menos los siguientes pasos:

En principio, una de las primeras actividades de configuración será el cambio o bloqueo de las contraseñas de acceso que estos dispositivos traen desde su origen (contraseñas default o de fábrica).

A continuación, debería implementarse una "denegación total de servicios" (deny all), bajo el principio general de seguridad que dice: "lo que no está explícitamente permitido, está totalmente prohibido".

El paso a seguir es implementar las políticas o condiciones de operación de cada servicio que debe ser activado, creando un documento formal denominado reglas de seguridad perimetral, que no es otra cosa que la descripción de cada uno de los permisos, privilegios y registros otorgados a cada servicio requerido.

A partir de este momento se deben realizar las consabidas pruebas de operación, con el fin de preparar el despliegue o paso a producción del dispositivo.

Ejecutantes

Profesional Universitario, Técnico

Duración

40.00

3.1.6. ☐Administrar reglas

Descripción

En esta actividad el responsable de la administración de la seguridad perimetral y de los dispositivos asociados, debe llegar un control de las condiciones de operación que se han configurado en cada elemento, puesto que, ante posibles solicitudes de acceso o navegación, se deben evitar traslapes o conflictos de definición que anulen las restricciones o controles actuales.

Ejecutantes

Profesional Universitario, Técnico

Duración

1.00

3.1.7. ☐Revisar log de eventos

Descripción

El responsable de la administración de la seguridad perimetral y de los dispositivos asociados, debe revisar rutinariamente (preferiblemente a diario) los registros de eventos de cada uno de estos dispositivos con el fin de identificar posibles alertas no reportadas de forma automática, o advertencias sobre el funcionamiento del dispositivo.

Ejecutantes

Profesional Universitario, Técnico

Duración

1.00

3.1.8. ¿Hay alertas?

Descripción

Se verifica la existencia de alertas en los registros automáticos de los dispositivos.

Flujos

No

Condición

Programar actividades de actualización

Si

Condición

Verificar reglas de seguridad

3.1.9. Verificar reglas de seguridad

Descripción

Mediante la realización de esta actividad, se verifican los registros de alerta comparándolos contra las reglas o políticas operativas configuradas en el dispositivo, con el fin de identificar qué tipo de evento que se está presentando.

Ejecutantes

Profesional Universitario, Técnico

Duración

1.00

3.1.10. ¿Afecta la seguridad?

Descripción

Se valida si la verificación arroja como resultado una afectación a la seguridad.

Flujos

Si

Condición

Implementar medidas de contención

No

Condición

Validar funcionamiento

3.1.11. Validar funcionamiento

Descripción

Ante la verificación de que no hay afectación de la seguridad perimetral y que no se ha comprometido la información de Instituto, se debe proceder a verificar el correcto funcionamiento del dispositivo que reporta la alerta. Se debe tener acceso a la documentación técnica y de soporte otorgada por el fabricante respecto al dispositivo, con el fin de descartar cualquier falla que pueda deshabilitar parcial o totalmente el dispositivo.

Ejecutantes

Profesional Universitario, Técnico

Duración

2.00

3.1.12. Aplicar correctivos

Descripción

En esta actividad, se deben realizar las tareas que sean pertinentes (propias o indicadas por el proveedor) para solucionar los impases o alertas reportadas por el dispositivo.

Ejecutantes

Profesional Universitario, Técnico

Duración

2.00

3.1.13. ¿se corrigió?

Descripción

Se valida que las soluciones hayan sido efectivas, de lo contrario se debe escalar al proveedor para solicitar soporte especializado.

Flujos

Si

Condición

Aplicar correctivos

No

Condición

Solicitar soporte especializado

3.1.14. Solicitar soporte especializado

Descripción

Mediante el uso de los canales acordados, se debe reportar al proveedor del dispositivo los eventos acontecidos y las acciones que fueron emprendidas, con el fin de obtener una pronta solución, respecto a la alerta presentada.

Ejecutantes

Profesional Universitario, Técnico

Implementación

Servicio Web

3.1.15. Esperar soluciones

Descripción

Se considera que este tipo de dispositivos no pueden detenerse sin una causa justificada, razón por la cual los tiempos de solución pactados con el proveedor no deben superar las ocho (8) horas.

3.1.16. Implementar medidas de contención

Descripción

Cuando se compromete la integridad, disponibilidad o confidencialidad de la información o la operatividad de los dispositivos, se deben realizar todas las medidas que sean necesarias para evitar que los eventos o daños puedan ser mayores.

Estas medidas pueden incluir:

- Bloqueo de las direcciones IP (públicas o internas) que están produciendo la alerta.
- Desconexión física o lógica de los equipos que están produciendo la alerta.
- Grabación de los eventos que están produciendo la alerta.
- Reporte a las autoridades policiales o jurídicas respecto a los eventos ocurridos.

IMPORTANTE: Esta actividad no puede terminar si no se contiene o detiene el evento o alerta reportada. Por el contrario, si requiere de la participación de otros grupos de trabajo, estos deberán atender y apoyar en el menor tiempo posible el requerimiento de seguridad.

Ejecutantes

Profesional Universitario, Técnico

Duración

2.00

3.1.17. Informar a Seguridad de la Información

Descripción

Una vez se ha logrado estabilizar el evento o alerta, se debe informar al Subsistema de Gestión de Seguridad de la Información del Instituto, a fin de que se tomen las acciones y revisiones que sean pertinentes.

Ejecutantes

Profesional Universitario, Técnico

Duración

1.00

3.1.18. Fin por reporte a Seguridad de la Información

Descripción

Se finalizan las actividades por reporte a SGSI.

3.1.19. Programar actividades de actualización

Descripción

Para los dispositivos de seguridad perimetral, se deben realizar actividades periódicas programadas de revisión, actualización y mantenimiento preventivo.

La mayoría de actualizaciones están relacionadas con los archivos y parámetros de control y funcionamiento de las actividades de control propias de cada dispositivo que no implican la detención o cambios de los servicios prestados, como pueden ser la actualización de firmas autorizadas de paquetes informáticos, registros de las bases de datos de antivirus, registros de direcciones válidas, la inclusión de listas de validación (black list) y listas de prevención.

Algunas actividades asociadas con el mantenimiento preventivo, si implican detención de servicios como por ejemplo las actualizaciones de micro código del fabricante o la actualización de parches de seguridad para los sistemas operativos de los dispositivos (cuando aplique). En estos casos se deben programar dichas actividades preferiblemente para días y horarios no hábilies y se deben presentar como una solicitud de cambio a la mesa de trabajo de gestión de cambios de TI, con el fin de obtener su aprobación y consentimiento de realización.

Ejecutantes

Profesional Universitario, Técnico

Duración

4.00

3.1.20. Aplicar actualizaciones

Descripción

En esta actividad, el responsable de la seguridad perimetral, realiza las tareas que sean necesarias para actualizar el dispositivo, bien sea para atender labores programadas o para cumplir con actividades específicas resultantes de atención de eventos seguridad o alertas de operación. Estas actualizaciones pueden afectar la configuración del dispositivo o de los servicios atendidos a través de él, razon por la cual cuando son actualizaciones programadas se deben presentar a la mesa de trabajo de gestión de cambios de TI con la debida anticipación y cuando corresponden a actualizaciones no programadas se deben presentar a la mesa de trabajo de gestión de cambios de TI como cambio emergente.

Ejecutantes

Técnico, Profesional Universitario

Duración

8.00

3.1.21. Notificar cambios

Descripción

Esta actividad consiste en notificar a la mesa de trabajo de gestión de cambios de TI las actividades de actualización que se deben aplicar a los dispositivos de seguridad perimetral, por cualquiera de las motivaciones posibles (atención programada o evento emergente).

Ejecutantes

Profesional Universitario, Técnico

Implementación

Servicio Web

3.1.22. ☐Gestionar solicitudes de publicación

Descripción

Esta actividad debe realizarse cuando se ha terminado o adquirido un servicio o aplicación que se debe exponer o publicar a través de las redes públicas (servicios web hacia Internet).

Estas solicitudes deben contener las condiciones de operación, tipo de seguridad aplicable, interacción y re direccionamiento interno de solicitudes, con el fin de poder confrontar dichos requerimientos contra las reglas de seguridad perimetral aplicables que se deben modificar o construir.

Ejecutantes

Profesional Universitario, Técnico

Duración

8.00

3.1.23. ☐Validar las publicaciones realizadas

Descripción

Esta actividad consiste en la revisión detallada de los servicios que se han publicado para tender la solicitud realizada, respecto al tráfico de datos entrantes y salientes que se realizan a través de este servicio, controlar los registros de los dispositivos de seguridad perimetral involucrados y las posibles novedades reportadas formalmente a través de los canales dispuestos de atención (internamente registro de la mesa de servicios o externamente a través de las solicitudes que recibe la Oficina de Atención al Ciudadano) frente al servicio publicado.

Ejecutantes

Profesional Universitario, Técnico

Duración

40.00

3.1.24. ☐ Actualizar inventario de URL e IP públicas

Descripción

Una vez que se han publicado los servicios o aplicaciones a través de las redes públicas, con las debidas validaciones y ajustes, será necesario actualizar los registros de inventario de servicios publicados con los datos de dirección visible al usuario (URL), de dirección IP utilizada, puertos de comunicación usados para servicio y para mantenimiento y re direccionamientos hacia la red interna aplicables.

Ejecutantes

Profesional Universitario, Técnico

Duración

2.00

3.1.25. ☐ Reportar la publicación

Descripción

Concluido el proceso de publicación, validación y actualización de los registros correspondientes se debe notificar formalmente al solicitante de la publicación que los servicios o aplicaciones han quedado totalmente disponibles, según lo requerido.

Ejecutantes

Profesional Universitario, Técnico

Duración

2.00

3.1.26. ☐ Gestionar solicitudes de navegación

Descripción

Esta actividad consiste en atender los requerimientos de segundo nivel que hacer referencia al uso de Internet por parte de los usuarios.

Básicamente los usuarios del Instituto, pueden hacer uso de consulta de información a través de internet, cuyo acceso está controlado de acuerdo a las buenas prácticas de uso de los recursos.

Algunos sitios de consulta que no están debidamente clasificados, pueden presentar restricciones de acceso, razón por la cual el administrador de la seguridad perimetral debe realizar las validaciones correspondientes, para que dependiendo de las características del sitio o servicio al que están solicitando acceder, se procede a conceder o a revocar los permisos correspondientes.

Ejecutantes

Profesional Universitario, Técnico

Duración

2.00

3.1.27. ☐Aplicar cambios en las condiciones

Descripción

De acuerdo con las validaciones de seguridad e integridad de solicitudes de navegación atendidas, se procede a realizar los cambios en las reglas o políticas de navegación aplicables al usuario o grupos de usuarios.

Ejecutantes

Técnico, Profesional Universitario

Duración

2.00

3.1.28. ☐Notificar resultados

Descripción

Mediante esta actividad se le informa al solicitante, respecto a la aprobación o rechazo de las solicitudes de modificación a los permisos de navegación y se procede a cerrar y documentar los casos que la hayan sido asignados. Si esta solicitud no fue realizada por este medio, el administrador de la seguridad perimetral deberá hacer el trámite de documentación de la solicitud en la herramienta de mesa de servicios.

Ejecutantes

Profesional Universitario, Técnico

Duración

1.00

3.1.29. Agrupamiento de actividades

Descripción

Metodológicamente, se incluye esta compuerta para unir los flujos de trabajo de las acciones realizadas para gestionar solicitudes de navegación y para gestionar solicitudes de publicación de servicios

Flujos

cierre mensual

3.1.30. cierre mensual

Descripción

Las actividades descritas en este procedimiento se cumplen en ciclos mensuales para facilitar el control y evaluación de la gestión.

3.1.31. Preparar informes

Descripción

En esta actividad que se debe realizar mensualmente, se reúnen los registros de las actividades ejecutadas en el periodo relacionado con la gestión de la seguridad perimetral, para crear informe que contenga los resultados de los eventos más significativos, los cambios efectuados, la disponibilidad y el uso de estos servicios y posibles recomendaciones que se deriven de esta gestión.

Ejecutantes

Profesional Universitario, Técnico

Duración

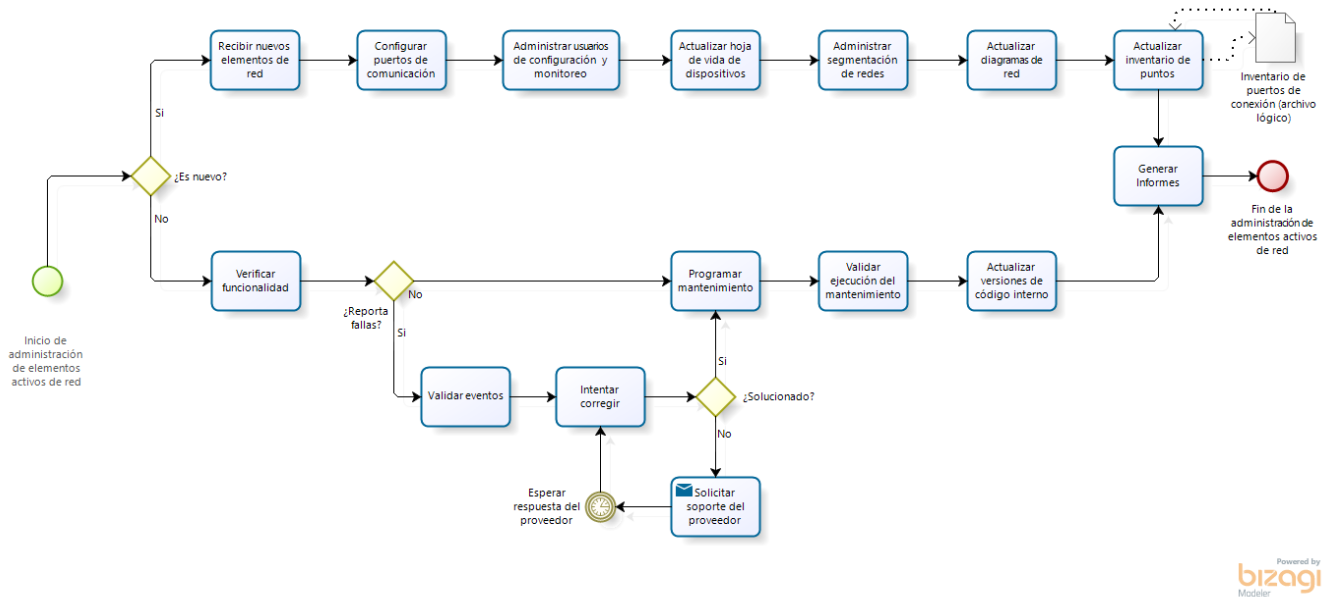
16.00

3.1.32. Fin administrar seguridad perimetral

Descripción

Se marca la finalización de actividades de gestión de la seguridad perimetral.

4.ADMINISTRAR ELEMENTOS ACTIVOS DE RED



4.1. ELEMENTOS DEL PROCESO

4.1.1. Inicio de administración de elementos activos de red

Descripción

Se marca el inicio de la gestión de la administración de elementos activos de la red (switch, routers, bridges, switch de borde) que permiten la prestación de los servicios de intercambio de datos lógicos a través de la red local (LAN).

4.1.2. ¿Es nuevo?

Descripción

Se valida que conjunto de actividades se deben realizar tanto para equipos nuevos como para equipos ya instalados.

Flujos

No

Condición

Verificar funcionalidad

Si

Condición

Recibir nuevos elementos de red

4.1.3. Verificar funcionalidad

Descripción

Esta es una actividad rutinaria que debe realizarse a diario, y consiste en verificar los resultados de las consolas de monitoreo y de la revisión de los registros automáticos de cada elemento activo de red, con el fin de descartar posibles anomalías, detectar condiciones irregulares de operación y posibles alertas tempranas respecto a cada elemento.

Ejecutantes

Profesional Universitario, Técnico

Duración

1.00

4.1.4. ¿Reporta fallas?

Descripción

Se verifica sí existen fallas o alarmas en elemento activo de red.

Flujos

Si

Condición

Validar eventos

No

Condición

Programar mantenimiento

4.1.5. Validar eventos

Descripción

En esta actividad se hace una revisión de los archivos de registro (logs) para confirmar la alerta o falla. Se descartan actividades externas que hayan podido producir el evento como pueden ser fluctuaciones o cortes de energía eléctrica o aumentos de temperatura en el área en donde está ubicado.

Se toma nota de los códigos de alerta o alarma y se hacen las consultas correspondientes en la documentación suministrada por el fabricante y/o en los foros especializados publicados en Internet para determinar los pasos a seguir respecto a cada caso.

Ejecutantes

Profesional Universitario, Técnico

Duración

1.00

4.1.6. Intentar corregir

Descripción

En esta actividad, se deben realizar todas las tareas que sean pertinentes (propias o indicadas por el proveedor) para solucionar los impases o alertas reportadas por el elemento activo de red que se está atendiendo.

Ejecutantes

Profesional Universitario, Técnico

Duración

1.00

4.1.7. ¿Solucionado?

Descripción

Se verifica que las acciones realizadas hayan solucionado la alerta o falla registrada.

Flujos

Si

Condición

Programar mantenimiento

No

Condición

Solicitar soporte del proveedor

4.1.8. Solicitar soporte del proveedor

Descripción

Mediante el uso de los canales acordados, se debe reportar al proveedor del elemento activo de red, los eventos acontecidos y las acciones que fueron emprendidas, con el fin de obtener una pronta solución, respecto a la alerta presentada.

Ejecutantes

Profesional Universitario, Técnico

Implementación

Servicio Web

4.1.9. Esperar respuesta del proveedor

Descripción

El proveedor mediante los canales acordados remitirá alternativas de solución sobre el caso reportado. Este tiempo no puede ser mayor a cinco (5) días o cuarenta (40) horas hábiles.

4.1.10. Programar mantenimiento

Descripción

Para los elementos activos de red, se deben realizar actividades periódicas programadas de revisión, actualización y mantenimiento preventivo y cuando sea relevante, se deben programar actividades puntuales de mantenimiento correctivo, para solucionar alertas o fallas que se hayan presentado sobre alguno de dichos elementos.

Ejecutantes

Profesional Universitario, Técnico

Duración

8.00

4.1.11. ☐Validar ejecución del mantenimiento

Descripción

En esta actividad el responsable de la administración de los elementos activos de red revisará los resultados de las tareas y actividades realizadas internamente o por el proveedor asignado, respecto a los mantenimientos (preventivos o correctivos) realizados, con el fin de aceptar o rechazar los resultados derivados de dichas tareas.

Ejecutantes

Profesional Universitario, Técnico

Duración

2.00

4.1.12. ☐Actualizar versiones de código interno

Descripción

En esta actividad se deben aplicar las actualizaciones de código interno o micro código de los elementos activos de red, de acuerdo con las recomendaciones de los fabricantes, con el objetivo de disminuir o cerrar brechas de seguridad, mejorar el rendimiento o corregir posibles fallas operativas.

Ejecutantes

Profesional Universitario, Técnico

Duración

2.00

4.1.13. ☐Recibir nuevos elementos de red

Descripción

En esta actividad se realiza la recepción formal del elemento activo de red (nuevos dispositivos o transferidos) para ser revisados y configurados según las instrucciones definidas para cada elemento en el Instituto.

Cada dispositivo que conforma la red tiene algunas características propias que se deben configurar dependiendo de su función, marca y modelo, pero en general se deben aplicar al menos los siguientes parámetros:

- Asignar la dirección IP de administración del dispositivo
- Establecer credenciales de administración del dispositivo

Ejecutantes

Profesional Universitario, Técnico

Duración

2.00

4.1.14. ☐ Configurar puertos de comunicación

Descripción

En esta actividad, el responsable de la administración de los elementos activos de red debe habilitar los puertos de comunicación de administración y de enlace, así como también deshabilitará los demás puertos, con el propósito de brindar la primera capa de seguridad que consiste en evitar conexiones no autorizadas a través de estos puertos.

En los casos en donde el dispositivo que se está configurando vaya a ser instalado y puesto en operación, se deben habilitar únicamente los puertos que se han documentado como necesarios para la interconexión a la red.

Ejecutantes

Profesional Universitario, Técnico

Duración

2.00

4.1.15. ☐ Administrar usuarios de configuración y monitoreo

Descripción

Se hace una relación de los usuarios definido para llevar a cabo la configuración y monitoreo del dispositivo, así como la vinculación del dispositivo a las consolas de administración remota (si aplica) o la habilitación de los protocolos de administración remota (sin aplica).

Se verifica no localmente en el dispositivo no existan o queden habilitados más usuarios de los que se requieran.

Ejecutantes

Profesional Universitario, Técnico

Duración

1.00

4.1.16. ☐ Actualizar hoja de vida de dispositivos

Descripción

En esta actividad se crean o actualizan los registros de control de los elementos activos de red, conocidos como hoja de vida de dispositivos.

Ejecutantes

Profesional Universitario, Técnico

Duración

1.00

4.1.17. ☐ Administrar segmentación de redes

Descripción

Cuando sea pertinente se aplican las condiciones de vinculación, desvinculación, revisión, control de tráfico y monitoreo de las redes virtuales (VLAN) configurados para facilitar la administración y seguridad de la red.

Ejecutantes

Profesional Universitario, Técnico

Duración

2.00

4.1.18. ☐ Actualizar diagramas de red

Descripción

En esta actividad se crean y actualizan los diagramas y gráficas que permiten una adecuada gestión de la red. Estas gráficas pueden ser generales (topografía de la red del Instituto), detalladas (topografía de la red de cada sede y/o piso), de segmentación (administración de VLAN) y de gestión de centros de cableado.

Ejecutantes

Técnico, Profesional Universitario

Duración

8.00

4.1.19. Actualizar inventario de puntos

Descripción

En este punto se actualiza el documento del inventario de puntos de red con el fin de mantener un control adecuado de la capacidad de conexión del piso que se está afectando y los controles necesarios para determinar necesidades de ampliación o instalación de elementos de red adicionales.

Ejecutantes

Profesional Universitario, Técnico

Duración

1.00

4.1.20. Generar Informes

Descripción

En esta actividad que se debe realizar mensualmente, se reúnen los registros de las actividades ejecutadas en el periodo relacionadas con la gestión de los elementos activos de red, para crear informe que contenga los resultados de los eventos más significativos, los cambios efectuados, la disponibilidad y el uso de estos servicios y posibles recomendaciones que se deriven de esta gestión.

Ejecutantes

Profesional Universitario, Técnico

Duración

1.00

4.1.21. Fin de la administración de elementos activos de red

Descripción

Marca el fin de las actividades propias de la administración de elementos activos de red.