MANUAL DE SEGURIDAD DE LA INFORMACIÓN

MARTHA CECILIA CASTRILLÓN

Gerente ESE Metrosalud

Dirección de Sistemas de Información

28/09/2021

Versión [02]

Alcaldía de Medellín

Contenido

PLATAFORMA ESTRATÉGICA Y CONTENIDO INSTITUCIONAL

Misión, Visión Ventaja competitiva, Promesa de valor, Objetivos corporativos, Competencias corporativas. Ver enlace http://www.metrosalud.gov.co/metrosalud/institucional

Principios y valores corporativos. Ver enlace: http://www.metrosalud.gov.co/metrosalud/principios-y-valores

Organigrama institucional. Ver enlace:

http://www.metrosalud.gov.co/metrosalud/organigrama

Mapa de procesos. Ver enlace:

http://www.metrosalud.gov.co/metrosalud/estructura-de-procesos

Deberes y Derechos de los usuarios. Ver enlace

http://www.metrosalud.gov.co/usuarios/derechos-y-deberes

1. INTRODUCCIÓN

La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos.

Para la ESE Metrosalud es de vital importancia avanzar en el fortalecimiento de la seguridad de la información, que es un factor diferenciador y que da un valor agregado a la labor que se desarrolla en la prestación de servicios de salud.

Las políticas, directrices, lineamientos y mecanismos de control informático para el aseguramiento de la información hacen referencia a la protección de la Información Institucional almacenada en forma electrónica o digital, y valorada como activo de información institucional digital.

Es por ello que en el presente manual se recopilan los principales lineamientos para la administración y gestión de los recursos tecnológicos de la institución que intervienen en el manejo de los datos, personas, tecnología y demás aspectos relacionados con la administración de información producto del desarrollo de los procesos.

2. OBJETIVO:

Definir, adoptar y legitimar los lineamentos, directrices, controles y políticas de seguridad informática para proteger y salvaguardar la autenticidad, integridad, disponibilidad y confidencialidad de la información institucional de la E.S.E Metrosalud, brindando a los usuarios la orientación en el buen uso de los sistemas y servicios informáticos que apoyan la misión de la institución.

2.1 OBJETIVOS ESPECÍFICOS:

- Documentar los lineamientos específicos de la ESE Metrosalud en cuanto a la política de seguridad y el componente de seguridad del Modelo del Sistema de información
- Generar una cultura de seguridad de la información a través de la implementación de los lineamientos establecidos en el manual
- Proteger la información institucional de daño, pérdida, modificación accidental o intencional, describiendo el uso apropiado de los sistemas y servicios informáticos, así como de los activos de tecnologías de información y comunicaciones.

3. ALCANCE:

El presente manual es aplicable a todas las áreas de la ESE Metrosalud, unidades hospitalarias, Centros de salud y laboratorio, áreas administrativas.
Es de obligatorio cumplimiento para todo el personal que participa en cualquier de los procesos de la organización.

4. POLÍTICAS RELACIONADAS

PE02 MO 41 MODELO SISTEMA DE INFORMACIÓN

PE01 PO 57 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

PE01 PO 51 POLÍTICA DE GESTIÓN DOCUMENTAL

PE01 PO 56 POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES

PE01 PO 58 POLÍTICA DE GESTIÓN DE LA TECNOLOGÍA

5. DESARROLLO DEL MANUAL:

5.1 MARCO NORMATIVO

Que según los estándares internacionales NTC/IEC ISO 27001 y NTC/IEC ISO27002, debe existir una declaración formal por parte de Metrosalud en la definición, implementación, seguimiento, revisión, mantenimiento y mejora de los controles, lineamientos y directrices garantizando niveles apropiados de seguridad de la información que impidan su daño o destrucción accidental o intencional, y que es responsabilidad de los usuarios cumplir con estos controles con el fin de evitar que la información institucional sea expuesta a daño, modificación, robo o sea revelada a terceros.

Que se adoptan lineamientos de acuerdo con la ley 603 del 27 de Julio de 2000, Derechos de autor: "por la cual se modifica el artículo 47 de la ley 222 de1995", como también al decreto 3942 del 25 de octubre de 2010, por el cual se reglamenta el ejercicio de la gestión colectiva e individual del derecho de autor y los derechos conexos.

5.2 MARCO OPERATIVO

5.2.1 ACCESO AUTORIZADO

Los líderes de proceso y directores de unidades administrativas, establecen la necesidad del uso de la funcionalidad de los servicios y/o sistemas informáticos, autorizando a los funcionarios, servidoras y servidores públicos, contratistas y terceros que según la naturaleza de sus funciones o competencias, requieran tener acceso a la Información institucional a través de los servicios y/o sistemas informáticos de la entidad, informando oportunamente a la Dirección de Sistemas de información a través de la mesa de ayuda de sistemas.

Es obligación de todos los funcionarios, servidoras y servidores públicos, Contratistas y Terceros con acceso autorizado al uso de los servicios y/o sistemas informáticos, cumplir con todas las políticas y disposiciones de seguridad informática adoptadas por la entidad.

Los funcionarios, servidoras y servidores públicos, Contratistas y Terceros con acceso autorizado al uso de los servicios y/o sistemas informáticos, serán considerados usuarios de los sistemas, los cuales tienen la responsabilidad de actualizarse en temas relacionados con la Gestión de Seguridad de la Información adoptados y socializados a través de la gestión de la Dirección de Sistemas de información.

La Dirección de Sistemas de información establece los niveles de protección de la Información institucional digital, de acuerdo con su clasificación, roles y responsabilidades asignados a los usuarios del sistema, permitiendo el acceso a los servicios y/o sistemas informáticos través de la asignación de un identificador y contraseña inicial, previa autorización formal del jefe de área.

Para el trabaja en casa se cuenta con la publicación de la conexión al servidor de SAFIX por IP Publica igual mente conectado con el cliente de JAVA con una doble autenticación que comprueba que el usuario tiene los privilegios para realizar la conexión fuera de las instalaciones de Metrosalud.

Metrosalud cuenta en cada Centro de salud o Unidad hospitalaria con mínimo 1 Centros de datos estos se tienen como punto de concentración del cableado estructurado de red de datos, telefonía y proveedor de servicios de internet y conectividad. Estos centros de su seguridad y custodia de los dispositivos que se encuentran que, en cada uno, son responsables los directores y coordinadores. En SACATIN se cuenta con 5 centros de datos y un data center, todos son manejados desde sistemas de información.

Para los accesos a la red inalámbrica disponibles en SACATIN, San Cristobal y Belén se cuanta con acceso restringido solo para equipos de Metrosalud que pertenezcan al dominio y una serie de parámetros para que se puedan tener acceso a la red y navegación.

La E.S.E tiene implementado el sistema de acceso remoto para funcionarios autorizados y terceros a través de una VPN (Red privada virtual), la cual es validada por las políticas de

acceso implementadas en el firewall, lo que garantiza un nivel de seguridad contra acceso no autorizado desde el exterior.

Todo el intercambio de información desde la institución hacia redes externas o internet y viceversa son validadas por un conjunto de políticas firewall.

Los aplicativos del sistema de Safix de la E.S.E y módulos administrativos cuentan con un módulo de administración de privilegios los cuales delimitan la acción de los usuarios en los módulos del sistema. El perfil de los usuarios debe ser definido por los jefes de cada área y ser solicitados a sistemas para la creación y configuración de los usuarios.

Cuando los usuarios dejen sus puestos de trabajo deben cerrar la aplicación y la sesión de trabajo, para evitar accesos no autorizados a datos o recursos compartidos del sistema.

Los equipos de terceros que ingresan a la institución y deseen tener acceso a recursos como internet, deben solicitar al área de sistemas la configuración para acceso a la red, este acceso se direcciona por la VLAN 60 para separar su tráfico de los datos de nuestros equipos y servidores mediante un canal diferente.

Todos los equipos propiedad de la E.S.E como computadores de escritorio, equipos portátiles, impresoras y equipos relacionados con sistemas de información no deber retirarse de las instalaciones físicas por ninguna persona a menos que esté previamente autorizado por escrito bajo la responsabilidad del Jefe de la dirección de sistemas.

Los usuarios del sistema de información no pueden extraer información institucional para usos diferentes a los laborales.

Todos los equipos de la E.S.E cuentan con protección de antivirus la cual se actualizada en forma centralizada y automática. Si se detecta la presencia de un virus u otro agente potencialmente peligroso, se debe notificar inmediatamente al área de Sistemas. Los equipos de terceros que usan la red de datos de la E.S.E deben contar con un sistema de antivirus actualizado que será validado previamente por el área de sistemas.

Para prevenir demandas legales o la introducción de virus informáticos, se prohíbe estrictamente la instalación de software no autorizado, incluyendo el que haya sido adquirido por el propio usuario. Así mismo, no se permite el uso de software de distribución gratuita o shareware, a menos que haya sido previamente aprobado por el área de Sistemas.

Todo dispositivo de almacenamiento externo, memorias usb, cd, dvd, dd usb, disquete debe ser vacunado antes de abrir sus contenidos.

Ver Anexo 1. CREACION DE USUARIOS EN EL SISTEMA DE INFORMACION DE LA E.S.E METROSALUD

Ver anexo 12. SEGURIDAD WIFI

Ver anexo 13. MANUAL ACCESO SAFIX PÚBLICO

Ver anexo 14. CONTROL ACCESO CENTROS DE DATOS

5.2.2 PROTECCION DE LA INFORMACION DIGITAL.

Para salvaguardar la información institucional como activo de información institucional digital, la Dirección de Sistemas de información gestiona y dispone los recursos informáticos necesarios para su clasificación, valoración, custodia y respaldo.

Los usuarios de los sistemas y servicios informáticos deben ser conocedores de los riesgos asociados al uso de las nuevas tecnologías de información y comunicaciones, y son responsables de garantizar la protección de este activo.

En la actualidad la seguridad perimetral de toda la ESE Metrosalud la soporta la infraestructura de UNE contando con firewall Fortinet en HA (alta disponibilidad) con la capacidad necesaria para soportar los más de 2000 usuarios que diario usamos los servicios de red tanto internet como correo electrónico.

Todo el software de la E.S.E está protegido por derechos de autor y requiere licencia de uso. Por tal razón es ilegal y está terminantemente prohibido hacer copias o usar ese software para fines personales.

Todos los originales de instalación deben permanecer bajo seguridad de acceso físico, junto con las claves de instalación y actas de licencias en el área de sistemas y es responsabilidad del jefe del área velar por su correcto uso. Se debe realizar una copia de los medios de instalación y con ellos se realizará la instalación en los equipos, nunca con el original. Esta copia se encuentra en el área de sistemas y es material de trabajo de los auxiliares de sistemas.

Al terminar la jornada laboral, los escritorios y áreas de trabajo deberán quedar desprovistos de documentos sensibles que puedan comprometer los intereses de la organización. Estos deben quedar bajo llave en archivadores, cajas fuertes o demás medios de almacenamiento físico seguros.

Dado que cualquier tipo de desastre natural o accidental ocasionado por el hombre (cortos circuitos, vandalismo, fuego y otras amenazas etc.) podrá afectar el nivel de servicio y la imagen de la E.S.E, se debe prever que los equipos de procesamiento y comunicaciones se encuentren localizados en áreas aseguradas y debidamente protegidas contra inundaciones, robos, interferencias electromagnéticas, fuego, humo y demás amenazas que puedan interferir con el buen uso de los equipos y la continuidad del servicio.

El plan de Contingencia y de Recuperación debe permanecer documentado y actualizado de manera tal que sea de conocimiento general y fácilmente aplicable en el evento que se requiera permitiendo que los recursos previstos se encuentren disponibles y aseguren la continuidad de los procesos de la E.S.E en un tiempo razonable para cada caso, y contemplando como mínimo los riesgos más probables de ocurrencia que afecten su continuidad.

Anexo 2. CONFIGURACIÓN DE POLÍTICAS DE DIRECTORIO ACTIVO

Anexo 3. CONFIGURACIÓN DE ANTIVIRUS

Anexo 4. METODOLOGÍA BACKUP

Anexo 5. SISTEMA DE RESPALDO Y RECUPERACION

Anexo 11. SEGURIDAD PERIMETRAL TIGO UNE

5.2.3 DESARROLLOS DE PROYECTOS CON TECNOLOGÍA:

Todos los proyectos que involucren elementos y/o procesos de Tecnologías de la Información y las comunicaciones deben contemplar el componente de seguridad de la información y propiedad intelectual cuando aplique, de tal forma que se articule a los lineamientos de seguridad definidos en la Política de Seguridad de la información.

5.2.4 DESARROLLO DE APLICACIONES

La institución no cuenta con un área de desarrollo de aplicaciones, para las aplicaciones del ERP que lo requieren, se soporta un contrato para ajustar o modificar los aplicativos que requieran ser personalizados de acuerdo con las necesidades institucionales.

El proceso de gestión de la información en su procedimiento de estructuración y diseño de soluciones TIC contempla el análisis de las necesidades y requerimientos para formular el desarrollo necesario, es por eso que se definen tres ambientes:

- Desarrollo: Administrado por el proveedor del software (XENCO)
- Pruebas: Administrado por los analistas de la institución
- Producción: Administrado por el proveedor de servicios (infraestructura y DBA) UNE

El personal que desempeña este perfil en cada ambiente tiene las siguientes responsabilidades:

- Acceder directamente a las bases de datos o tablas necesarias bajo perfil de administrador.
- Tener privilegios de administrador sobre los ambientes de los aplicativos.
- Tener la posibilidad de instalar aplicaciones necesarias para los desarrollos, previo licenciamiento.
- Definir la ubicación de los archivos de código fuente para garantizar la realización Back Up de acuerdo con las políticas establecidas.

5.2.5 CONFIGURACIÓN DE APLICACIONES

El personal que desempeña este perfil tiene la función de realizar las configuraciones de fachada, preparación de insumos y administración de usuarios necesarios para el funcionamiento de los aplicativos. Para ello, debe:

a. Tener privilegios de administrador sobre los ambientes de producción de los aplicativos.
b. Realizar la administración de usuarios.
d. Mantener y documentar la conceptualización de las aplicaciones y publicación de datos.
e. Disponer de un ambiente de pruebas.

5.2.6 ADMINISTRADOR DE BASES DE DATOS

a administración de la base de datos del ERP está contratado con UNE, quien tiene las siguientes responsabilidades:

- Tener privilegios de administrador sobre los componentes de bases de datos.
- Tener privilegios de administrador sobre los ambientes de producción de los aplicativos.
- Garantizar la realización de back up sobre las bases de datos administradas.
- Mantener una bitácora con las solicitudes realizadas por las áreas a través de correo electrónico que soporten las operaciones realizadas sobre la base de datos.
- Administrar usuarios y protocolos de seguridad sobre las bases de datos.
- Las gestiones de los ambientes de base de datos se detallan en el anexo 10.

5.2.7 USO DE LA PLATAFORMA TECNOLÓGICA

Todos los activos de infraestructura tecnológica y de comunicaciones de la ESE Metrosalud hacen parte del inventario de la entidad. Los usuarios del sistema son responsables por el manejo que den a los activos que les sean asignados para el cumplimiento de su labor, procurando uso adecuado a fin de lograr y mantener los niveles adecuados de protección de los mismos.

Para la gestión de estos activos se cuenta con un catalogo de servicios de TI que tiene como fin proporcionar una fuente única de información sobre todos los servicios y plataforma tecnológica vigentes y acordados por la Dirección de Sistemas de Información, alineando los servicios basados en TI (Tecnologías de la Información) y para apoyo de las áreas estratégicas, misionales, evaluación y control de Metrosalud

El Catálogo recoge los servicios que la Dirección de Sistemas de Información presta a las demás dependencias y procesos de Metrosalud como soporte al desarrollo de sus actividades de negocio.

Ver anexo 15. CATALOGO DE SERVICIO DE TI

La Dirección de sistemas de información es responsable de la protección de los activos de información y comunicaciones, asignando por medio de su equipo de apoyo y proveedores, la administración de los sistemas y servicios informáticos que soportan la operación tecnológica de la entidad.

5.2.7.1 **Seguridad del Hardware**

Los computadores de la E.S.E son instalados por el área de sistemas de acuerdo a los requerimientos de las normas para cableado TIA/EIA 568B y en la parte eléctrica se siguen las recomendaciones del código eléctrico colombiano RETIE, garantizando un ambiente seguro, alejados de zonas de humedad y en ubicaciones que cuentan con las instalaciones eléctricas y de red datos adecuadas.

Los equipos de cómputo de la E.S.E son para el desarrollo de las actividades institucionales no para otros fines y es responsabilidad del jefe de área o coordinador de servicio velar por su correcto uso.

No puede modificarse la ubicación ni la configuración del hardware y software instalado en los equipos de cómputo por parte de los usuarios sin el acompañamiento del departamento de sistemas; se ha configurado en el directorio activo una serie de políticas que restringen a los usuarios la modificación de la configuración de los equipos.

Se realiza mantenimiento preventivo del 100% de los equipos de la E.S.E, de acuerdo al Cronograma de mantenimiento y limpieza de equipos de cómputo, garantizando un mantenimiento anual.

Cualquier falla en los computadores, impresoras o la red de datos debe reportarse inmediatamente al área de sistemas y no tratar de manipular los equipos, ya que podría causar problemas como pérdida de la información o daño del equipo,.. El área de sistemas registra la solicitud en el reporte de incidentes, clasifica la prioridad del evento y asigna un responsable para solucionarlo.

Todos los equipos de cómputo y equipos de comunicaciones deben estar ubicados en lugares asegurados para prevenir el robo. Para ello la E.S.E protege contra robo los equipos portátiles y algunos de escritorio que se encuentran en zonas expuesta mediante un sistema de guayas de seguridad con contraseña, Los demás equipos están ubicados en áreas con restricción de acceso físico a personal no autorizado y es responsabilidad del jefe de área velar por su seguridad.

Los equipos de cómputo y de red de la E.S.E se encuentran marcados y relacionados en un inventario detallando sus componentes principales como, marca, serial, garantía, ubicación, dirección IP y programas instalados. Los registros de inventario se mantienen actualizados, registrando las novedades de ingresos de equipos nuevos o bajos de inventario cuando se presentan.

La pérdida o robo de cualquier componente de hardware debe ser reportada inmediatamente al jefe del área, quien informa a la administración para iniciar la investigación respectiva y la afectación de pólizas para la reposición de equipos. El área de sistema evaluara la alternativa para dar continuidad a los requerimientos del área afectada.

5.2.7.2 ***USO DEL COMPUTADOR, PORTATIL y TABLETS*** (Dispositivos móviles inteligentes).

El procedimiento de control de inventario y bienes muebles, hace la entrega oficial del equipo de cómputo, La configuración y puesta a punto de acuerdo a los procesos en los cuales se va a utilizar, la realiza la Dirección de Sistemas de información.

Si el usuario es trasladado del Área con sus elementos tecnológicos, es responsabilidad de éste avisar de acuerdo con los procedimientos establecidos, al equipo de Bienes Muebles para realizar dicho movimiento y a Sistemas para realizar los ajustes.

Los computadores de la ESE Metrosalud, no podrán ser utilizados para visualizar almacenar material no permitido y/o obsceno.

Los usuarios son responsables de proteger sus contraseñas para poder ingresar a la red de la ESE Metrosalud. Ningún usuario puede acceder a la red con la contraseña o cuenta de otro usuario, en caso de infringir deberá someterse a lo dispuesto en la ley 1341 de 2009. El usuario debe bloquear su pantalla cada vez que abandone su puesto de trabajo.

La ESE Metrosalud, no será responsable por las transacciones financieras electrónicas que realicen los empleados desde el computador asignado o desde cualquier computador que esté disponible para uso público y se encuentre en las instalaciones de la ESE Metrosalud.

Ningún empleado o contratista de la ESE Metrosalud, o a quien le ha sido asignado un computador, podrá instalar software o hardware que no haya sido aprobado o adquirido por la entidad, solamente la mesa de ayuda o quién sea autorizado por la Dirección de Sistemas de Información, podrá realizar esta labor.

Ningún empleado de la ESE Metrosalud, contratista o personal que le haya sido asignado un computador de la Entidad, podrá adulterar el hardware o intentar desactivar el software de seguridad o de trabajo instalado en el computador, sin previa autorización de la Dirección de Sistemas de Información.

La ESE Metrosalud, permitirá, en cierto límite, el almacenamiento de información personal en los discos duros de los computadores asignados a cada empleado o contratista, sin embargo,

no será responsable de dicha información ni se ejecutarán esfuerzos tendientes a su recuperación.

Restricciones

Intentar o realizar accesos a cuentas de usuario que no sean las propias (utilizando cualquier protocolo o programa, telnet, ftp, etc.).

invadir la privacidad de los demás a través del computador asignado, así como intentar modificar o tener acceso a archivos, contraseñas o datos que pertenecen a otros.

Utilizar los computadores de la Entidad para Introducir virus computacionales, programas espías o cualquier otro programa diseñado para dañar el equipo o el software utilizado en la ESE Metrosalud, o de cualquier manera, arriesgar la seguridad de las computadoras o el sistema de red de la Entidad.

Exportar los archivos de contraseñas o realizar cualquier manipulación sobre los mismos, en concreto, intentar averiguar las contraseñas de los usuarios.

Afectar o paralizar algún servicio por la ejecución intento de ejecución de programas indebidos.

Modificar archivos que no sean propiedad del usuario, aunque se tengan permisos de escritura.

Acceder, analizar o exportar archivos que sean accesibles a todo el mundo pero que no sean del usuario, salvo que se encuentre en una ubicación que admita su uso público.

Cambiar la imagen institucional usada en los fondos de pantalla.

Impresión de documentos personales en los recursos de la Empresa.

Uso de los recursos tecnológicos de la empresa por familiares o amigos de los funcionarios, o por personal no autorizado.

Recomendaciones

No se debe comer o colocar líquidos cerca del computador (CPU, teclado), se pueden producir choques eléctricos y por ende el daño irreparable del mismo.

Siempre, al final de la jornada, se debe apagar el computador y el monitor.

Se debe apagar el monitor, cuando el usuario se retire de su puesto de trabajo, por periodos de tiempo superiores a una hora.

El usuario debe cambiar la contraseña regularmente o cuando considere que la misma pudo haber sido copiada.

Reportar inmediatamente las anomalías detectadas

Mantener depurado el correo institucional para evitar el riesgo de no recibir comunicación efectiva.

Consideraciones

Reparación y mantenimiento de equipos: Los usuarios deben saber que el personal técnico tiene la autoridad para acceder a archivos individuales o datos cada vez que deba realizar un mantenimiento, sin embargo, el personal técnico de la mesa de ayuda no puede exceder su autoridad en ninguna de estas eventualidades, para usar esta información con propósitos diferentes a los de mantenimiento o reparación.

Respuesta al uso indebido de computadores y sistemas de información: Cuando por alguna causa razonable determinada, se presuma el uso indebido de un computador o portátil, soportado en lo dispuesto en la ley 1341 de 2009, la Dirección de la Empresa puede acceder cualquier cuenta, datos, archivos, o servicio de información perteneciente a el(los) involucrado(s) en el incidente, para investigar y aplicar las sanciones a que hubiere lugar. Todos los empleados de la Dirección de Sistemas de Información y a quienes se designe, están en la obligación de monitorear constantemente los computadores y portátiles de la Entidad a través de los medios correspondientes, para responder oportunamente frente a cualquier acción que atente contra la disponibilidad, seguridad o desempeño correcto de los mismos.

5.2.7.3 ***SOPORTE Y MANTENIMIENTO DE LOS RECURSOS***.

El soporte y mantenimiento de los activos de TI que soportan los sistemas de información de la entidad, su funcionamiento, disponibilidad y actualización es responsabilidad de la dirección de sistemas de información

- El aseguramiento, guarda y custodia de la información misional y administrativa institucional almacenada en los sistemas informáticos es responsabilidad de Planeación y Sistemas.
- Sólo el personal autorizado (por quien) puede llevar a cabo cualquier tipo de mantenimiento tanto del hardware como del software y de la configuración de acceso a la red, teniendo en cuenta las políticas establecidas.
- La dirección de sistemas de información no se hará responsable de mantenimiento, soporte o licenciamiento de los equipos o software que no hacen parte del Inventario oficial de la entidad, y que sean utilizados dentro de las instalaciones.
- La dirección de sistemas de información dispondrá los recursos tecnológicos y humanos necesarios para el soporte y acompañamiento de los diferentes programas que en la ESE Metrosalud laboran.

- Sistemas de información debe gestionar los elementos necesarios para adelantar el plan de soporte y mantenimiento de los activos tecnológicos de la entidad.
- Los mantenimientos se realizan de acuerdo con lo contemplado en el ANEXO 8. MANTENIMIENTO DE EQUIPOS DE CÓMPUTO

5.2.7.4 ***USO DE CONTRASEÑAS***.

Es responsabilidad de Sistemas de información, efectuar la creación de Usuarios y la asignación de una contraseña que cumpla con niveles de seguridad previamente establecidos bajo el medio institucional vigente, con el fin autorizar y garantizar el acceso de los usuarios a los sistemas informáticos de acuerdo a perfiles, roles y responsabilidades previamente definidos.

- El usuario del sistema debe ser consciente que la contraseña es de uso personal e intransferible y es responsable por el manejo adecuado que dé a la misma, la cual no deberá ser revelada, divulgada o expuesta por ningún motivo, evitando exponer a los sistemas informáticos de abuso intencional o accidental, cualquier acción que sea llevada a cabo bajo esta circunstancia no exime al funcionario de la responsabilidad por algún tipo de daño, perdida, modificación, sustracción o eliminación de información sensible para la entidad.
- Contraseñas de acceso a aplicaciones misionales y de apoyo. La asignación de contraseñas para el acceso y uso de las aplicaciones estará a cargo de la dirección de Sistemas de información, previa autorización formal del jefe de área. El usuario del sistema con acceso a estas aplicaciones es responsable por los cambios que se generen bajo su autenticación.
- Las cuentas de usuario, funcionarios y contratistas, que se desvinculen de la entidad, o que se les terminen sus contratos de prestación de servicios, se desactivaran de inmediato. Previo un aviso formal del área encargada a mesa de ayuda.
- Es responsabilidad de los Directores, Coordinadores de las diferentes dependencias Centros de salud y Unidades hospitalarias informar oportunamente a Sistemas de información la creación, modificación y eliminación de las cuentas de usuarios, por la mesa de ayuda.

5.2.7.5 USO DE LA RED DE DATOS

La dirección de sistemas de información es responsable de suministrar y administrar la infraestructura de Datos y Comunicaciones necesaria para el cumplimiento de su gestión, y podrá a través de Sistemas realizar monitoreo y seguimiento de las comunicaciones electrónicas, hasta donde sea permitido por las disposiciones legales, procurando respetar la autonomía y privacidad del usuario.

El monitoreo, seguimiento y control efectuado sobre las comunicaciones, tiene como finalidad prevenir y detectar el uso no autorizado de la infraestructura de comunicaciones

con propósitos que incumplan los lineamientos, directrices, políticas dispuestas y cualquier otro documento o disposición legal vigente.

Los usuarios de los equipos de cómputo de la ESE Metrosalud son responsable de la información que en los equipos asignados guardan local, porque sistemas de información no se hace responsable de la pérdida o modificación que les ocurra.

Los usuarios de los equipos de cómputo de La ESE Metrosalud no deben por ningún motivo desarrollar, comprar, distribuir, instalar o ejecutar software malicioso que afecte el normal funcionamiento y/o cause cualquier tipo de daño a los activos de infraestructura tecnológica.

Los usuarios de la red de datos no deberán intentar acceder a la configuración de los activos de IT, o intentar acceder a información considerada confidencial que esta almacenada en bases de datos o cualquier otro medio digital.

En el evento en que un usuario requiera ingresar un equipo de cómputo ajeno a la entidad a la red de datos, debe solicitar a la dirección y Sistemas las credenciales de acceso previo concepto técnico de la viabilidad sobre el activo tecnológico.

La nomenclatura de la red de datos, se establece de acuerdo con lo contemplado en el Anexo 9 Arquitectura IP Metrosalud.

5.2.7.6 USO DE LA INFRAESTRUCTURA DE VOIP

Los usuarios de la plataforma de telefonía VoIP deben ser conscientes que esta es una herramienta de apoyo al cumplimiento de las labores asignadas y no debe ser destinada a uso personal, comercial o de otra naturaleza ajena a la función de la entidad.

La dirección de sistemas de información a través de la dirección general Corporativa, realizará la configuración, asignación y/o reasignación de extensiones telefónicas previa autorización formal del jefe de área.

5.2.7.7 USO DEL CORREO ELECTRÓNICO

Sistemas adoptará medidas de control sobre el uso del correo electrónico institucional con base en el documento institucional vigente.

Los usuarios del correo electrónico no deberán distribuir material que se pueda de alguna manera considerar como ofensivos, difamatorios o que contenga material pornográfico, sexista, racista o político.

Los usuarios del correo deben tener especial cuidado al momento de descargar archivos adjuntos que puedan contener software malicioso que pueda afectar la plataforma tecnológica de la entidad.

Los usuarios del correo electrónico institucional son responsables por el contenido de los mensajes enviados desde su cuenta, así como del intercambio de los mismos.

Sistemas, realizará la atención de requerimientos especiales como el envío de correos masivos, creación de carpetas personales o ampliación en el tamaño del buzón, previa autorización formal de los jefes de área.

No está permitido que los usuarios de correo electrónico usen la cuenta para el envío de correos masivo.

El aseguramiento, guarda y custodia de la información contenida en las carpetas personales es responsabilidad del usuario.

La configuración de las cuentas de correo se realiza de acuerdo con lo contemplado en el anexo 7.

5.2.7.8 ***USO DE INTERNET***

Sistemas, pondrá a disposición regular y supervisará el uso de Internet bloqueando el acceso a sitios web quesean considerados inapropiados o que contengan contenidos pornográficos, sexistas, racistas, difamatorios u ofensivos, a través de la implementación de los controles informáticos necesarios.

Sistemas, garantizará la navegación en internet sin restricciones en los casos en que los usuarios lo requieran previa autorización formal del jefe de área, a través del procedimiento institucional vigente.

Los usuarios de Internet no deben descargar, copiar, poseer y distribuir material de Internet salvo autorización expresa del Jefe Inmediato y Sistemas previa verificación de los derechos de autor y licenciamiento.

El acceso a redes sociales está restringido a excepción de los usuarios que por su actividad requieran este servicio, previa autorización del jefe inmediato.

Los usuarios de Internet, deben abstenerse de descargar, copiar, distribuir, reproducir software que esté protegido por derechos de propiedad intelectual.

En el anexo 6 se describe uso del servicio de Internet dentro de la ESE Metrosalud

5.2.7.9 INTRANET Y PAGINA WEB

Es responsabilidad de Sistemas mantener disponible el servicio de la Intranet, por otra parte, la Oficina de Comunicaciones se encarga de la administración de la intranet, garantizando la revisión y aprobación del material publicado en este servicio informático.

5.2.7.10 USO DE SOFTWARE

Los recursos informáticos están disponibles para fortalecer el flujo de información interna y externa y para lograr eficiencia operativa, por lo tanto, estos deberán ser utilizados en las actividades propias del cargo.

El usuario se obligará a respetar todos los derechos de la propiedad intelectual y a usar el software de forma diligente, correcta, lícita, y en particular, se comprometerá a abstenerse de:

Utilizar el software con fines contrarios a la ley y a lo establecido por la ESE Metrosalud.

Copiar, modificar, reproducir o utilizar el software propiedad de la ESE Metrosalud con fines de lucro.

La ESE Metrosalud se reserva el derecho de retirar las licencias de software, en cualquier momento, a aquellos usuarios que hagan uso indebido del software, o que incumplan total o parcialmente estos términos de uso.

Cualquier información o inquietud de los usuarios con relación a la copia o utilización de un software determinado, deberá solicitarse mediante oficio o a través de correo electrónico, enviado al líder de proyecto de soporte de la Dirección de Sistemas de Información

Asignación cuentas de usuario en los Software de la empresa.

La asignación de usuario y contraseña en los diferentes SW de la Empresa, es única e intransferible, todo lo que se haga con su usuario será responsabilidad del funcionario

Una vez asignada la cuenta y la contraseña, la asignación de los permisos a este usuario deberá ser solicitada a los líderes funcionales que se encargan de administrar las autorizaciones de ingreso a los diferentes módulos.

Cada usuario que haga uso de los diferentes SW de la Empresa, deberá tener definido un rol específico según su cargo y perfil profesional y/o funcional

Antes de asignar usuario y contraseña a los diferentes funcionarios de la empresa estos deben estar en la base de datos con la información personal requerida por la oficina de Talento Humano.

6 DEFINICIONES O CONCEPTOS:

Información institucional:
Corresponde a todo dato creado, procesado, adquirido, modificado, y/o almacenado en el desarrollo de los procesos de la institución y para la cual se adoptan directrices con el fin de garantizar su Integridad.

Información Confidencial:
Toda información institucional destinada al cumplimiento de los objetivos de la entidad de carácter reservada qué debe ser conocida únicamente al interior de la entidad con la debida autorización y limitación de uso a terceros, o cuya restricción a terceros se encuentre reglamentada según sentencia de la corte T – 729 de2002.

Información Pública:
Hace referencia a la información institucional destinada al cumplimiento de los objetivos de la entidad, y además reconstituye fuente de información y consulta de terceros.

Cuando la información se haya obtenido sin hacer uso de un servicio o sistema informático de la entidad, y cuyo origen sea el producto o resultado de un contrato, convenio u otra figura contractual, será considerada como activo de información Institucional, siempre que se encuentre en cualquier formato digital accesible.

Controles Informáticos:
Son métodos y mecanismos técnicos o tecnológicos para reducir el riesgo frente a la posible materialización de incidentes y eventos de seguridad informática con el fin de mantener niveles apropiados de Integridad, Confidencialidad, Autenticidad y Disponibilidad de los datos contenidos en los sistemas informáticos.

Evento informático:
Es la presencia identificada de un estado del sistema informático y/o servicio informático y/o de la infraestructura de comunicaciones, que indica un posible incumplimiento de la política de seguridad y/o una falla de controles informáticos, o una situación desconocida que impacte la seguridad de la información digital.

Usuario del sistema:
Funcionario, servidor público, contratista o tercero que hace uso autorizado de los recursos tecnológicos, sistemas y servicios informáticos de la entidad.

Alias:
Dirección de correo electrónico alternativa que dirige a una cuenta de usuario existente.

Password, contraseña o palabra clave:
Serie secreta de caracteres que permite a un usuario tener acceso a un archivo, computador o programa.

Perfil:
Es una colección de datos personales asociados a un determinado usuario. Un perfil se refiere por lo tanto a la representación explícita digital de una persona de identidad.

Rol:

Definición que da alcance al uso de las funcionalidades de los servicios y/o sistemas informáticos o software aplicativo y de gestión a los usuarios de sistema.

Sistema Informático:
Conjunto de partes que funcionan relacionándose entre sí con un objetivo preciso. Sus partes son: hardware, software y las personas que lo usan.

Servicio informático:
Es un sistema informático orientado a proveer acciones específicas asociadas al manejo automatizado de la información digital que satisfacen las necesidades de comunicación de los usuarios del sistema, dentro de estas están el acceso a Internet, Correo electrónico, Antivirus, Mesa de Ayuda, entre otras.

Delito Informático:
Alterar, dañar, borrar o utilizar datos electrónicos para ejecutar un esquema de fraude, engaño, extorsión u obtención de dinero, propiedades o datos, utilizando servicios de computadora sin autorización, interrumpiéndolos, asistiendo a otros en el acceso no autorizado a sistemas de cómputo o introduciendo contaminantes en un sistema informático o una red de comunicaciones.

Infraestructura Tecnológica:
Conjunto de dispositivos físicos y aplicaciones de software que se requieren para la operación de la Entidad, e implica un conjunto de servicios y elementos compuestos por Hardware, Software, bases de datos, telecomunicaciones, personas y procedimientos todos configurados para recolectar, manipular, almacenar y procesar datos para ser convertidos en información.

TIC -Tecnologías de Información y Comunicaciones:
Conjunto de servicios, redes, software y hardware que tienen como fin la mejora de la calidad de vida de las personas dentro de un entorno u organización, y que se integran a un sistema de información interconectado e integrado.

Activos de información institucional digital:
Son bienes intangibles de la entidad que se pueden catalogar como la información digital contenida en los sistemas informáticos de gestión, necesaria para la operación misional y administrativa de la entidad.

7 BIBLIOGRAFÍA / WEBGRAFÍA

Sistemas de Gestión la Seguridad de la Información, ISO 27001, 2013

8 DOCUMENTOS RELACIONADOS

PA04 GESTIÓN SISTEMA DE INFORMACIÓN

PE02 MO 41 MODELO SISTEMA DE INFORMACIÓN

PE01 PO 57 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

PA07 IS 73 IS TABLA DE CONTROL DE ACCESO A LA INFORMACIÓN DE METROSALUD

PE01 PL 14 PLAN ESTRATÉGICO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

PE01 PL 18 PLAN SEGURIDAD Y PRIVACIDAD INFORMACIÓN

PE01 PL 19 PLAN TRATAMIENTO RIESGOS SEGURIDAD Y PRIVACIDAD INFORMACIÓN

9 ANEXOS

Anexo 1. CREACION DE USUARIOS EN EL SISTEMA DE INFORMACION DE LA E.S.E METROSALUD

A continuación se detallan los aspectos a tener en cuenta ante las solicitudes de creación, modificación, o retiro de cuentas de usuario para acceder a las aplicaciones y uso de los recursos tecnológicos como archivos, directorios, aplicaciones, entre otros.

Estas actividades se realizan únicamente en los sistemas que se basen en contraseñas, la identificación y autenticación de los usuarios.

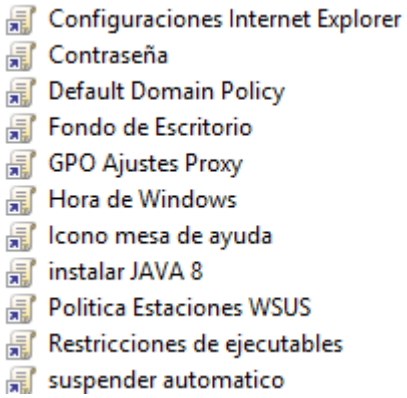
Nº	Actividad	Responsable
1	Se realiza la solicitud a la mesa de ayuda de la dirección de sistemas para la creación, modificación o retiro de los usuarios.	Director, coordinador y/o jefes de área
2	Se recibe la solicitud por el jefe o encargado únicamente, con el Requerimiento, creación de cuentas (Correo, Safix, Pandion, Almera, Sevenet), modificación, desactivación, bloqueo intencional y/o el retiro de usuarios de las aplicaciones.	Dirección de sistemas
3	De acuerdo con la solicitud se pueden realizar las siguientes actividades: Si la solicitud es para creación de usuarios nuevos realice las actividades 1, 2 y 3. 1. **Cuentas Safix**: Se verifica que el usuario no se encuentre en la base de datos. Se solicita Creación del tercero. El Ingreso del usuario se hace teniendo en cuenta Dependencia a la que pertenece y permisos de acceso y/o consulta. Se asocian los roles y/o formas según solicitud. (Ver cuadro anexo de roles y perfiles) Se asigna una clave temporal y una vez ingresado al aplicativo el usuario la debe cambiar. 2. **Cuentas Correo**: Se verifica que el usuario no se encuentre en la base de datos de la plataforma de correo. En el equipo del usuario, se configura la cuenta, claves. (Outlook) Se envían correos de prueba para verificar el correcto funcionamiento de la cuenta de correo electrónico. 3. **Cuentas Almera**: Recibida la información del usuario con nombre, cargo y dependencia, se realiza la creación de la cuenta. El técnico que crea la cuenta, notifica al área de planeación para terminar la definición de roles del usuario en el aplicativo.	Dirección de sistemas / mesa de Ayuda

	Se asigna una contraseña temporal y una vez ingresado al aplicativo el usuario la debe cambiar. 4. **Cuenta Sevenet**: Recibida la información del usuario con nombre, cargo y dependencia, se realiza la creación de la cuenta. Se asocian permisos. Se excluyen los derechos de acceso a hojas de vida y contratos. Estos solo se asignan con solicitud exclusiva del jefe de talento humano y dirección administrativa respectivamente. Se asigna una contraseña temporal y una vez ingresado al aplicativo el usuario la debe cambiar. Ir a la actividad 6.	
4	Si la solicitud tiene que ver con alguna modificación puede presentarse lo siguiente: 1. **Bloqueo intencional** Este bloqueo es solicitado por el jefe directo o encargado para suspender temporal los accesos a un sistema de información bien sea por novedades como vacaciones, licencias, incapacidades u otro trámite de suspensión a un usuario. 2. **Desbloqueo de cuentas** Solicitud para desbloquear claves de acceso a los sistemas de información internos cuando el usuario ha olvidado su clave o por intentos fallidos o expiración de la misma. Ir a la actividad 6.	Dirección de sistemas / mesa de Ayuda
5	Si la solicitud es para retiro de usuarios puede presentarse lo siguiente: 1. Desactivación y/o eliminación de cuentas de usuarios El correo electrónico se desactiva la cuenta y si es una cuenta de nivel general (Cartera, dirección de sistemas, autorizaciones, etc.) se asociara luego el nuevo usuario como un alias a la cuenta. Los usuarios de Pandion se desactivan. Para Safix se inactiva la cuenta ya que se debe conservar histórico y la integridad referencial impide la eliminación si tienen movimientos asociados. Los usuarios de Almera se inactivan y se realiza el traslado de tareas pendientes a quien corresponda	Dirección de sistemas / mesa de Ayuda

Anexo 2. CONFIGURACION DE DIRECTORIO ACTIVO

Directiva de grupo un conjunto de reglas que controlan el entorno de trabajo de cuentas de usuario y cuentas de equipo. Directiva de grupo proporciona la gestión centralizada y configuración de sistemas operativos, aplicaciones y configuración de los usuarios en un entorno de Active Directory. En otras palabras, la Directiva de Grupo, en parte, controla lo que los usuarios pueden y no pueden hacer en un sistema informático. Aunque la Directiva de Grupo es más frecuente en el uso de entornos empresariales y otros tipos de organizaciones. Directiva de grupo a menudo se utiliza para restringir ciertas acciones que pueden presentar riesgos de seguridad potenciales, por ejemplo: Bloquear el acceso al Administrador de tareas, restringir el acceso a determinadas carpetas, deshabilitar la descarga de archivos ejecutables, etc.

En La E.S.E Metrosalud se tienen unas GPO habilitadas como se muestra en la siguiente Imagen



Estas políticas con generales para todos los equipos y servidores dentro de la red y agregados al Directorio Activo (DA).

Y hay otras políticas habilitadas solo para estaciones de trabajo

Prioridad	GPO	Ubicación
1	Deshabilitar cuentas administradores loca...	METROSALUD
2	Default Domain Policy	metrosalud.local
3	Fondo de Escritorio	metrosalud.local
4	Restricciones de ejecutables	metrosalud.local
5	Icono mesa de ayuda	metrosalud.local
6	Contraseña	metrosalud.local
7	Hora de Windows	metrosalud.local
8	Politica Estaciones WSUS	metrosalud.local
9	Configuraciones Internet Explorer	metrosalud.local
10	GPO Ajustes Proxy	metrosalud.local
11	suspender automatico	metrosalud.local
12	instalar JAVA 8	metrosalud.local

Cada política de grupo (GPO) es tomada bajo los esquemas y necesidades de seguridad necesita Metrosalud para su operación.

Se describen las políticas más importantes que se aplican en las estaciones

Configuración de internet explorer: en esta política se parametriza la configuración de la conexión del internet explorer como Proxy predeterminado para navegación, borrado de temporales de internet al salir y exclusiones del proxy para navegación local.

Fondo de Escritorio: En esta política se configura para que todos los equipos de Metrosalud vinculados al DA. Tengan un único fondo del escritorio y se restringe el cambio del mismo esto con el fin de tener una imagen corporativa estandarizada y como medio de promoción de recordación de campañas institucionales.

Restricciones Ejecutables: Esta política no permite a los usuarios de los equipos que ejecuten aplicaciones no autorizadas por sistemas de información, para prevenir malware o software ilegal dentro de la organización que podría a su vez crear vulnerabilidades en la plataforma tecnológica.

Hora de Windows: Esta GPO nos sincroniza con la hora legal de Colombia y restringe el cambio de la hora por el usuario, garantizando un buen registro de log y hora y fecha precisa para el tema de análisis forenses y también garantiza la seguridad y buena ejecución de plataformas WEB con certificados como Bancos.

Política Estaciones WSUS: Esta GPO sirve para tener en la red de Metrosalud un solo repositorio de actualizaciones de seguridad de Windows, esto con el fin de no consumir el canal de internet por cada PC la realzar las actualizaciones por el fabricante de Microsoft. Estas Actualizaciones permiten que el PC no tenga falla o vulnerabilidades por el sistema Operativo.

Contraseña: Esta Política nos permite restringir las contraseñas que ponen los usuarios para que les exija niveles de complejidad como 8 caracteres mínimos y usar mayúsculas y números en la creación de las contraseñas para el ingreso a los equipos.

Las demás que se especifican son GPO para facilidades en la operación como poner iconos automáticos en el escritorio y que el pc no se suspenda esta última fue creada para que los pc no se apaguen y siempre esté disponible para el uso desde casa.

ANEXO 3. CONFIGURACIÓN ANTI VIRUS

Kaspersky Anti-Virus for Windows Workstations version 6.0.4.x

A continuación se explica cada uno de los módulos de este antivirus.

Antivirus de archivos

Es el componente más importante de ***Kaspersky Anti-Virus*** que proporciona la protección de archivos frente a la infección con virus, troyanos, y otros programas maliciosos.

El Antivirus de archivos intercepta todas las operaciones con archivos (abrir, iniciar, guardar), y analiza todos los archivos accedidos en busca de código malicioso.

El método principal usado por ***Kaspersky Anti-Virus*** para la detección de archivos infectados es el análisis de firmas que permite detectar los virus conocidos por las peculiaridades de su código de programa (firmas). Por éste motivo, el software antivirus requiere que las bases de firmas sean actualizadas regularmente para funcionar correctamente.

Adicionalmente puede usar el análisis heurístico que analiza la actividad de objetos en el sistema. Por defecto, el análisis heurístico está desactivado porque el método heurístico consume muchos recursos.

Antes de desinfectar o eliminar un objeto, el **Antivirus de archivos** guarda una copia de él en la carpeta de respaldo. Ésta función permite restaurar los objetos eliminados o desinfectarlos cuando sea posible.

Este módulo siempre se encuentra activo es uno de los más importantes del software. El antivirus siempre debe estar actualizado. En algunos casos no puede ser posible su actualización ya que se pueden presentar problemas en la consola de antivirus o problemas de red.

Antivirus del correo

El **Antivirus del correo** sirve para detectar y desinfectar los virus que se propagan a través de correo electrónico. **Antivirus del correo** analiza los mensajes y los archivos adjuntos del correo electrónico antes de la descarga y desinfecta o elimina los objetos infectados. El análisis de los mensajes de correo electrónico se efectúa de dos formas:

- Análisis de los mensajes de correo electrónico a través de los protocolos POP3, SMTP, IMAP, MAPI, NNTP, y por conexiones seguras (SSL) a través de los protocolos POP3 e IMAP;
- Usando los plugins para los clientes de correo Microsoft Office Outlook y The Bat!.

Cuando trabaja con los programas de correo Outlook Express (Windows Mail), Mozilla Thunderbird, Eudora, Incredimail, ***Kaspersky Anti-Virus*** analiza el correo a través del tráfico de los protocolos POP3, SMTP, IMAP y NNTP.

Para reducir al mínimo la posibilidad de que el usuario reciba un archivo adjunto infectado, por defecto se usan el análisis de firmas y el análisis heurístico y se analizan todos los archivos incluso los comprimidos.

El **Antivirus del correo** también analiza los archivos y enlaces enviados por las mensajerías instantáneas ICQ y MSN.

Antivirus Internet

Analiza todos los objetos que el usuario descarga a través del protocolo HTTP y proporciona una protección frente a la infección por virus o troyanos durante la navegación en Internet.

El Antivirus Internet analiza todos los objetos de descarga usando el análisis de firmas y el análisis heurístico para detectar los virus, verifica las direcciones de los sitios Web abiertos, y pide al usuario una confirmación para abrir el sitio si está en la lista de amenazas potenciales.

Este módulo no se activa ya que el antivirus da por sospechoso la entrada del aplicativo safix al sistema bloqueando el acceso y por ende generando problemas.

La Protección Proactiva

Permite detectar nuevos programas maliciosos antes de que produzcan algún daño.

El componente **Protección Proactiva** analiza la actividad de las aplicaciones y pide al usuario una confirmación para la ejecución de las acciones potencialmente peligrosas. Las acciones potencialmente peligrosas son: autoduplicación, procesos, controladores o ficheros ocultos, intentos de modificar el núcleo del sistema operativo, y otras. El usuario puede desactivar las acciones a ciertos tipos de eventos o el análisis de actividad de ciertas aplicaciones.

Este módulo no se activa ya que constantemente genera alertas al funcionario sobre programas peligrosos. En la consola de antivirus se crearon políticas de seguridad para dar fiabilidad a los programas más usados.

Anti-Spy

Intercepta y bloquea los programas de tipo adware (banners, pop-ups) y dialers.

No se activa este módulo ya que el aplicativo safix no puede funcionar de forma correcta.

Anti-Hacker

Realiza un filtrado de toda la actividad de la red del equipo de usuario. Intercepta todos los paquetes de la red y permite o bloquea su transmisión según las reglas de filtrado configuradas.

El control de las conexiones de la red le permite al usuario vigilar la actividad de la red del sistema y de las aplicaciones. Hay muchas aplicaciones que intentan acceder a Internet para

descargar actualizaciones, verificar la licencia, registrarse, etc… sin informar de una forma clara al usuario sobre esta actividad. **Anti-Hacker** permite bloquear tal actividad si el usuario la considera indeseada.

En este módulo se desactiva el bloqueo de equipo atacante y el firewall ya que nosotros como soporte no deja ingresar a los pc.

Anti-Spam

Éste componente sirve para detectar y filtrar el spam de forma automática.

Anti-Spam intercepta los mensajes de correo electrónico entrantes y aplica una serie de criterios para definir su estatus. Hay dos formas de verificar el correo en la etapa de recepción:

- Interceptando el tráfico POP3. En éste caso hay que configurar las reglas del filtro de mensajes en el cliente de correo. El filtrado se realiza por el texto introducido por **Anti-Spam** a la cabecera de mensajes;
- A través de plug-ins en los clientes de correo Microsoft Office Outlook, Outlook Express (Windows Mail), The Bat! En éste caso, las reglas de clasificación de mensajes se configuran en el plug-in del cliente de correo. Todos los mensajes que contienen spam reciben una cabecera especial. Es también posible configurar **Anti-Spam** para procesar el spam (eliminar, mover a una carpeta especial, etc. de forma automática).

Anti-Spam analiza el tráfico a través de POP3/SMTP/NNTP/IMAP.

Anti-Spam implementa varias tecnologías para detectar spam: análisis de frases usando una base de datos actualizable, análisis de cabeceras de mensajes, reconocimiento de imágenes, algoritmo de análisis de texto con autoaprendizaje.

Control de Acceso

Limita el acceso a dispositivos externos (dispositivos de USB, Firewire, Bluetooth, etc.) a las aplicaciones.

Conector al Agente de Administración del Administration Kit

Mantiene comunicación entre el ***Kaspersky Anti-Virus*** y el ***Agente de Administración*** instalados en el mismo equipo.

El **Conector** no está en el interfaz de la aplicación y no requiere ninguna configuración.

La gestión (instalar/eliminar) del componente **Conector** se efectúa a través de la opción de instalación **Personalizar** en el Asistente de instalación que permite seleccionar si el conector es instalado.

Para verificar si el **Conector** está instalado, vea si la carpeta de instalación del Kaspersky anti-virus contiene un archivo **avpcon.dll**.

Es necesario instalar el **Conector** si desea controlar la aplicación a través de ***Administration Kit***.

Existe una consola principal de antivirus encargada de controlar las actividades de virus, instalación de paquetes, creación de políticas para el antivirus y por último llaves de licencias. Esta consola se encuentra ubicada en un data center de la firma UNE.

ANEXO 4. METODOLOGIA BACKUP

Sistemas, Servicio y Aplicaciones que son Respaldados

En primera instancia se hace conocer que Metrosalud tiene en un servicio de HOSTING con la firma UNE, el cual aloja el sistema de información más importante para la empresa, el cual contempla la infraestructura necesaria que garantice la operación de la atención de los usuario en los puntos de servicios.

Esta infraestructura contratada con UNE contempla los mecanismos de respaldo al ab base de datos, así como una alternativa de una Base de Datos en Stanby, la cual permite recuperase de una forma más rápida ante la eventualidad de un daño o perdida de información de la base de datos.

Igualmente para los sistemas, servicio y/o aplicaciones que corren en el ambiente virtualizado del edificio Sacatín, también se les dirige las acciones de para respaldo de información en el edificio Sacatín de Metrosalud, siendo los siguientes:

- Remoto
- VCENTER
- OMNI
- IIS - ALPHASIG
- OCS
- SEVENET
- Mesa de Ayuda
- Mensajería
- Wireless Controller
- Correo electrónico
- WEB - HL7
- Antivirus
- DA Primario
- DA Secundario
- DELL Enterprise
- SQL
- Pandion
- Termlite (Sistema SX)
- Eventos Adversos
- WSUS
- Página WEB e Intranet
- Eventos Adversos
- OTRS
- Interaxion

- Netsight
- Cubos BI
- FTP Facturación electrónica
- File Server

Se tiene un sistema de File Server que nos permite tener en el área administrativa Sacatin unas carpetas personales y otras grupales con permisos específicos para cada usuario de lectura y ejecución o lectura y escritura. Cada carpeta está limitada por 10 Gb y por política no se permite contener dentro de ella ningún archivo multimedia. Se cuenta con un backup diario de estos archivos y un backup cada 10 minutos por medio de Windows backup.

Con el directorio activo tenemos implementado varias políticas de grupo

Políticas

- Tiene grupos de navegación
  - WF_General
  - Wf_VIP
  - WF_Sistemas
  - Invitados
- Solo existirá un usuario administrador de directorio activo
- El usuario administrador solo se puede loguear en el servidor de dominio.
- Se crea un perfil para usuarios TECNICOS plenamente identificados, con permiso:
  - Cambiar clave
  - Crear Usuarios
  - Gestión de Grupo
  - Instalar software
  - Cambio de configuración de la maquina
- El usuario administrador e invitado de la maquina estará desactivado en cada computador
- El escritorio tendrá una sola imagen institucional y la administrara el área de comunicaciones
- El usuario no puede ingresar a panel de control / Reg Windows
- El navegador ingresa por defecto a la intranet y no permite cambiar el proxy ni la página de inicio.
- Ningún usuario podrá tener permiso de administrador local ni del dominio excepto los técnicos de sistemas
- Los computadores deben tener un nombre basado en el formato sede M centro de costos W/P (computador o portátil) consecutivo tres números (ultimo octeto dirección IP)

Anexo 5. SISTEMA DE RESPALDO Y RECUPERACIÓN

En la E.S.E METROSALUD se ha adoptado el sistema de backup (Abuelo, Padre e Hijo) para hacer copias de seguridad. Este método es más eficiente ya que la mayoría de los aplicativos se mantienen en constante modificación.

Para hacer las copias de seguridad se cuenta con un software llamado Veeam backUp y Replication. Este software maneja diversos esquemas de copias de seguridad por ejemplo.

Pasos Para Realizar Las Copias De Seguridad

El sistema de backup (Veeam backUp y Replication) está programado para realizar las copias de seguridad a las 8 PM diariamente ya que a esta hora no afecta el trabajo de los funcionarios.

Al siguiente día se verifica que la tarea del backup se haya cumplido con éxito. Como se resume a continuación:

Se tienen 6 tareas de backup

- Backup Windows Diarios: esta actividad recoge todos los servidores en Windows y realiza una copia de Backup full a la semana y los demás incrementales.
- Backup Linux Diarios: Esta recoge todos los servidores Linux realiza una copia de Backup full a la semana y los demás incrementales.
- Backup Window Mensuales: Realiza en los 5 primeros días del mes un backup full y guarda 5 meses atrás
- Backup Linux mensuales: Realiza en los 5 primeros días del mes un backup incremental dentro de un Full y guarda 15 incrementales y un full.
- Backup Windows Anual: Guarda por un año el primer día del año 1 backup full.
- Backup Linux Anual: Guarda por un año el primer día del año 1 backup full.

Pasos para recuperar la información

En el aplicativo Veeam backUp y Replication se ingresa a la opción restore. Se verifica el punto de restauración más reciente y se procede a restaurar.

Por seguridad se hacen pruebas periódicas de restauración de servidores aleatorios.

Si al momento de restaurar una copia de seguridad el punto de restauración no funciona estos de eliminan y se programa otra tarea y se crea un punto de restauración nuevo.

Pruebas De Backup

- Una vez al mes se selecciona aleatoriamente una de las copias y se realiza prueba de restauración.
- Se valida la consistencia de los datos
- Se registra el resultado de la prueba, detallando la copia, el aplicativo, el resultado, fecha y hora de la restauración.

CONCEPTOS TÉCNICOS RELACIONAS CON RESPALDOS

Discos Duros

Con el paso de los años, los discos duros se han ido haciendo cada vez más grandes, dándonos la posibilidad de almacenar una gran cantidad de datos. Sin embargo, con el incremento de los volúmenes de información que se manejan, también han surgido nuevos problemas. Uno de ellos es la posibilidad de perder el contenido que tenemos debido a algún fallo. Por eso se mitiga el riesgo con los arreglos de los discos.

Aunque también tenemos que decir que esos inconvenientes han sido solventados con diversos tipos de utilidades y programas. Además, continuamente se siguen investigando nuevas formas y tecnologías para que no tengamos pérdidas de información.

Básicamente, la forma de hacer una copia de seguridad de nuestros discos duros es copiar la información a otra ubicación, o a un sitio en el que sepamos que tendremos disponibles esos datos, en el caso de que falle la herramienta original. Podríamos decir que la copia será un respaldo que utilizamos en el caso de que la información original resulte dañada o tenga algún problema.

San

Una SAN (Storage Area Network - Red de área de almacenamiento) es una red de almacenamiento integral. Se trata de una arquitectura completa que agrupa los siguientes elementos:

- Una red de alta velocidad de canal de fibra o SCSI
- Un equipo de interconexión dedicado (conmutadores, puentes, etc.)

- Elementos de almacenamiento de red (discos duros)

La SAN de Metrosalud en la que alberga todas las máquinas virtuales que contienen los sistemas, servicio y/o aplicaciones Alojadas en el la red del edifico Sacatin, red que se conecta con las de más redes de las sedes de Metrosalud.

La capacidad de una SAN se puede extender de manera casi ilimitada y puede alcanzar cientos y hasta miles de terabytes. Una SAN permite compartir datos entre varios equipos de la red sin afectar el rendimiento porque el tráfico de SAN está totalmente separado del tráfico de usuario. Son los servidores de aplicaciones que funcionan como una interfaz entre la red de datos (generalmente un canal de fibra) y la red de usuario (por lo general Ethernet).

Por otra parte, una SAN es mucho más costosa que una NAS ya que la primera es una arquitectura completa que utiliza una tecnología que todavía es muy cara.

Nas

El almacenamiento conectado en red, Network Attached Storage (NAS), es el nombre dado a una tecnología de almacenamiento dedicada a compartir la capacidad de almacenamiento a los respaldos del ambiente virtualizado de Metrosalud, los cuales se acceden con los protocolos CIFS, NFS, FTP o TFTP.

Los protocolos de comunicaciones NAS están basados en archivos, por lo que están orientados a manipular una gran cantidad de pequeños archivos. Los protocolos usados son protocolos de compartición de archivos como Network File System (NFS) o Microsoft Common Internet File System (CIFS).

Muchos sistemas NAS cuentan con uno o más dispositivos de almacenamiento para incrementar su capacidad total. Frecuentemente, estos dispositivos están dispuestos en RAID (Redundant Arrays of Independent Disks) o contenedores de almacenamiento redundante.

BUENAS PRÁCTICAS

Metrosalud ha iniciado a observar la seguridad de la información considerando la norma 2700 dentro de los estándares ISO/IEC (International Organization for Standarization / International Electrotechnical Commision).

Dentro de la serie 2700, se encuentra la norma ISO 27002, anteriormente denominada ISO17799 que refleja la guía de buenas prácticas y describe los objetivos de control y controles

recomendables en cuanto a seguridad de la información (con 11 dominios y 133 controles) y en su sección 10.5, aborda la cuestión de las copias de seguridad.

MODELOS DE COPIAS DE SEGURIDAD

Desde los primeros años de uso de copias de seguridad, se han desarrollado nuevas tecnologías que han intentado minimizar en la medida de lo posible el tamaño de los datos almacenados, el tiempo de copia y el tiempo de restauración de los mismos. Fruto de estas investigaciones son los cuatro modelos básicos que hoy día se utilizan en los procesos de generación de copias de seguridad:

- Copia total o completa (full backup).
- Copia diferencial.
- Copia incremental.
- Copia espejo.

La decisión de cuál de los métodos anteriormente citados se ha de utilizar cambia con las circunstancias particulares de cada situación y en la mayoría de los casos depende fundamentalmente de cuatro factores:

- La capacidad de los soportes sobre los que se va a gravar la información.
- El período de tiempo disponible para hacer la copia.
- El medio en el que se desarrolla el trabajo (local, intranet, internet, etc.).
- El nivel de urgencia a la hora de necesitar restaurar los datos.

Independientemente de los factores que determinen el tipo de copia a realizar, en la práctica, una buena política de gestión de copias de seguridad incluirá la conjunción de varios de los modelos expuestos. Una buena política de cooperación entre modelos de copias de seguridad garantizará un buen resultado final y la obtención de un respaldo de datos fiable, robusto y rápido.

Copia Total o Completa

Es el tipo básico e ideal de copia de seguridad ya que es el más exhaustivo y autónomo, y en el que se basan el resto de modalidades.

Una copia total incluye todos y cada uno de los archivos seleccionados para ser incluidos en la tarea programada de copia, sin importar si han sufrido cambio o no desde la última vez

que se realizó la anterior. Usualmente se genera un único archivo que se comprime con contraseña para ahorrar espacio de almacenamiento y aumentar la seguridad.

La copia total adolece de un inconveniente manifiesto; si la misma está programada para realizarse cada poco tiempo y no ha habido muchos cambios en los archivos a copiar, al realizarse una copia íntegra de todos los archivos de nuevo, en muchos de los casos las copias serán redundantes existiendo pocas diferencias entre ellas, lo cual supone un desperdicio de tiempo y espacio. Para solucionar este problema lo más adecuado consiste en programar copias totales, por ejemplo, semanales, en conjunción con copias incrementales (de las que más tarde se hablará) entre las anteriores.

La principal ventaja que ofrece este tipo de copias de seguridad reside en que el más rápido y seguro (en ámbitos donde el volumen de datos lo permite es, sin duda, la elección más aconsejable a la hora de decidir la política de copias de seguridad a seguir) si es necesario realizar una restauración total de los archivos copiados; como contrapartida es el que más recursos y tiempo de copia consume, por lo que hay que tenerlo en cuenta a la hora de programarlas.

Un aspecto importante que se debe tener en cuenta al decidirse por este tipo de copias es el de la confidencialidad y la seguridad. Como ya se ha comentado anteriormente, el modo de copia completa implica que se copiarán la totalidad de los archivos seleccionados, lo que implica que si se produce algún tipo de acceso no autorizado a la misma o incluso un robo, el intruso dispondrá de toda la información.

Por lo tanto se deberá salvaguardar tanto la integridad física de las copias como su nivel de consulta por parte de personal no autorizado, estableciendo las medidas de seguridad adecuadas en cada caso.

Copia Diferencial

Normalmente las aplicaciones de copias de seguridad mantienen un registro del día y hora en el que se realizan las copia. La fecha de modificación o creación de archivos es comparada con la marca de la última copia de seguridad y dependiendo de la modalidad de copia actúa en consecuencia.

La copia diferencial contiene todos los archivos que han cambiado desde la última copia completa. Las copias diferenciales son acumulativas entre sí, es decir, si se tienen

programadas varias copias diferenciales entre copias totales, cada una de ellas no tendrá en cuenta la anterior e irá acumulando los cambios desde la última total

Las copias diferenciales tienen la ventaja de que su tiempo de restauración es menor que el de otros modelos; al restaurar los archivos únicamente hace falta restaurar la última copia total y la última diferencial. Como contrapartida el espacio de almacenamiento que se utiliza es mayor que el de otros tipos, como por ejemplo el diferencial, ya que cada copia contiene los nuevos archivos modificados o creados más la totalidad de la última diferencial, si no es la primera, incrementando progresivamente el espacio utilizado para su almacenamiento.

El tiempo de creación de la copia dependerá, como en todos los casos, del volumen de datos modificados o creados. Comparativamente es mayor que el de las copias incrementales y mayor que el de las totales.

Como ya se ha comentado anteriormente, la modalidad de copia diferencial normalmente se utiliza en conjunción con las totales. Una configuración estándar de copias de seguridad comprende la programación de una copia total a la semana junto con copias diferenciales (o incrementales, de las que se hablará seguidamente) diarias hasta la siguiente total.

Copia Incremental

Las copias de tipo incremental contienen únicamente los archivos que fueron modificados o creados desde la última copia total, o incremental. La diferencia fundamental respecto a las copias diferenciales, es que no son redundantes (la información no se repite de una copia a la siguiente).

La siguiente imagen muestra el funcionamiento de la modalidad de copia incremental.

La principal ventaja de este tipo de copias es, por regla general, su menor tiempo de creación. Al copiarse únicamente los archivos modificados o creados desde la última copia diferencial, el volumen de datos es manejable y requiere menor espacio de almacenamiento, posibilitando reducir el periodo de tiempo programado entre copia y copia.

Como contrapartida, el tiempo de restauración es mayor, ya que en el caso de un volcado total de archivos, se deberá restaurar en primer lugar la última copia total y cada una de las copias incrementales existentes hasta la fecha. Por otro lado, si la necesidad de restauración

consiste en determinados archivos dispersos, se necesitará buscarlos, hasta encontrarlos, en todos los archivos de copia.

Copia Espejo (Mirror Backup)

Una copia espejo es básicamente una copia total a la que no se le ha aplicado ningún tipo de compresión. Algunos autores mantienen que este tipo de copia de seguridad en realidad no responde a las características propias de funciones de respaldo de datos, sino que se trata más bien de un mero proceso de "copiar y pegar".

Las copias en espejo están especialmente recomendadas en sistemas de datos que ya se encuentran comprimidos de por sí: archivos de música en mp3 o wma, imágenes en jpg o png, vídeos en divx o mov o archivos de instalación ya comprimidos.

Tienen principalmente dos ventajas frente al resto de modelos: son las más rápidas trabajando con archivos comprimidos y al no estar la información contenida en un solo archivo, el riesgo de perder datos producido por corrupción de archivos se minimiza, ya que de producirse sólo afectaría al archivo, o archivos, en cuestión y no a la totalidad de la copia.

Su inconveniente manifiesto es, generalmente, que al no encontrarse comprimida, el volumen de espacio necesitado es mayor que una copia de los mismos datos comprimida.

QUÉ DATOS COPIAR

La primera tarea a realizar en el momento de planificar una buena política de copias de seguridad, consiste en la identificación de una manera exhaustiva de todos aquellos datos que deben ser respaldados.

Una regla básica al respecto determina que se deberían respaldar todos aquellos datos que se necesitarían para efectuar la total recuperación de los sistemas, o que fueran necesarios en orden a consideraciones legales o financieras.

La identificación de dichos datos no es una tarea sencilla. Desde el punto de vista de la ingeniería del software requiere un profundo conocimiento del entorno de trabajo de la

organización para la que se diseñará la política de copias de seguridad, y tal fin no se conseguirá, sino la consecución de tres pasos secuenciales:

- Recopilación de la información: en este primer paso se recabará toda la información necesaria del entorno de trabajo objeto de las futuras copias de seguridad.
- Realización de inventario: en el que se aunará la información anteriormente conseguida y los medios físicos de los que se dispone.
- Decisión sobre los datos a respaldar: finalmente teniendo en cuenta los pasos anteriores se procederá a decidir qué datos respaldar.

La recopilación de información se puede realizar mediante tres vías: entrevistas con usuarios del sistema, conocimiento del software utilizado y observación sobre el terreno. La conjunción de la información obtenida por cada una de ellas ofrecerá una visión de conjunto necesaria para la toma de decisiones finales.

Mediante entrevistas con los usuarios del sistema, y utilizando técnicas propias de la ingeniería del software, será necesario identificar qué tareas realizan en su habitual modo de trabajo. Dicha información permitirá conocer qué tipo de software utilizan normalmente y cómo hacen uso del mismo, posibilitando la identificación del tipo de datos que usualmente manejan.

Así mismo es importante conocer cuál es la política que ha establecido la organización en cuanto a almacenamiento de datos por parte de los usuarios. En este sentido se pueden dar, principalmente dos tipos de situaciones:

- Los usuarios no pueden almacenar ningún tipo de dato en sus equipos, ya sean computadores portátiles o personales. Toda la información generada por el usuario es mandada a un servidor central, bien en tiempo real o asincrónicamente.
- Los usuarios pueden almacenar en sus equipos aquella información que consideren necesaria en el desarrollo de su trabajo. En este supuesto se pueden dar a su vez dos casos; que el usuario no mande ningún tipo de información al servidor o que envíe aquella que considera oportuno.

Otro aspecto a tener en cuenta es qué tipo de software es utilizado habitualmente en la organización por parte de los usuarios. Se ha de saber qué tratamiento de datos realiza cada una de las aplicaciones utilizadas. Toda información relativa a qué tipo de datos genera,

dónde los almacena o en que formato es fundamental a la hora de diseñar una planificación del respaldo de dichos datos.

En el caso de tratarse de software de código abierto o privado pero de pública distribución, dicha información se puede obtener de manera relativamente fácil, ya que normalmente se encuentra publicada y accesible a través de distintos medios (internet, libros, manuales).

Si por el contrario se trata de software específico para el tipo de actividad desarrollado por la organización, se deberá acudir a las especificaciones del mismo, o en su defecto, a la comunicación directa con la empresa desarrolladora del mismo a fin de que dicha información sea suministrada.

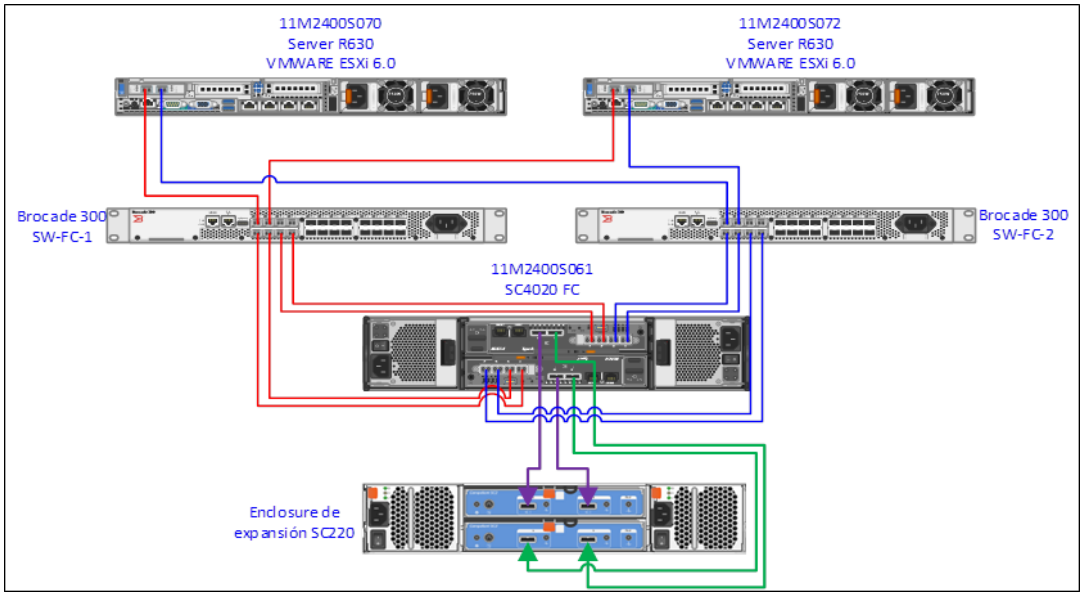
El último paso necesario en la labor de obtención de información consiste en la observación sobre el terreno. Es buena práctica acudir al puesto de trabajo de los usuarios y observar cómo realizan su tarea, ya que por un lado se podrá confirmar la información obtenida mediante las entrevistas realizadas y por otro se podrá detectar determinados hábitos de los usuarios de los cuales, bien por error o por omisión, no han informado.

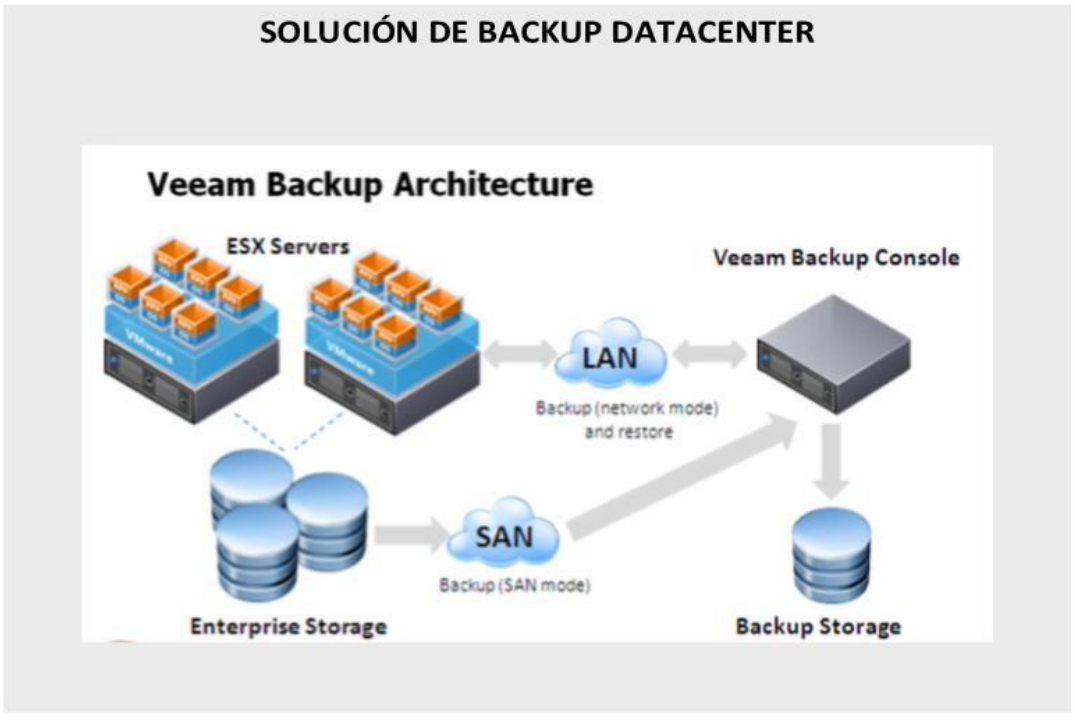
ANEXO 4.1: Resumen de respaldo a sistemas, servicios y/o aplicaciones

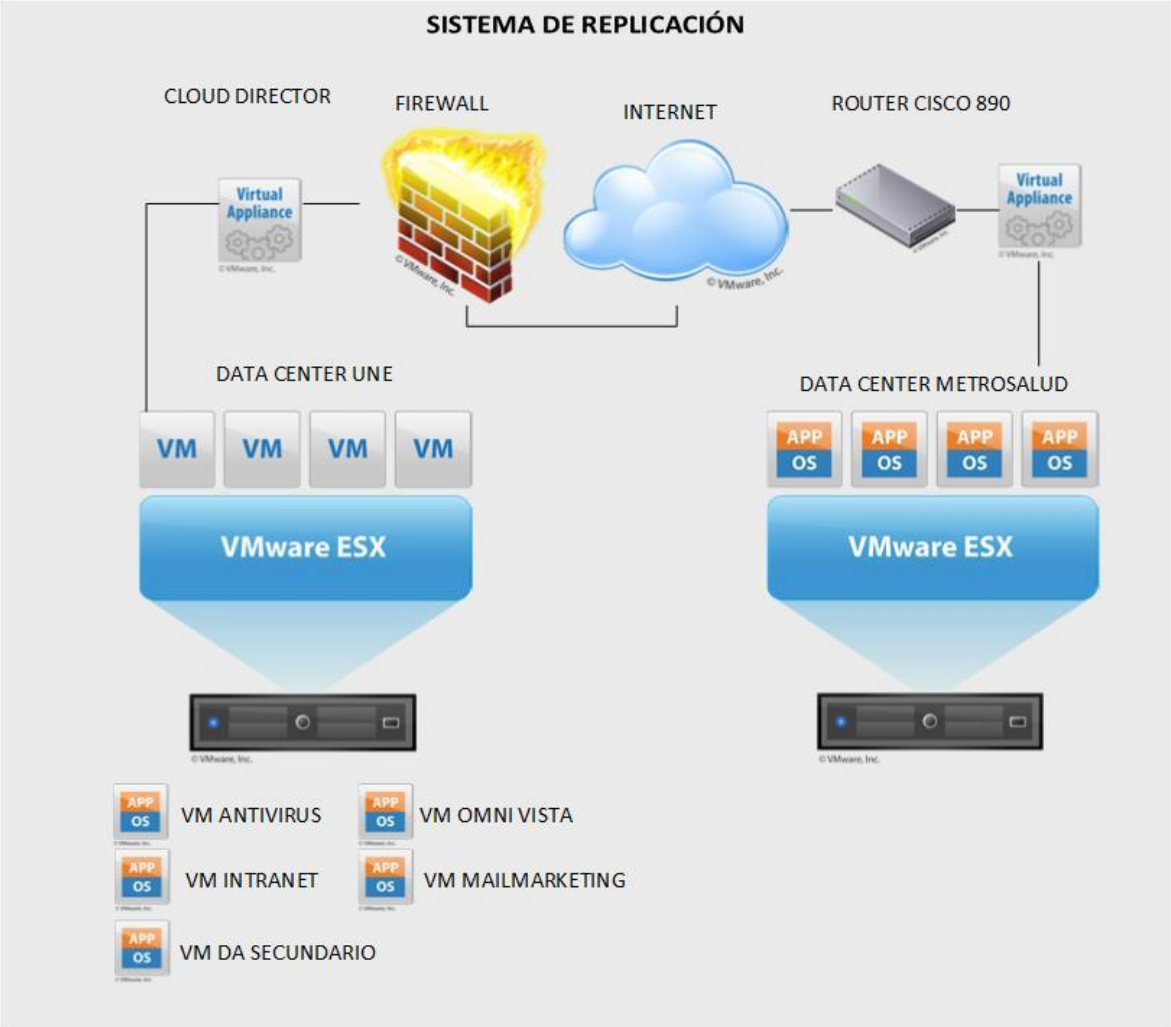
Direccion IP	Nombre Máquina Virtual	Tipo	SERVICIO	Sistema Operativo	Espacio en Disco	Tipo de Copia y Frecuencia	
						Total	Diferencial
10.11.1.60	11M2400S060.metrosalud.local (REMOTO)	Máquina Virtual	REMOTO	WS 2012	60GB	x	
10.11.1.77	11M2400S077.metrosalud.local (VCENTER)	Máquina Virtual	VCENTER	VMWARE	3236GB	x	
10..11.1.84	11M2400S084.metrosalud.local (OMNI)	Máquina Virtual	OMNI	WS 2008 R2	200GB	x	
10.11.1.86	11M2400S086.metrosalud.local (IIS - ALPHASIG)	Máquina Virtual	IIS - ALPHASIG	WS 2008 R3	180GB	x	
10.11.1.87	11M2400S087.metrosalud.local (OCS - GLPI)	Máquina Virtual	OCS - GLPI	Linux Centos 7	40GB	x	
172.31.1.2	11m2400s094.metrosalud.local (Pagina Web)	Máquina Virtual	Página Web	Centos 6,5	40GB	x	

Direccion IP	Nombre Máquina Virtual	Tipo	SERVICIO	Sistema Operativo	Espacio en Disco	Tipo de Copia y Frecuencia	
						Total	Diferencial
10.11.1.98	11M2400S098.metrosalud.local (OCS)	Máquina Virtual	OCS	Centos 6,5	40GB	x	
10.11.1.99	11M2400S099.metrosalud.local (SEVENET)	Máquina Virtual	SEVENET	Centos 6,5	800GB	x	
10.11.1.100	11M2400S100.metrosalud.local (Mesa de Ayuda)	Máquina Virtual	Mesa de Ayuda	Debian	91GB	x	
10.11.1.102	11M2400S102.metrosalud.local (RaaS)	Máquina Virtual	RaaS	Centos 6,5	80GB	x	
10.11.1.103	11M2400S103.metrosalud.local	Máquina Virtual	Mensajeria	Centos 6,5	40GB	x	
10.11.1.50	11M41630S050.metrosalud.local (Costos ABC)	Máquina Virtual	Costos ABC	WS 2003 R2	80GB	x	
10.11.1.13	ECW	Máquina Virtual	Wireless Controller	Linux	25GB	x	
10.11.172.3	11M2400S003.METROSALUD.LOCAL (CORREO)	Máquina Virtual	CORREO	Centos 6,5	3000GB	x	
10.11.1.74	11M2400S074.metrosalud.local (WEB - HL7)	Máquina Virtual	WEB - HL7	WS 2012	65GB	x	
10.11.1.78	11M2400S078.metrosalud.local (ANTIVIRUS)	Máquina Virtual	ANTIVIRUS	WS 2012	200GB	x	
10.11.1.80	11M2400S080.metrosalud.local (DA PRIMARIO)	Máquina Virtual	DA PRIMARIO	WS 2012	190GB	x	
10.11.1.81	11M2400S081.metrosalud.local (DA SECUNDARIO)	Máquina Virtual	DA SECUNDARIO	WS 2012	40GB	x	
10.11.1.83	11M2400S083.metrosalud.local (DELL ENTERPRISE)	Máquina Virtual	DELL ENTERPRISE	WS 2012	90GB	x	
10.11.1.85	11M2400S085.metrosalud.local (SQL)	Máquina Virtual	SQL	WS 2012	90GB	x	
10.11.1.88	11M2400S088.metrosalud.local (Pandion)	Máquina Virtual	Pandion	Linux	30GB	x	
10.11.1.89	11M2400S089.metrosalud.local (TERMLITE)	Máquina Virtual	TERMLITE	W7	40GB	x	
10.11.1.91	11M2400S091.metrosalud.local (EVENTOS ADVERSOS)	Máquina Virtual	EVENTOS ADVERSOS		40GB	x	
10.11.1.92	11M2400S092.metrosalud.local linux	Máquina Virtual		Centos 6,5	30GB	x	
10.11.1.95	11M2400S095.metrosalud.local (WSUS)	Máquina Virtual	WSUS	WS 2012	110GB	x	
10.11.1.96	11M2400S096.metrosalud.local (PAGINA WEB e INTRANET)	Máquina Virtual	PAGINA WEB e INTRANET	Linux	120GB	x	
10.11.1.97	11M2400S097.metrosalud.local (EVENTOS ADVERSOS 2)	Máquina Virtual	EVENTOS ADVERSOS	Linux	40GB	x	
10.11.1.100	11M2400S100.metrosalud.local (Otrs)	Máquina Virtual	OTRS	Debian	100GB	x	
10.11.8.22	interaxion26102015	Máquina Virtual	interaxion	Linux Oracle 6	500GB	x	
10.11.1.12	Netsight	Máquina Virtual	Netsight	Linux	100GB	x	
	SX - Archivos cobol	Espacio					

Diagrama del ambiente de virtualización del Sacatin







Anexo 6: GUÍA DE USO DEL SERVICIO DE INTERNET

DIRECTRICES

1.- El servicio de INTERNET es provisto por la Dirección de Sistemas a sus funcionarios de tal forma que lo utilicen para efectos de desempeñar de mejor manera sus respectivas tareas.

2.- El servicio de INTERNET es una serie de recursos de hardware y software que son limitados y es La Direccion de Sistemas el encargado de velar por la buena utilización de este recurso.

3.- Los usuarios deben acceder a INTERNET usando el navegador que se provee en sus respectivos computadores. El navegador por defecto es el Microsoft Internet Explorer versiones 7, 8 o 9.

4.- Los usuarios tienen prohibido instalar y usar programas para "bajar" información desde INTERNET hacia sus computadores. Queda totalmente prohibido el uso de programas como Emule, Ares, Kazaa y cualquier otro programa P2P (Peer to Peer).

5.- Los usuarios deben utilizar las aplicaciones provistas por la DIRECCION DE SISTEMAS usando los navegadores instalados en los computadores.

6.- Los usuarios pueden acceder a la red (Intranet) del servicio y cualquier otro sitio Internet que tenga relación con el quehacer Institucional. Quedan restringidos los accesos a las redes de tipo social (Facebook, Hi5, etc.), sitios de contenido sexual, terrorismo, descarga de piratería, media on-demand (videos, tv, radios, streaming en general).

7.- Lo indicado en el punto anterior podría sufrir cambios para asegurar la entrega de contenido útil para la Institución en casos que la Gerencia o sub direcciones así lo indique. Lo cual deberá ser informado por los canales formales.

8.- Por razones de buen servicio la Dirección de Sistemas, tiene la facultad de filtrar cualquier tipo de contenido NO útil para las labores de la E.S.E. Contenidos como Videos online, radios online, TV online, descarga de películas o algún otro programa podrían quedar restringidos para asegurar mejor rendimiento y la entrega de nuestras aplicaciones institucionales (Safix, Omega-Roche, Web e Intranet de Metrosalud, entre otros).

9.- Las configuraciones del PC y su navegador es de exclusiva responsabilidad de la Dirección de sistemas y siempre orientado a asegurar el ancho de banda para las aplicaciones y uso de interés y de apoyo a los procesos.

10.-La Dirección de Sistemas tiene la facultar de bloquear cualquier tráfico NO institucional que dificulte la "libre" circulación de información útil para la E.S.E.

11.-El uso de INTERNET podrá ser registrado por La Dirección de Sistemas por cualquier requerimiento de La Gerencia o Sub Dirección, de tal forma que sirva como evidencia en cualquier situación.

12.-Está prohibido que cualquier persona ajena a la Institución haga uso del acceso a INTERNET.

13.-Cada usuario deberá responsabilizarse de cualquier efecto NO deseado que provoque al intentar visitar algún sitio no permitido o bien instalar un programa NO autorizado ni licenciado.

14.-Todo usuario que acceda a un sitio de contenido NO apropiado deberá responsabilizarse por cualquier eventual contagio o desperfecto ocasionado por la sola visita a este tipo de sitios.

15.-Queda prohibido que los usuarios accedan a otras redes privadas o públicas a través de dispositivos wifi sin la autorización La Dirección de Sistemas.

16.-El uso de dispositivos de INTERNET Móvil (BAM: banda ancha móvil) queda absolutamente prohibido en computadores que pertenezcan a la E.S.E Metrosalud.

17.-La Dirección de Sistemas, realizará monitoreo permanentes, mediante las herramientas con las que cuenta para determinar el cumplimiento de estas políticas.

18.-El no cumplimiento de algunas de estas reglas podría facultar al Departamento de TI a informar dicha situación a los estamentos competentes de la DIRECCION DE SISTEMAS.

CATEGORIAS PERMITIDAS Y LIMITADAS

Son los agrupadores en los que están clasificadas todas las páginas de internet y nos permiten realizar restricciones por tipos de página. A continuación las categorías en rojo las que se bloquean y en verde las permitidas.

1. **Anonimizadores**. Sitios web que permitan a los usuarios navegar por Internet y acceder a contenido de Internet sin ser registrados por terceros.

2. **Anorexia y Bulimia**. Sitios web dedicados a promover y fomentar los trastornos alimenticios.

3. **Anuncios**. Anuncios publicitarios que formen parte de un sitio web.

4. **Arte**. Sitios web que ofrezcan información acerca del mundo el arte, p. ej. Sobre museos, escultura, fotografía, literatura, etc.

5. **Bancos e instituciones financieras**. Sitios web de bancos e instituciones financieras de todo el mundo.

6. **Blogs**. Sitios web en los que los usuarios puedan mostrar sus diarios y cualquier experiencia, comentario, ideas, etc. que deseen compartir a través de Internet.

7. **Bombas**. Sitios web que expliquen cómo se diseñan, se fabrican y se utilizan los explosivos y dispositivos explosivos.

8. **Buscadores**. Sitios web utilizados para realizar búsquedas de contenido y explorar Internet

9. (google.com, yahoo.com, altavista.com, alltheweb.com, etc.).

10. **Chat**. Sitios web en los que los usuarios finales puedan comunicarse con otros usuarios en tiempo real.

11. **Compras**. Sitios web para realizar compras en línea.

12. **Contactos**. Sitios de contactos en los que el usuario pueda conocer a otras personas, hacer amigos, buscar pareja, etc.

13. **Correo en web**. Sitios web que proporcionen servicios de correo en web con los que se pueda enviar y recibir mensajes de correo electrónico desde cualquier PC que tenga una conexión a Internet (Hotmail, Yahoo, Gmail, etc.).

14. **Deportes**. Sitios web que ofrezcan contenido relacionado con los deportes, los equipos deportivos, etc.

15. **Derecho**. Sitios web que contengan información sobre asuntos jurídicos.

16. **Drogas**. Sitios web que fomenten el consumo de drogas o proporcionen contactos e información sobre puntos de venta de drogas. Esta categoría no incluye información genérica o medidas preventivas contra el consumo de drogas.

17. **Economía**. Sitios web con contenido sobre mercados bursátiles, banca, inversiones financieras, seguros, etc.

18. **Educación**. Sitios web de colegios, institutos, universidades, academias y centros de formación.

19. **Empleo**. Sitios web de búsqueda de empleo. Esta categoría también incluye los cazatalentos así como cualquier contenido relacionado en Internet.

20. **Foros**. Sitios web que inviten a los usuarios a participar en debates sobre determinados temas.

21. **Gobierno**. Sitios web de entidades e instituciones públicas, como ministerios, secretarías gubernamentales, ayuntamientos, la Unión Europea y cualquier otra dirección URL o página web que ofrezca información relacionada con las instituciones gubernamentales de todo el mundo.

22. **Guías telefónicas y callejeras**. Sitios web que incluyan mapas de ciudades y callejeros así como información de contacto, como direcciones, números de teléfonos, etc.

23. **Hackers**. Sitios web en los que se pueda encontrar información sobre piratería informática, software pirateado e ilegal así como software utilizado con fines de piratería informática.

24. **Hospedaje de dominios**. Sitios web de hospedaje en los que se puedan adquirir dominios de

25. **Información**. Sitios web que ofrezcan información general sobre las condiciones del tráfico, el tiempo, etc.

26. **Informática**. Sitios web con información relacionada con el hardware, el software, Internet, etc.

27. **Juegos**. Sitios web en los que los usuarios puedan jugar a juegos en línea o descargar juegos para el ordenador.

28. **Juegos de Apuestas**. Sitios web que proporcionen acceso a juegos de apuestas en línea, como casinos, y cualquier otro servicio en línea de realización de apuestas.

29. **Logotipos/Tonos**. Sitios web en los que se puedan descargar imágenes y/o tonos (melodías monofónicas o polifónicas) para el teléfono móvil.

30. **Mensajería Instantánea**. Sitios web en los que se pueda descargar software de mensajería instantánea (p. ej. MSN Messenger, Yahoo Messenger, etc.).

31. **Modelos**. Sitios web que contengan fotografías de modelos. Los sitios web en los que este tipo de fotografías muestren a los modelos total o parcialmente desnudos se incluyen en la categoría de pornografía.

32. **Música**. Sitios web en los que los usuarios puedan adquirir o descargar música, u obtener información sobre cantantes y grupos musicales en general.

33. **Ocio**. Sitios web que contengan información sobre actividades de tiempo libre, p. ej. cine, teatro, literatura, gastronomía, aficiones, etc.

34. **Pay-per-surf**. Páginas web en las que los usuarios puedan ganar dinero en Internet a cambio de recibir mensajes de correo electrónico, navegar en ciertas páginas web, inscribirse en ofertas gratuitas, etc.

35. **Pornografía**. Sitios web con contenido pornográfico y erótico. Esta categoría incluye el acceso a salas de chat en las que se pueda encontrar este tipo de material.

36. **Portales**. Sitios web que ofrezcan una amplia gama de contenido (p. ej. noticias, ocio, deportes, juegos, música, etc.) centralizado.

37. **Prensa**. Periódicos o revistas en línea.

38. **Racismo**. Sitios web con contenido de naturaleza abiertamente xenófoba o que promueva y/o defienda un comportamiento discriminatorio basado en la cultura, la raza, la religión, la ideología, etc.

39. **Redirectores**. Sitios web que redirijan o transformen otras páginas web.

40. **Salud**. Sitios web con información no científica acerca de las enfermedades y sus curas.

41. **Sectas**. Sitios web sobre organizaciones universalmente reconocidas como sectas. En esta categoría, se incluyen las direcciones URL que fomentan de manera directa o indirecta: (i) el daño a grupos, animales o individuos, (ii) el contenido esotérico (iii) el contenido que constituye un mal ejemplo para los niños: que enseña y alienta a los niños a realizar actos perjudícales o a imitar comportamientos peligrosos, (iv) el contenido que genera sentimientos de miedo, intimidación, terror o terror psicológico, (v) la incitación o la descripción de daños contra un individuo o un grupo por motivos de género, orientación sexual, etnia o identidad religiosa o nacional.

42. **Servicios de DNS**. Sitios que bloqueen el acceso a los servicios de DNS dinámico.

43. **Servidores P2P**. Sitios web que posibiliten a los usuarios el uso compartido de archivos o la descarga de archivos legales e ilegales. Esta categoría también incluye los sitios web que contengan aplicaciones y programas de punto a punto.

44. **Sexualidad**. Sitios web que proporcionen información sobre sexo, sexo y adolescencia, educación sexual, etc., sin contenido pornográfico.

45. **Sitios web personales**. Sitios web personales creados por usuarios de todo el mundo para presentarse a sí mismos o temas concretos que les interesen.

46. **Software malicioso**. Sitios web que contengan código o programas maliciosos como virus o troyanos.

47. **Sociedad**. Sitios web con contenido relacionado con los famosos, la moda, el estilo de vida, etc.

48. **Spyware (Programas espía)**. Sitios web que contengan programas espía. Los programas espía son programas que recogen información confidencial y general en los PC y

la transmiten a terceros. Todo esto tiene lugar sin el conocimiento ni el consentimiento del usuario.

49. **Telecomunicaciones**. Sitios web que proporcionen información acerca de telefonía fija, telefonía móvil, conexiones a Internet, etc.

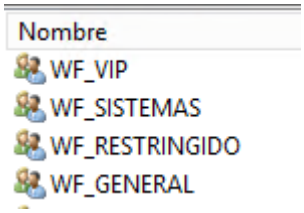
50. **Viajes**. Portales de agencias de viales y sitios web con información sobre ciudades, hoteles y transporte.

51. **Violencia**. Sitios web y/o páginas web que ofrezcan contenido de carácter explícitamente violento y/o fomenten o defiendan la violencia.

52. **VoIP (Voz sobre IP)**. Sitios web que proporcionen acceso a aplicaciones que ofrezcan transmisiones de voz en directo a través de Internet, mediante protocolos TCP/IP.

Privilegios de navegación según Grupo del directorio

Los permisos de navegación de dan de acuerdo al grupo que pertenezca cada usuario en el directorio AC que son los siguientes:



Donde VIP y sistemas tienen los privilegios mas altos permitiendo la navegación a las redes sociales.

El grupo de General permite la navegación de todos los sitios menos las redes sociales

El restringido e invitados tiene navegación solo aun listado de páginas Web para solo acceder en lo que necesita para trabajar como para un perfil de facturación o auxiliar administrativo.

Vale decir que sea cual sea el grupo que pertenezca el usuario tiene **bloqueadas** las páginas Velicas y para adultos o que contengan contenido no seguro que pueda afectar la integridad de la información.

Anexo 7. CONFIGURACIÓN DE CUENTAS DE CORREO

Cómo configurar cuentas de correo POP3 en Outlook Metrosalud

Configurar el **correo de tu negocio** en el gestor de correos de Microsoft Outlook es muy fácil y así podrás **gestionar tus diferentes cuentas desde un solo lugar.** En el tutorial de hoy veremos el paso a paso para **configurar** correctamente una **cuenta de correo POP3 en Outlook.**

1. Abre el Outlook Express. Te aparecerá el asistente de Outlook que te guiará a través del proceso. Sin importar la versión que utilices de Outlook los pasos son los mismos.

2. Te preguntará si deseas configurar una cuenta de correo electrónico. Haz clic en sí.

3. Selecciona "Configurar manualmente las opciones del servidor o tipos de servidores adicionales". Haz clic en Siguiente.

4. Elige correo electrónico de Internet.

5. Llena todos los campos de la siguiente manera:

Información sobre el usuario

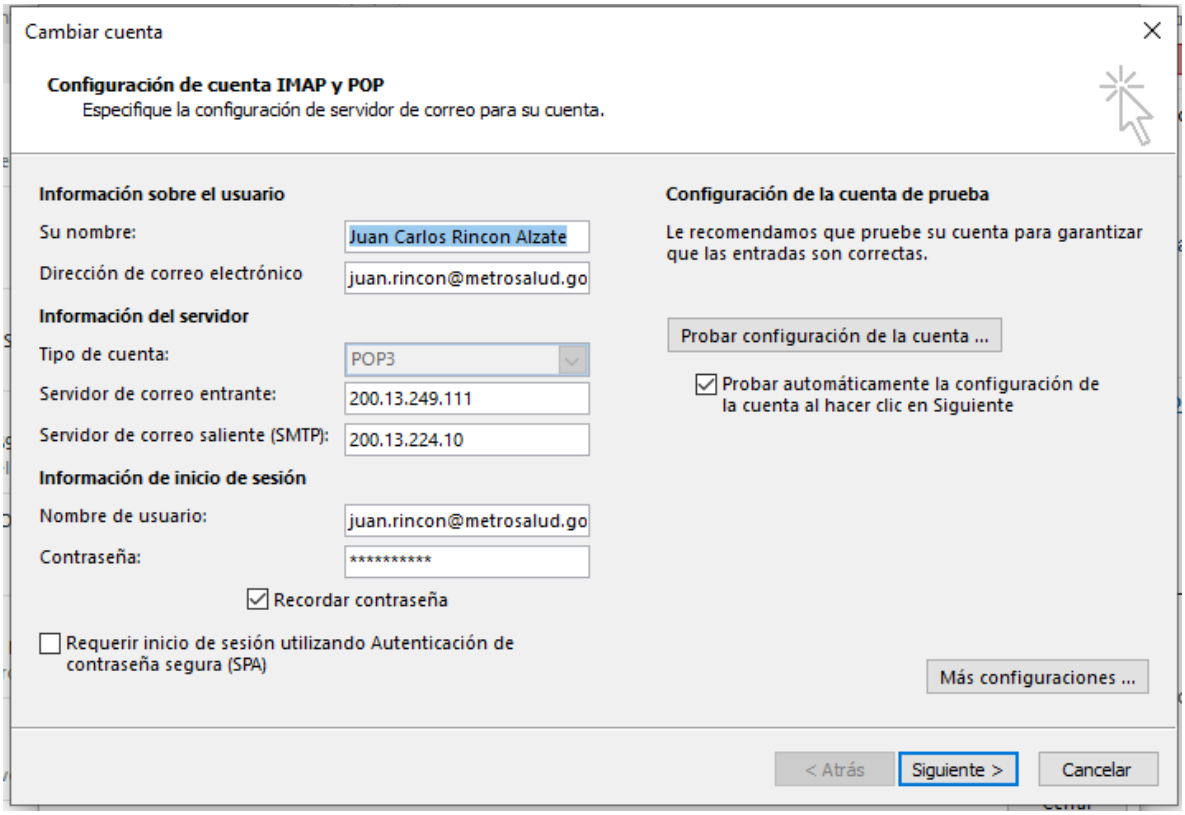
- Su Nombre: El nombre que quieres que aparezca al enviar un correo.
- Dirección de correo electrónico: Tu correo electrónico, por ejemplo: USUARIO@metrosalud.gov.co

Información del servidor

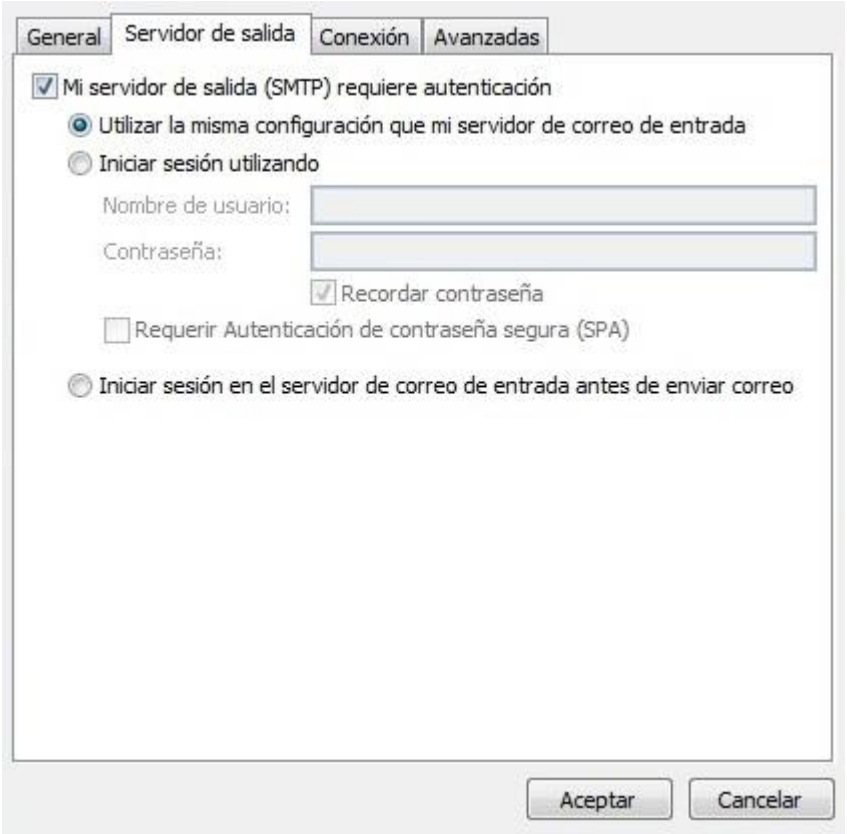
- Tipo de Cuenta: POP3
- Servidor de correo entrante: pop.une.net.co ó 200.13.249.111
- Servidor de correo saliente (SMTP): smtp.une.net.co ó 200.13.224.10

Información inicio de sesión

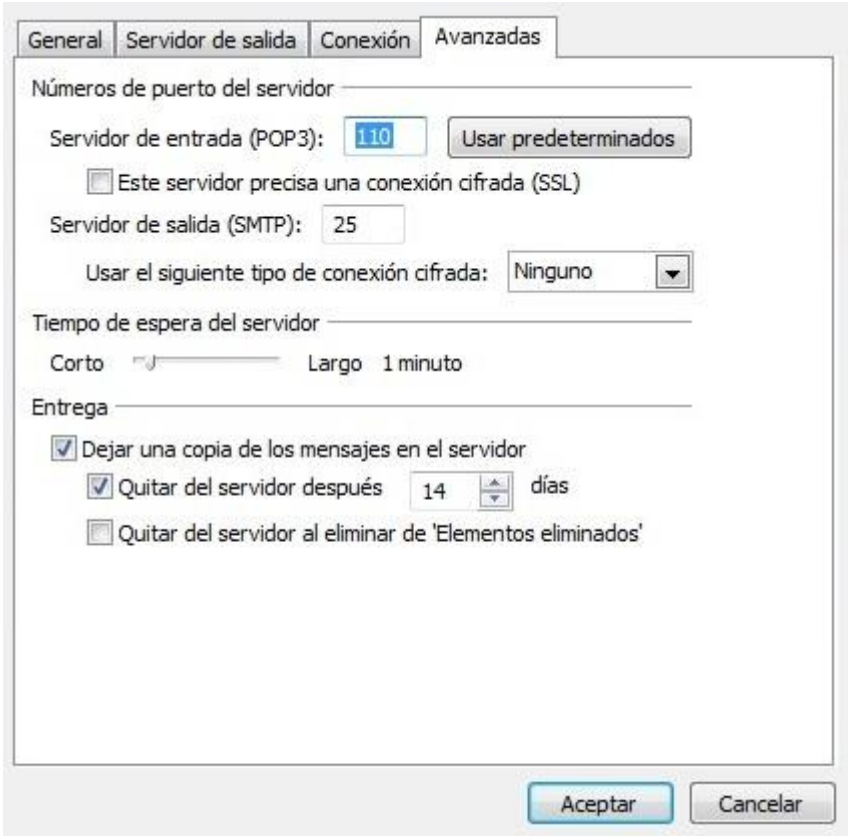
- Nombre de usuario: **USUARIO@metrosalud.gov.co**
- Contraseña: La contraseña de tu cuenta de correo.



6. En la misma ventana haz clic en "Más configuraciones…". Luego selecciona la pestaña Servidor de Salida y elige "Mi servidor de salida (SMTP) requiere autenticación" y "Utilizar la misma configuración que mi servidor de correo de entrada".



6. **Recuerda siempre verificar en la pestaña "Avanzadas" los números de puertos del servidor. Para POP3 deben estar como detalla la imagen.**



ANEXO 8. MANTENIMIENTO DE EQUIPOS DE CÓMPUTO

LIMPIEZA DEL HARDWARE PC´S

El proceso de mantenimiento preventivo se realiza de acuerdo con el "Cronograma de mantenimiento y limpieza de equipos de computo.xls"

COMPROBACIÓN ESTADO DEL PC O PORTATIL

Antes de comenzar con el procedimiento, se hace una verificación externa del estado del dispositivo (PC, Impresora, swiche, servidor, etc.), esto con el objetivo de evaluar posibles fallas que requieran un mantenimiento correctivo.

ABRIR Y DESMONTAR PARTES

Como medida de seguridad para iniciar, el dispositivo debe estar apagado, luego desconecta el cable de la fuente de poder, abra la CPU o dispositivo.

Para comenzar con todo el mantenimiento se verifica el estado de los componentes básicos de la placa base como son los condensadores, lo común es que cuando se dañan se hinchen en la parte superior o inferior, algunos suelen reventar botando un líquido a veces negro o a veces marrón o color café, si nota alguno de ellos dañado debe proceder a cambiarlo o reportarlo en garantía, porque es posible es que sea fuente de problemas. Aparte de los condensadores se debe prestar suma atención a la main board, para verificar que no tenga algún parche negro que demuestre quemadura, alguna pista rota, quemada o levantada, o alguna pieza averiada o floja.

Para tener en cuenta, se necesitan de herramientas para proceder a la limpieza, estas son:

- Brocha Pequeña y seca
- Soplador
- Juego de destornilladores, varios.
- Limpión o trapo de sacudir
- Limpia contactos y Limpiador Lubricante 5-56
- Alcohol isopropilico
- Barra de borrador
- Crema Frotex o similar
- Cepillo de pequeño

ACTIVIDADES DEL MANTENIMIENTO

1. Se desconectan de la Main Board los componentes como las memorias, el disco duro, las unidades de Cd y Diskette si los tiene, la fuente de poder.
2. Las memorias se limpian con el borrador en sus partes de contactos para eliminar cualquier tipo de polvo o sulfatación que tenga, terminando con la brocha quitando las partículas del borrador.
3. Se proceden eliminar el polvo de la placa base con el soplador, teniendo en cuenta que el ventilador hay que colocarle sostenimiento con el destornillador pequeño para que al pasar el soplador no lo haga tener muchas revoluciones y no se dañe.
4. Con la brocha se procede a terminar de limpiar cada una de las partes de conexión como correas, slots de expansión y partes eléctricas, quitando las pocas partículas de polvo que queden.
5. Con el limpiador de contactos se esparce por toda la placa base especialmente en las ranuras y slots de expansión y contactos, también a los ventiladores se les lubrica con el 5-56.
6. Una vez terminado este proceso se vuelven a conectar cada una de las partes verificando que queden bien, igualmente los ventiladores y refrigerante del procesador que este bien conectados y seguros.
7. Se tapa nuevamente el equipo.
8. Se limpia externamente el computador con un poco de Frotex y agua, revisando que no queden partículas de este en las ranuras.

MANTENIMIENTO DE LA PANTALLA

1. Para la limpieza de la pantalla, se limpian los cables de conexión tanto al computador como a la corriente eléctrica.
2. Con el soplador se limpia el polvo de las ranuras de ventilación.
3. La parte de atrás se limpia con un poco de Frotex y agua, revisando que no queden partículas de este en las ranuras.
4. La parte frontal de la pantalla se limpia con un sacudidor de pana y alcohol isopropilico.

MANTENIMIENTO DEL MOUSE

1. El Mouse tiene en la parte de abajo una tapa donde se encuentra la bolita que hace que se mueva, esta se gira hacia la izquierda para ser retirada, allí se extrae y se limpiar con un limpión de pana, revisando que no queden partículas de pelusas pegadas a él.
2. También tiene un tornillo el cual se puede quitar y se destapa, se limpia con la brocha internamente y revisando que los rodillos no tengan pegado ningún tipo de sucio.

3. Para los Mouse ópticos, se recomienda que si tiene pad mouse, estos se mantengan limpios de cualquier partícula para que el lente se mantenga sin obstrucción y en el momento de la limpieza se haga con alcohol.

MANTENIMIENTO DEL TECLADO

1. La limpieza del teclado se hace con soplador primeramente tratando que salgan todas las partículas que tenga incrustadas dentro de las teclas verificando que también salgan los ganchos de cosedoras que son muy comunes.
2. Si es necesario destapar el teclado porque está muy bloqueado por estas partículas y hay que hacerle mantenimiento correctivo se quitan los tornillos de la parte por debajo y con cuidado se abre, haciendo una limpieza más detallada y profunda de cada una de las teclas.
3. Para limpiar las teclas externamente, se hace con un cepillo de dientes y un trapo mojado y con Frotex diluido preferiblemente, pasando el cepillo por entre las ranuras de separación de las teclas.
4. Si el teclado tiene borrados los caracteres de las teclas se debe realizar una solicitud para reposición del dispositivo.

Al terminar de hacer el mantenimiento de cada uno de los dispositivos y periféricos del computador se conecta nuevamente cada una de las partes y a la energía por último, se prende y se verifica que no haya ningún problema en cuanto a la conexión del hardware.

MANTENIMIENTO FÍSICO DE LOS PORTÁTILES

Para los portátiles el proceso de limpieza es el siguiente:

1. Se abre el portátil quitando todos los tornillos en la parte de abajo.
2. Se levanta en la parte de arriba una pequeña tapa ubicada junto a la pantalla, comenzando por la parte derecha que tiene una pequeña rendija la cual se levanta con un destornillador hasta quitarla toda.
3. Se quitan los tornillos del teclado, la pantalla, la antena inalámbrica el panel de encendido para poder quitar del todo la cubierta del portátil.
4. Se busca el lugar donde está el procesador y allí se quita el ventilador y se limpia o sopla la rejilla que por lo general se llena de pelusa.
5. Se sopla el teclado y se limpia con un trapo mojado y el cepillo de dientes, se limpia la parte interna con la brocha y vuelve y se tapa el equipo verificando que quede conectado correctamente.

LIMPIEZA LOGICA PC´S

El siguiente es el proceso de limpieza lógica de los equipos de cómputo:

1. Se coloca por el Explorador de Windows **Herramientas-Opciones de Carpeta-Ver**, se busca la opción Mostrar archivos y carpetas ocultas y se activa, se da Aceptar.
2. En la ruta **C:\Documents and Settings\<Usuario>\Configuración local\Archivos temporales de Internet**, se muestran todos los archivos temporales que el sistema ha creado, se marcan y eliminan con shift+supr.
3. Ingresando a cualquier página en Internet se ingresa por menú **Herramientas-Opciones de Internet-General-Eliminar**, se eliminan los archivos temporales y también los Cookies de Internet.

Esto se hace para cada usuario que tenga perfil en el equipo, recordar que debe volver a ejecutar el primer paso para volver a restaurar las propiedades a los archivos ocultos.

También se debe revisar por el **Panel de Control Agregar o Quitar Programas**, aquellas aplicaciones que han sido instaladas por los usuarios que no son autorizadas por el área de Sistemas y se eliminadas, solo deben permanecer aplicaciones que sean autorizadas por las políticas de la clínica.

En la parte del Antivirus se debe revisar que esté actualizado y verificar que se halla realizada la última escaneada automáticamente de acuerdo a la programación, si no está escaneado entonces hacer un escaneo del sistema y actualizarlo.

ACTIVIDADES DE AUDITORÍA.

Esta actividad tiene como objetivo implementar auditoria a cumplimiento de política de seguridad informática

- Verificar que El software instalado es el autorizado y licenciado.
- Verificar la existencia de archivos tipo video y música (MP3, WAP, etc.).
- Verificar según usuario el tipo de acceso a internet.
- Verifica el histórico de navegación
- Realizar con el usuario el cambio de contraseña en cada mantenimiento.
- Verificar la cuarentena del sistema de antivirus evaluar y limpiar si es el caso.
- Verificar la marcación de activos fijos.
- Verifica que la marcación corresponde a la ubicación y asignación consignada en el inventario.

Al terminar el mantenimiento se socializan con el usuario las políticas de seguridad informática, mostrando su acceso desde la intranet.

Las novedades encontradas se registran mediante correo electrónico al jefe de sistema y jefe del área de la novedad.

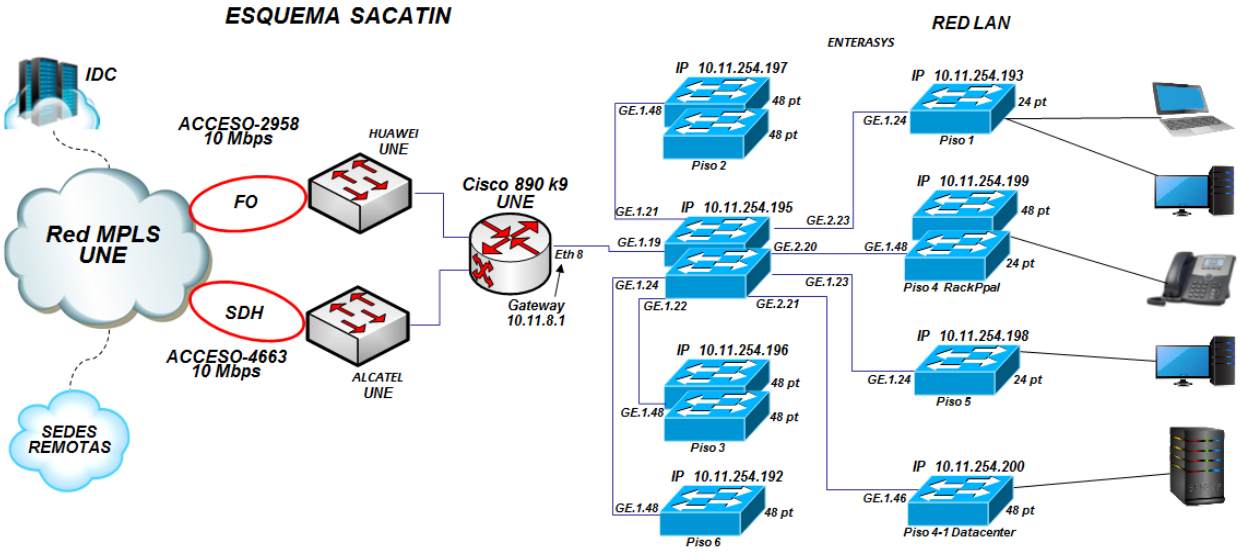
Anexo 9 ARQUITECTURA IP METROSALUD

Con miras a una mejora en el rendimiento de red es necesario establecer una nueva Arquitectura IP.

Como primera medida se plantea una segmentación de la red LAN en VLAN's (Redes virtuales), estas agrupaciones virtuales evitaran que diferentes tráficos se propaguen por toda la red, brindando esto mayor nivel de seguridad a la información.

Debido a las nuevas necesidades de la red, se hace necesario implementar estas mejoras que aumenten la capacidad de conmutación y en general la eficiencia de la red.

En el siguiente diagrama se detalla la topología de red de la sede Sacatin, tomada cómo ejemplo



Esquema de Asignación

Existen recursos que por su naturaleza deben estar separados en diferentes VLAN este el caso de las impresoras, servidores, servicios de telefonía, internet, WiFi corporativo y gestión de equipos activos de red.

Para esta propuesta se plantea continuar usando la red 10.0.0.0 /16, esta será subdividida en segmentos más pequeños que suplan las necesidades de cada VLAN de acuerdo su tamaño y teniendo en cuenta su capacidad de crecimiento

Se toma como referencia la red 10.0.0.0/16 para cada sede y subredes 10.0.0.0/24 para diferenciar servicios dentro de cada sede

Esquema de Asignación dentro de cada sede

Con el propósito de mantener uniformidad en la asignación de direcciones IP se establecen las siguientes condiciones para cada sede.

- El primer *octeto* es fijo, con un valor de 10.
- El segundo *octeto* diferencia ubicaciones o sedes.
- Se establece el tercer *octeto* de la asignación perteneciente a cada sede para diferenciar categorías de servicios y equipos.
- El último *octeto* corresponde a cada usuario final.

Segundo *Octeto*

El segundo *octeto* se utiliza para indicar la sede según tabla

SEDE	MAPA	MASCARA	ROUTER
APH (Alfonso Lopez)	10.199.0.1/24	255.255.0.0	10.199.11.1/24
C.S UNIDAD MENTAL	10.74.0.0/16	255.255.0.0	10.74.8.1/16
C.S. Alfonso López	10.29.0.0/16	255.255.0.0	10.29.0.0/16
C.S. Altavista	10.41.0.0/16	255.255.0.0	10.41.8.100/16
C.S. Aranjuez	10.104.0.0/16	255.255.0.0	10.104.8.100/16
C.S. Belén Rincón	10.20.0.0/16	255.255.0.0	10.20.8.100/16
C.S. Carpinello	10.43.0.0/16	255.255.0.0	10.43.8.100/16
C.S. Civiton	10.31.0.0/16	255.255.0.0	10.31.8.100/16
C.S. El Limonar	10.66.0.0/16	255.255.0.0	10.66.8.100/16
C.S. El Raizal	10.42.0.0/16	255.255.0.0	10.42.8.100/16
C.S. El Salvador	10.103.0.0/16	255.255.0.0	10.103.8.100/16
C.S. El Triunfo	10.55.0.0/16	255.255.0.0	10.55.8.100/16
C.S. Enciso	10.111.0.0/16	255.255.0.0	10.111.8.100/16
C.S. Estadio	10.38.0.0/16	255.255.0.0	10.38.8.100/16
C.S. Guayabal	10.12.0.0/16	255.255.0.0	10.12.0.0/16

SEDE	MAPA	MASCARA	ROUTER
C.S. La Cruz	10.44.0.0/16	255.255.0.0	10.44.8.100/16
C.S. La Esperanza	10.47.0.0/16	255.255.0.0	10.47.8.100/16
C.S. La Loma	10.33.0.0/16	255.255.0.0	10.33.8.100/16
C.S. La Quiebra	10.39.0.0/16	255.255.0.0	10.39.0.0/16
C.S. Las Margaritas	10.36.0.0/16	255.255.0.0	10.36.0.0/16
C.S. Llanaditas	10.40.0.0/16	255.255.0.0	10.40.0.0/16
C.S. Loreto	10.28.8.100/16	255.255.0.0	10.28.8.100/16
C.S. Manantial de Vida	10.45.0.0/16	255.255.0.0	10.45.0.0/16
C.S. Moravia	10.34.0.0/16	255.255.0.0	10.34.8.100/16
C.S. Pablo VI	10.24.0.0/16	255.255.0.0	10.24.8.100/16
C.S. Palmitas	10.110.0.0/16	255.255.0.0	10.110.8.100/16
C.S. Picachito	10.54.0.0/16	255.255.0.0	10.54.8.100/16
C.S. Poblado	10.21.0.0/16	255.255.0.0	10.21.0.0/16
C.S. Popular 1	10.23.0.0/16	255.255.0.0	10.23.0.0/16
C.S. Robledo	10.101.0.0/16	255.255.0.0	10.101.0.0/16
C.S. San Blas	10.16.0.0/16	255.255.0.0	10.16.8.100/16
C.S. San Camilo	10.73.0.0/16	255.255.0.0	10.73.8.100/16
C.S. San Lorenzo	10.25.0.0/16	255.255.0.0	10.25.0.0/16
C.S. Santa Elena	10.109.0.0/16	255.255.0.0	10.109.8.100/16
C.S. Santa Rosa de Lima	10.37.0.0/16	255.255.0.0	10.37.8.100/16
C.S. Santander	10.61.0.0/16	255.255.0.0	10.61.8.100/16
C.S. Santo Domingo Savio	10.19.0.0/16	255.255.0.0	10.19.8.100/16
C.S. Sol de Oriente	10.62.0.0/16	255.255.0.0	10.62.8.100/16
C.S. Villa del Socorro	10.17.0.0/16	255.255.0.0	10.17.8.100/16
C.S. Villa Laura	10.105.0.0/16	255.255.0.0	10.105.8.100/16
C.S. Villatina	10.59.0.0/16	255.255.0.0	10.59.8.100/16
C.S. Trinidad	10.14.0.0/16	255.255.0.0	10.14.8.100/16
DATA CENTER UNE	10.158.0.0/16	255.255.0.0	10.158.0.0/16
ESU - 123 - Sisme	10.132.0.0/16	255.255.0.0	10.132.8.100/16
LIVING LAB	10.188.0.0/16	255.255.0.0	10.188.8.100/16
SACATIN	10.11.0.0/16	255.255.0.0	10.11.8.100/16
U.H CLINICA MUJER	10.95.0.0/16	255.255.0.0	10.95.8.1/16
U.H. BELEN	10.1.0.0/16	255.255.0.0	10.1.8.1/16
BUENOS AIRES	10.8.0.0/16	255.255.0.0	10.8.8.1/16
U.H. CAMPO VALDEZ	10.48.0.0/16	255.255.0.0	10.48.8.1/16
U.H. CASTILLA	10.7.0.0/16	255.255.0.0	10.7.8.1/16

SEDE	MAPA	MASCARA	ROUTER
U.H. DOCE DE OCTUBRE	10.10.0.0/16	255.255.0.0	10.10.8.1/16
U.H. MANRIQUE	10.5.0.0/16	255.255.0.0	10.5.8.1/16
U.H. NUEVO OCCIDENTE	10.56.0.0/16	255.255.0.0	10.56.8.1/16
U.H. SAN A. DE PRADO	10.2.0.0/16	255.255.0.0	10.2.8.1/16
U.H. SAN CRISTOBAL	10.3.0.0/16	255.255.0.0	10.3.8.1/16
U.H. SAN JAVIER	10.6.0.0/16	255.255.0.0	10.6.0.0/16
U.H. SANTA CRUZ	10.9.0.0/16	255.255.0.0	10.9.8.1/16

La red de la UH Campo Valdez es 10.8.0.0 / 16 con Gateway 10.8.8.1

Tercer *Octeto*

El tercer *octeto* permite separar categorías de equipos, bien sea por su ubicación o por su propósito dentro de la red.

Esta separación tiene como propósito permitir un mejor manejo en grupos de seguridad o separación entre *VLAN*, así como una identificación rápida en estructuras de auditoria.

Para garantizar uniformidad, este *octeto* debe separarse por categorías, que permiten rápidamente establecer el propósito de cada equipo en la red. Permitiendo además una aproximación desde el punto de vista de prioridades de tráfico y/o seguridad.

Se presenta una separación por diez identificadores de VLAN, este espacio garantizara un crecimiento futuro, de esta forma si aparece una nueva dependencia o grupo se tendrán ID de VLAN disponibles.

Ejemplo:

SACATIN					
VLAN ID	**Nombre**	**ID de red**	**Mascara**	**Puerta de enlace**	**Broadcast**
10	Servidores	10.11.10.0	255.255.255.128	10.11.10.1	10.11.10.127
30	Usuarios	10.11.30.0	255.255.255.0	10.11.30.1	10.11.30.255
50	Telemedicina	10.11.50.0	255.255.255.0	10.11.50.1	10.11.50.255
60	WiFi corporativo	10.11.60.0	255.255.255.0	10.11.60.1	10.11.60.255
70	Telefonía	10.11.70.0	255.255.255.0	10.11.70.1	10.11.70.255
80	Gestión	10.11.80.0	255.255.255.192	10.11.80.1	10.11.80.63
90	Impresión	10.11.90.0	255.255.255.192	10.11.90.1	10.11.90.63
110	WiFi invitado	10.11.110.0	255.255.255.0	10.11.110.1	10.11.110.255
254	Admin SW	10.11.254.0	255.255.255.0	10.11.254.1	10.11.254.255
1	Default				

Se establece la siguiente categorización para el tercer *octeto*.

Tercer Octeto			
Segmento	**Función para cada segmento**	**Ejemplo Sacatin**	**Ejemplo Belén**
1	vlan default		
8	Infraestructura de red equipos de comunicación (switches, routers y Wireless)	10.11.8.0	10.02.8.0
9	Infraestructura de Impresión	10.11.9.0	10.02.9.0
1	Servidores		
3	Usuarios		
4	Usuarios vip		
14	programas (convenios con externos)		
11	Auditorios y zonas comunes		
13	Wireless institucional		
60	Wireless invitados		
70	Cámaras ip		
10	Inteligencia de edificios		
90	**Telefonía**		
5	**Imágenes y telemedicina**		

Cuarto *Octeto*.

El último *byte* distingue a un usuario de otro, dentro de cada dependencia.

Se sugiere que a las instalaciones temporales le sean asignadas direcciones a partir del 200, de tal forma que la dirección IP acarreé información adicional del estado o derechos de seguridad del usuario.

Disponibilidad de Direcciones

Teniendo en cuenta la segmentación realizada, para cada dependencias se pueden diferenciar en este esquema, se dispone de doscientas cincuenta y cinco (255) por dependencia.

Etapas

Debido a los cambios en configuraciones de infraestructura y cambios a distintos niveles, se contemplará el siguiente orden:

1. Se debe marcar la totalidad de los puntos de red para garantizar la conexión y trazabilidad
2. Se deben configurar en todos los router y enlaces de switches las troncales que permitan el flujo de las diferentes redes.

3. Se debe configurar en cada máquina el puerta de enlace y la máscara correspondiente
4. Se solicitará al UNE realice la configuración de los routers dejando una RED por defecto para permitirles una migración paulatina.
5. Migrar Sacatin y SISAM.
6. Migrar 9 Unidades Hospitalarias
7. Por ultimo migrar los centros de salud y programas
   A medida que centro termine su migración se desactivará la RED por defecto

Anexo 10. GESTIÓN DE AMBIENTES DE BASES DE DATOS

ACTUALIZACION DE LA DATA EN LOS AMBIENTES. DESCRIPCIÓN.

Se ha establecido como mínimo deseado 2 refrescos del ambiente de pruebas anualmente, estos se realizan en el mes de marzo y en el mes de octubre. Sin embargo, podrá realizarse cuando por solicitud del proveedor o de la E.S.E se requiera.

Este procedimiento se realiza mediante la restauración de un backup y la aplicación de archivelog hasta llegar al punto de la data en producción.

ADMINISTRACION DE LAS ACTULIZACIONES

Para mantener los ambientes homogéneos se estable que el proveedor de software trabaja en la BD DESA entrega a los ingenieros de Metrosalud para realizar el aval de las funcionalidades en la BD de PRUEBA, certificada la función se pasa a producción.

Lo anterior garantiza que frente a estructura de base de datos y funciones del aplicativo BD Pruebas y BD producción permanecen al mismo nivel, mientras que DESA permanece un paso adelante ya que contienen los nuevos ajustes o funcionalidades.

SOLICITUDES DE ACTULIZACION DE LA DATA DE LOS AMBIENTES

- Los ingenieros de Metrosalud validan que desarrollos se encuentran pendientes para salir a producción, se establecen la actualización de prueba para avalar el paso a producción.
- Se registra solicitud de ticket con el DBA del Datacenter y se establece la ventana requerida.
- Se notifica al proveedor del software de la ventana, para que no programe recurso
- Se recibe notificación de ejecución del ticket
- Se realizan pruebas de consistencia de datos y de versión de las aplicaciones
- Se levanta la ventana.

Nota: La actualización de los ambientes de pruebas y desarrollo no tienen afectación para los usuarios finales, solo afecta las labores de desarrollo y pruebas de nuevas funcionalidades.

TOPOLOGÍA DE LOS AMBIENTES. Componentes.

Clúster Aplicaciones:

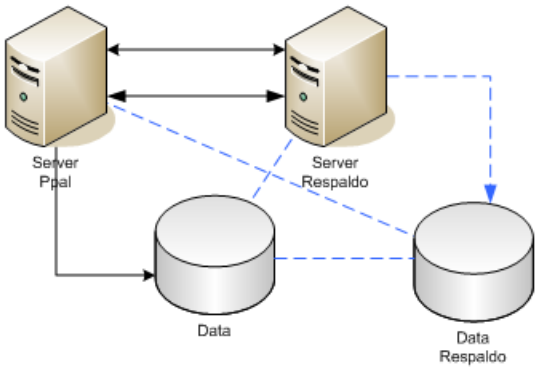
- (2) dos servidores T5-2 para el ambiente de producción. Las características técnicas de cada servidor son: un (1) procesador 16 core y 256 GB de RAM.
- un servidor T4-1 para el ambiente de Pruebas y Desarrollo (existente). Las características técnicas del servidor son: un (1) procesador 1 core y 256GB de RAM.

- Nota: la maquina T4-1 solo tendrá activo un (1) core.

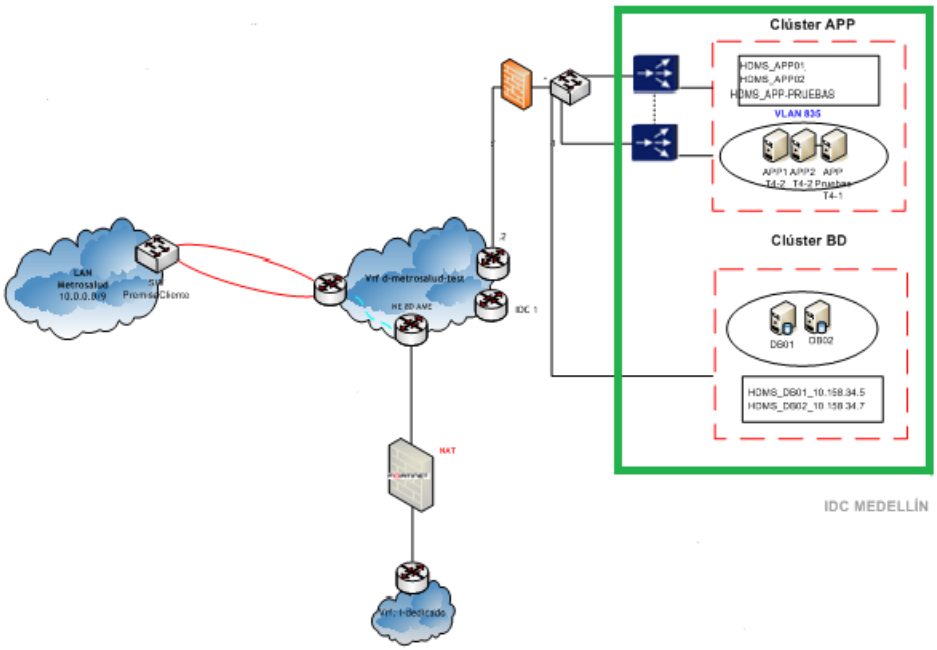
Clúster Base de Datos:

- (2) servidores Power 822 para el ambiente de producción (RAM 256GB, dos (2) procesadores power 8 (3.42Ghz de 10 Cores por procesador). Para suplir el licenciamiento de BD estándar solo se utilizarán 3 procesadores (30 Cores activos) y uno de los procesadores (10 cores) quedaría inactivo para futuros crecimientos.

- Para el ambiente de Pruebas y desarrollo, se asignará un LPAR en las maquinas Power 822 de producción.



Topología



Anexo 11. SEGURIDAD PERIMETRAL TIGO UNE

En **Tigo** nos tomamos muy en serio los temas de seguridad, agradecemos este tipo de casos. En la actualidad la versión de la plataforma de correo desde donde se brinda servicio para los buzones de correo del dominio ***metrosalud.gov.co*** y respondiendo a las inquietudes donde nos solicitan información acerca de los parámetros de seguridad configurados compartimos la siguiente información:

El dominio de correo ***metrosalud.gov.co*** a nivel de intercambio de mensajes de entrada y salida es protegido por una solución Antivirus/Antispam basado en un esquema de clúster con varios equipos en alta disponibilidad para la protección contra amenazas tipo virus y spam. También se cuenta con balanceadores de carga, cortafuegos (Firewall) entre otros.

Entre las características y beneficios de los equipos Antivirus/Antispam contamos:

Proveedor: **FortiNet**

Protección basada en Antispam:

El servicio de Antispam nos permite realizar un filtro y revisar su contenido que no venga con software malicioso o según du reputación, esta reputación la da si ya ha sido reportado como correo spam en la web. Esto nos da seguridad en la recepción de los correos que lleguen al buzón de bandeja de entrada de cada usuario.

Servicio antispam de FortiGuard
- Reputación global del remitente
- URI de spam y phishing y direcciones de correo electrónico
- Spam Object checksums
- Reglas heurísticas dinámicas

Protección Outbreak
Lista gris para direcciones IPv4, IPv6 y cuentas de correo electrónico (Greylisting)
Reputación local del remitente (basada en IPv4, IPv6 y End Point ID-based)
Análisis de comportamiento (Behavioral Analysis)
Inspección profunda del encabezado del correo electrónico (Deep Email Header Inspection)
Acción flexible y perfiles de notificación
URI de spam de terceros y listas negras en tiempo real (SURBL / RBL)
Chequeo de reputación de ip´s en múltiples RBLs [DNSBL]
Categoría completa FortiGuard URL Filtering (FortiGuard URL Filtering)
Cuarentena
Escaneo PDF y Análisis de Imagen
Listas negras y con excepciones a nivel global, de dominio y de usuario (Black/White Lists)
Filtrado bayesiano (Bayesian Statistic Filtering)
Detección de boletines y boletines sospechosos (Newsletter detection)

Protección basada en Antivirus:

Este servicio también analiza todos los documentos adjuntos de cada correo y cada paquete en cada tráfico relacionado en la transacción.
Servicio FortiGuard Antivirus
Acciones de cuarentena, reempaquetado, reemplazo y monitoreo
Escaneo de archivos anidados (Nested Archive Scanning)
Detección de malware
Emulación de código a bordo

Protección basada en contenido:

Realiza el filtro de todos los buzones revisando cada contenido archivo que contiene el Correo antes que le llegue al usuario destinatario.

Filtrado basado en diccionario
Diccionarios predefinidos HIPAA, GLBA y SOX
Filtrar por tipo de archivo adjunto y extensiones potencialmente inseguras o ejecutables
Filtrado de palabras prohibidas

Protección basada en Sistema:

Inspección para mensajes entrantes y salientes
Protección de denegación de servicio
Protección Ataque de dirección del destinatario
Protección contra epidemias de Spam
Límite de velocidad de mensajes entrantes y salientes
Cifrado de dirección del remitente falsificado
Cifrado basado en identidad para entrega push / pull de mensajes cifrados
Verificación inversa de DNS (Anti-Spoofing)
Inspección por usuario utilizando atributos LDAP en una base por política (dominio)
Cumplimiento de RFC por correo electrónico
Mantiene la lista de reputación del remitente local basada en:
- Marco de políticas del remitente (SPF)
- Correo identificado claves de dominio (DKIM)
- Soporte para protocolos criptográficos fuertes, incluidos HTTPS, SMTPS, SSH, IMAPS y POP3S

El servicio funciona en Alta disponibilidad (HA) con modo de sincronización de configuración (modo maestro de configuración y esclavo) permitiendo la detección y notificación de fallas de los dispositivos a través del monitoreo del estado del enlace, conmutación por error y soporte de interfaz redundante.

Las Políticas de Contraseñas actuales para las cuentas del dominio: *metrosalud.gov.co* definidas son:

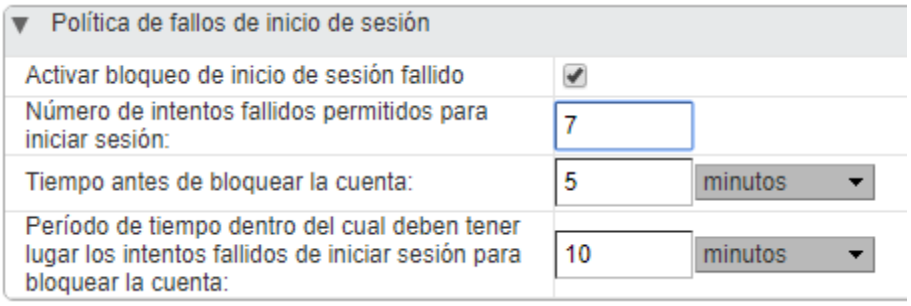
•Longitud mínima: 9 caracteres.
•Mínimo un carácter numérico: como Dígitos [0 - 9]

•Mínimo un carácter alfanumérico: Pueden ser caracteres minúscula [a – z] ó mayúsculas [A - Z]
•Mínimo un carácter especial como por ejemplo: Pueden utilizar los siguientes: [* . ! # & % $]
•Un carácter en mayúsculas [A - Z]
•Antigüedad: No se deben de repetir ninguna de las ultimas 15 contraseñas

Los parámetros asociados a: "**Políticas de Contraseñas" son personalizables**, si gustan realizar algún cambio nos lo pueden indicar para aumentar o disminuir algún valor el cual solo aplicara para el dominio utilizado y todas las cuentas de correo que dependan de él.

Políticas de fallos de inicio de sesión:

La política de fallos de inicio de sesión es la siguiente: Si en 10 minutos se registran 7 intentos fallidos la cuenta de correo cambia de estado de Activo a lockout/Bloqueo, si una cuenta cae en este estado, los mensajes continuaran siendo recibidos. Esta política es personalizable.



También podemos habilitar el cambio periódico de la contraseña, este cambio se debe de realizar a través del portal web (https://webmail.une.net.co/) no aplica por cliente de correo (Ej.: MS Outlook), si el servicio no es accedido por medio del sitio web puede generar alto impacto en la organización.

Temas de extensiones y adjuntos

La plataforma de seguridad por donde pasan los mensajes entrantes y salientes utiliza perfiles de contenido, donde podemos personalizar uno para el dominio: ***metrosalud.gov.co*** si así lo requieren

El control actual básicamente es aplicado sobre extensiones ejecutables en varios grupos como por ejemplo: ActiveX, visual Basic, JavaScript, extensiones para Windows y personalizadas.

Habilita...	Filtro de Archivos
●	executable_activex
●	java
●	javascript
●	executable_vbs
●	executable_vba
●	executable_windows
●	extensiones

Consideramos que existen mejoras a nivel de seguridad que se pueden implementar, ponemos a su disposición la personalización de dichas configuraciones, en este orden de ideas podemos:

- Crear un perfil de contenido solo para los buzones de correo del dominio: ***metrosalud.gov.co*** y bloquear las extensiones que nos comparten.
- Crear reglas personalizadas contra los mensajes que ingresan y son catalogados como sospechosos, es decir, bloquear todo lo que es catalogado como "spam" y evitar que llegue a la bandeja de entrada rebotando al emisor un mensaje de no entrega.
- Envío de reportes con el filtrado de mensajes para el dominio: ***metrosalud.gov.co***
- Afinar las políticas de contraseña a todos los usuarios.
- Bloqueo de cadenas de texto mediante diccionarios personalizados
- Implementar cambios de contraseña obligatorios.
- Evaluar cambios que nos soliciten y poner a su disposición la implementación de los mismos siempre y cuando sea viable.

Anexo 12. SEGURIDAD WIFI

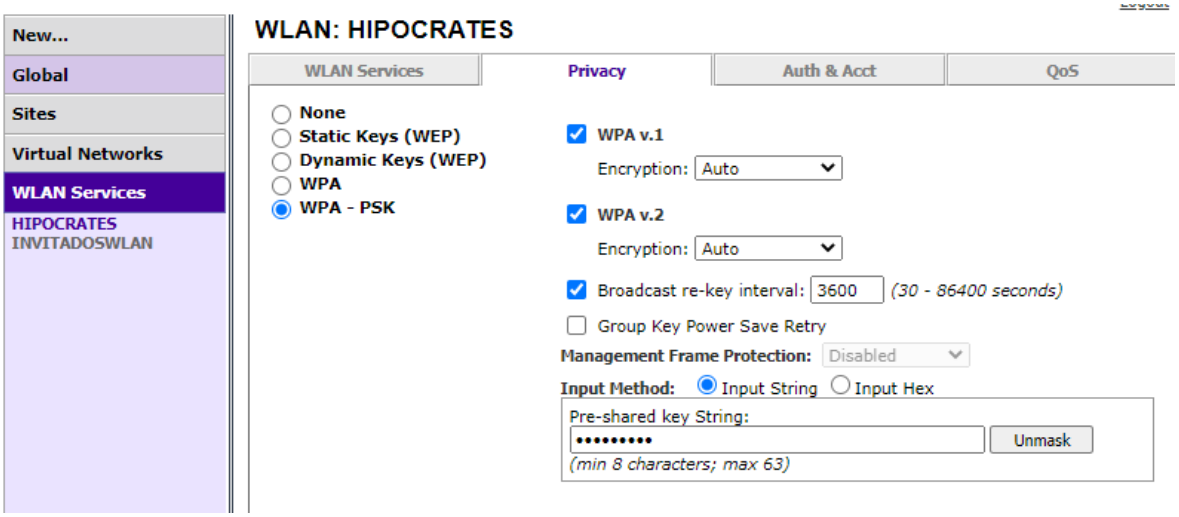
Para Sacatin San Cristobal y Belén se tiene red Wifi habilitada para conexión de equipos de Metrosalud.

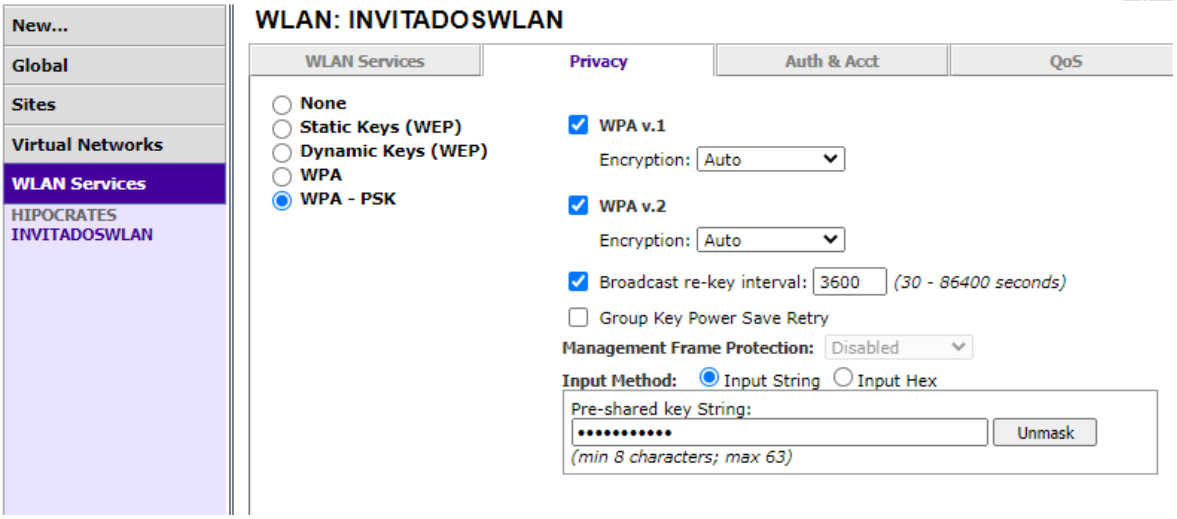
Existen dos SSID HIPOCRATES E INVITADOS SACATIN y en Belén se llama Metrosalud las dos redes HIPOCRATES Y METROSALUD son únicamente para conexión de equipos portátil que estén dentro del dominio de Metrosalud. Local.

La red INVITADOS-SACATIN es una res como su nombre lo dice de invitados para persona Externas o conexión de equipos móvil de los empleados del edificio es una red con una VLAN aparta y un acceso diferente de internet para que el consumo de navegación no perjudique el rendimiento de la red corporativa.

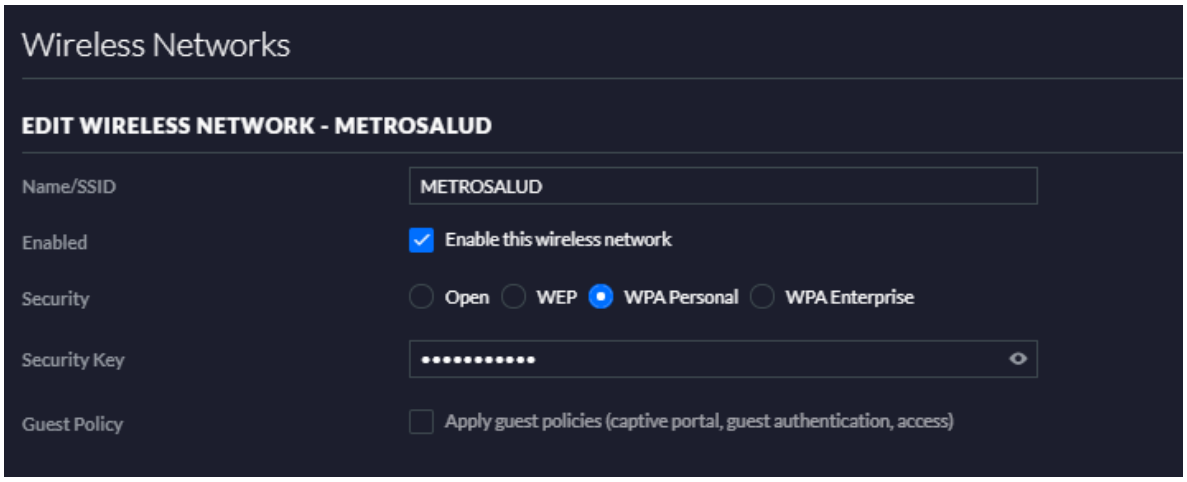
Todas los SSID están protegidas con una configuración de seguridad de WPA con encriptación PKS esto nos asegura que ningún escaneo de redes externo a METROSALUD pueda interceptar las señales y visualizar el tráfico de datos que pasa por la red WIFI habilitadas.

Se muestra evidencias de pantallazos de las configuraciones mencionadas





Esta mismo aplica para la red de San Cristobal para la red de Belén es otra soluciona de WIFI llamada UNIFI y mostramos la imagen de configuración



Es una seguridad de WPA personal donde todos los dispositivos comparten esta clave cifrada y antes de realizar una conexión valida que sea la correcta para certificar la conexión igual esta señal va encriptada de punta a punta para proteger el tráfico de intercepciones no autorizadas.

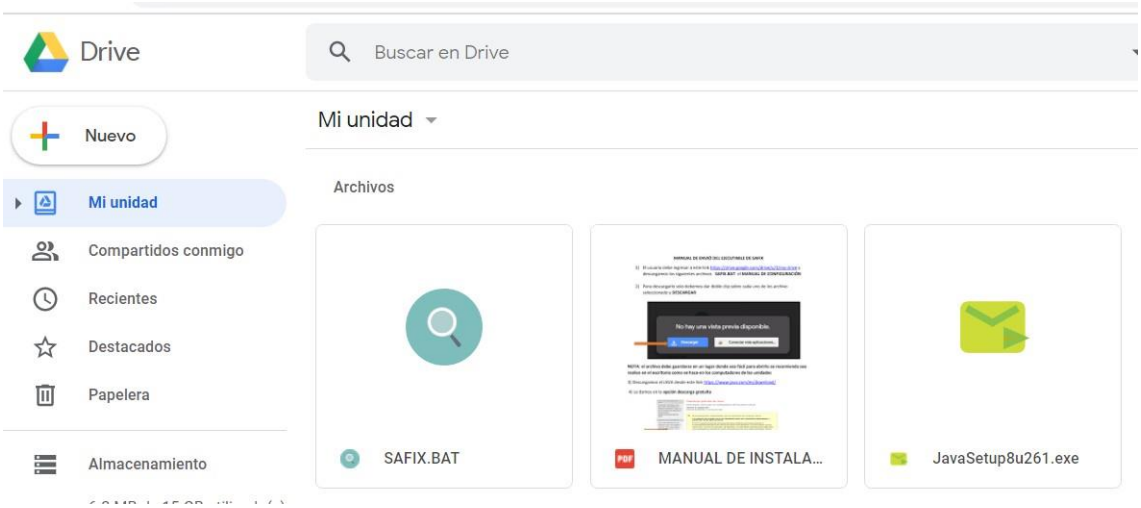
Anexo 13. MANUAL ACCESO SAFIX PÚBLICO

ENVÍO DEL EJECUTABLE DE SAFIX

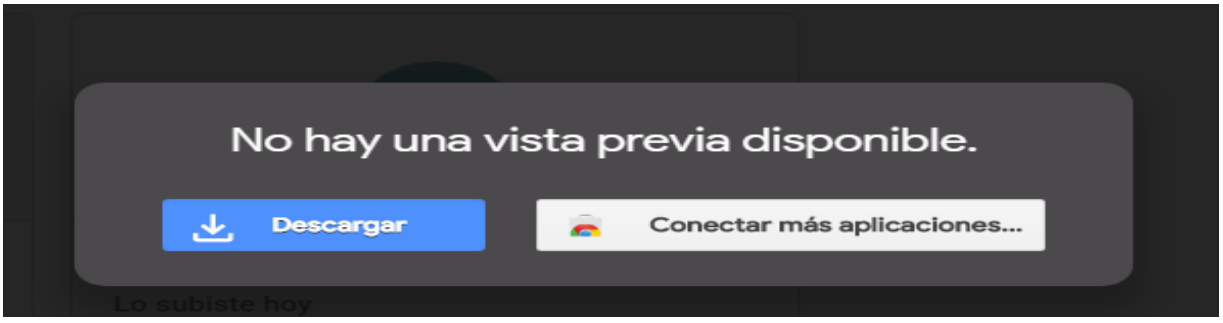
1) El usuario debe ingresar a este link https://drive.google.com/drive/folders/1Xll0LdiWKwwzlJrpDNp2Dk3YGH5eUbLr?usp=sharing

Descargamos los siguientes archivos y seguimos cada uno de los pasos que dice el manual
MANUAL DE CONFIGURACIÓN

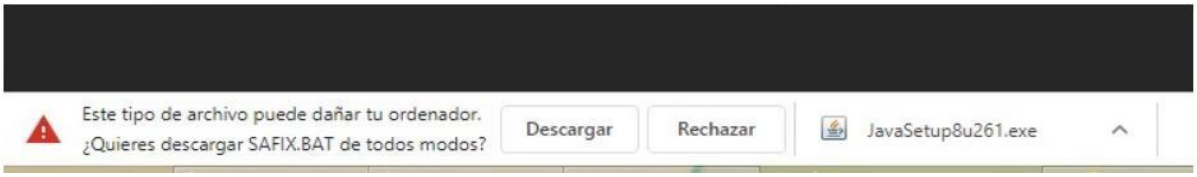
1) **SAFIX.BAT**
2) **javasetup8u261.exe**



2) Para descargar los archivo solo debemos dar doble clip sobre cada uno de los archivo seleccionado y darle la opción **DESCARGAR**

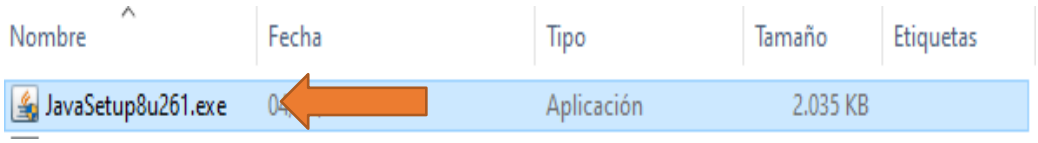


Si sale este mensaje cuando estemos descargando los archivos le damos DESCARGAR

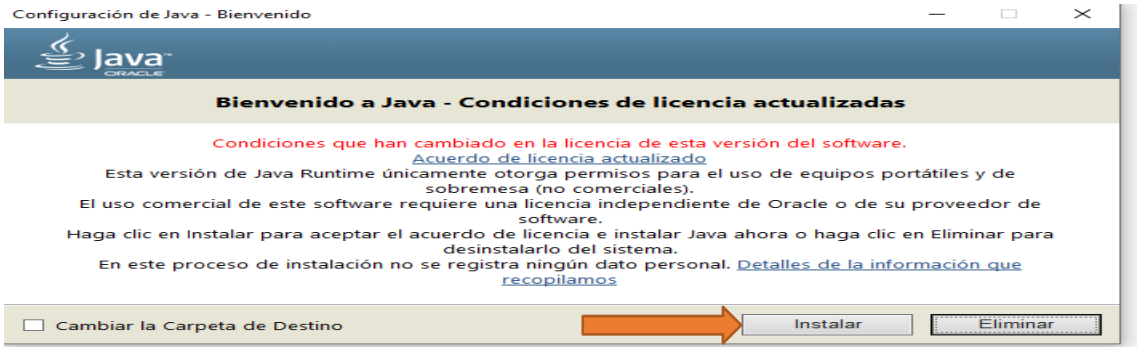


NOTA: el archivo SAFIX.BAT debe guardarse en un lugar donde sea fácil para abrirlo se recomienda guardarlo en el escritorio como se hace en los computadores de las unidades

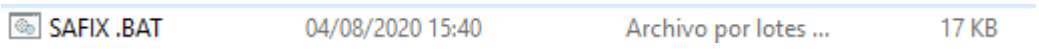
3) Después de descargar todos los archivos procedemos a instalar el que dice **javasetup8u261.exe** dando doble clip sobre el programa



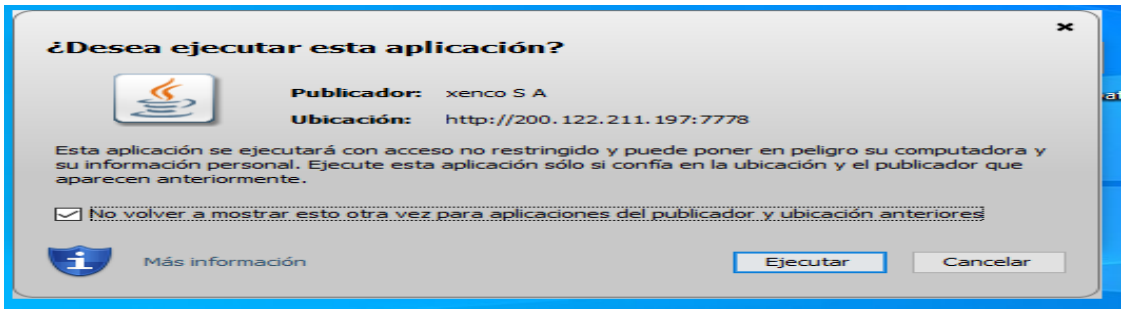
4) Le damos **INSTALAR** aquí el programa comienza el proceso de instalación



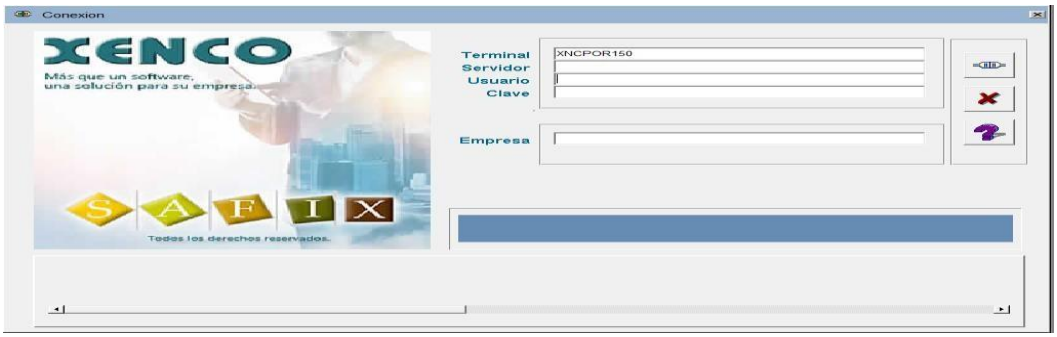
5) Luego abrimos el archivo con el nombre de **SAFIX .BAT** que descargamos en el **PASO 2**



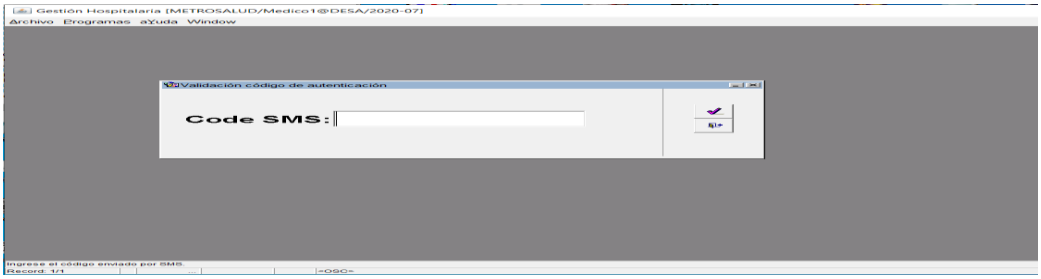
Marcamos **NO VOLVER A MOSTRAR** y le damos **EJECUTAR**



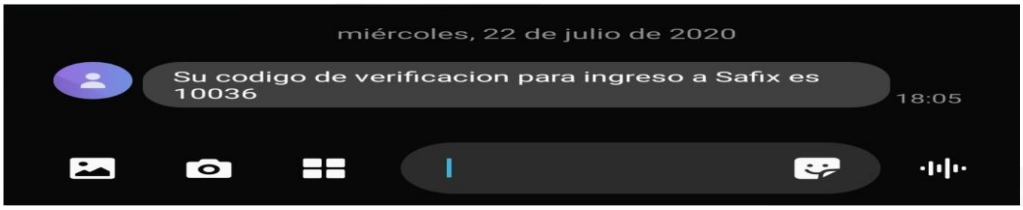
6) Al abrir la conexión se carga por defecto la maquina real desde la que se están conectando.



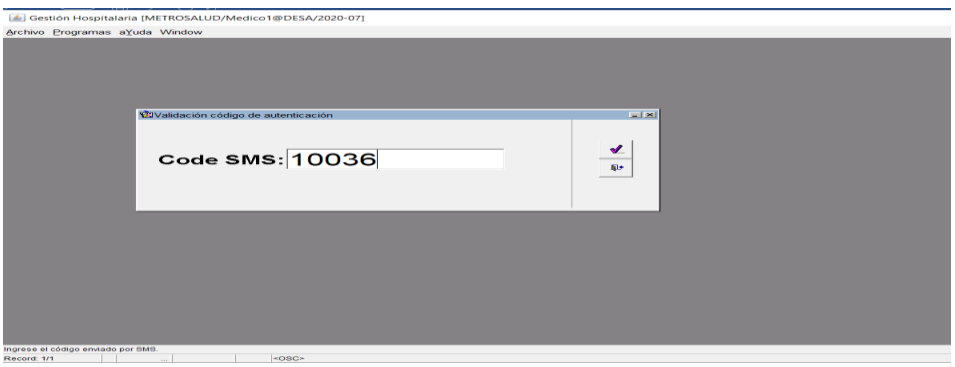
7) Automáticamente se abre la siguiente pantalla para que el usuario ingrese el código enviado a su número de celular.



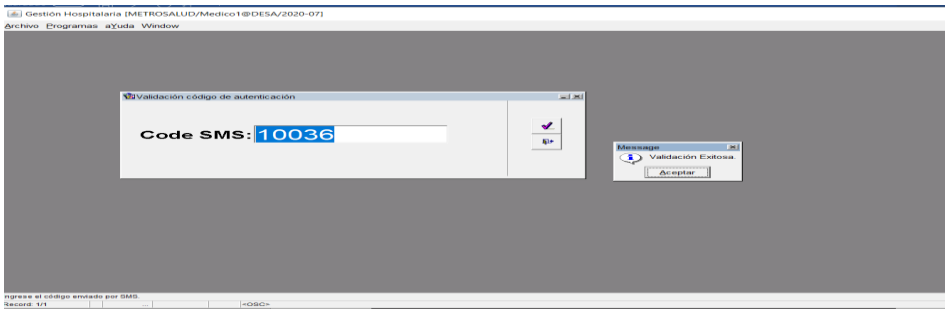
8) Al usuario le llega un mensaje de texto con el código de ingreso



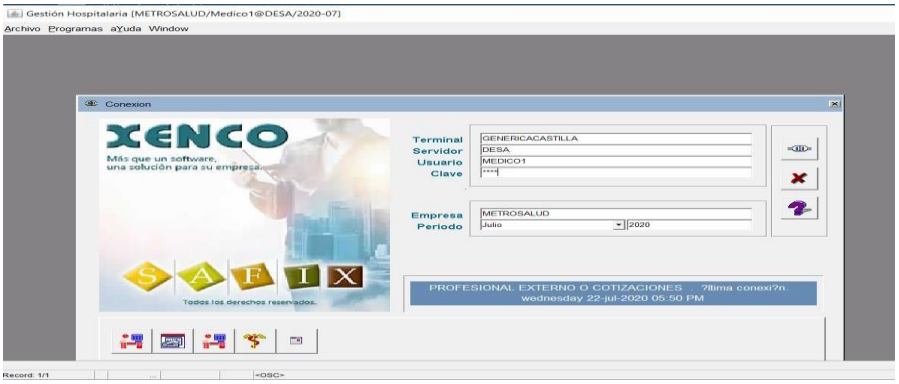
9) El usuario ingresa el código recibido



10) El sistema valida el que el código coincida con el enviado



11) Si la validación es exitosa el sistema regresa a la pantalla de módulos para que el usuario ingrese al módulo deseado



NOTA: se recomienda que el navegador predeterminado sea
INTERNET EXPLORE

LINK CONSUTA DE RESULTADO DE LABORATORIO

http://laboratorio.metrosalud.gov.co:81/login.aspx?ReturnUrl=%2fDefaultMedico.aspx

Anexo 14. CONTROL ACCESO CENTROS DE DATOS

Metrosalud cuenta en cada Centro de salud o Unidad hospitalaria con mínimo 1 Centros de datos estos se tienen como punto de concentración del cableado estructurado de red de datos, telefonía y proveedor de servicios de internet y conectividad. Estos centros de su seguridad y custodia de los dispositivos que se encuentran que en cada uno, son responsables los directores y coordinadores. En SACATIN se cuenta con 5 centros de datos y un data center, todos son manejados desde sistemas de información.

DATA CENTER: este cuenta con parte de la infraestructura importante para la ESE por tal motivo se controla el ingreso a este lugar con un control de acceso biométrico donde se registra la hora, fecha y la persona esto con el fin de no permitir el ingreso a personas no autorizadas para estar en ese lugar.

CENTRO DE DATOS: En ellos están solo el cableado de red y dispositivos activos que permiten la conectividad de los servicios de internet y telefonía. En algunos centros de salud se encuentra un servidor que solo es para una replica del DA (Directorio Activo) para agilizar la conexión de los usuarios y distribuir la carga de los recursos que consumen los usuarios, evitando la congestión o saturación de los canales MPLS (Multiprotocol Label Switching) que puedan afectar el rendimiento de los aplicativos corporativos.

No se tiene registro de acceso en los Centros de Datos porque resulta difícil porque no se tiene una persona disponibles contante que esté pendiente de dar acceso y documentar en planilla cada ingreso, además no se es necesario por que todos los Rack están en custodia a puerta cerrada o alguno están el consultorios o partes donde difícilmente pueda llegar un externo a manipular estos dispositivos, además que no hay ni aplicativos ni información cencibel en estos lugares y los dispositivos no son de fácil manipulación o extracción.

Anexo 15. CATÀLOGO DE SERVICIOS

En este documento se dan a conocer los servicios e infraestructura que gestiona la dirección de sistemas de información para apoyar la operación del negocio.

A.CONECTIVIDAD

Internet

Descripción: Acceso a la red de internet la cual permite navegar en sitios web, consultar y descargar información de interés.
Características Técnicas: Ancho de banda de 60 Mbps Sacatin, 12 Mbps Unidad Hospitalarias y centros de Salud todos en Fibra óptica Redundante en tecnología SD-Wan (Canal principal de 200 Mbps, Canal de internet 120 Mbps)
Categoría: Conectividad
Responsable: Tecnologías y Sistemas de la Información Infraestructura (proveedor TIGO-UNE)
Usuario objetivo: Todas las sedes de Metrosalud y Programas
Horario prestación del servicio: 24 horas
Contacto de Soporte: Soporte al Servicio: Tecnología y Sistemas de la Información, Ext. 1911 opción 1 Email: mesadeayudasistemas@metrosalud.gov.co
Horario de soporte al servicio: lunes a jueves de 7:00 a.m. – 5:00 p.m. viernes de 7:00 a.m. – 4:00 p.m. Sábados y domingos 7:00 a.m. – 3:00 p.m.

WiFi

Descripción: Acceso a la red de internet de forma inalámbrica a través de dispositivos móviles y computadores portátiles SSID INVITADOS SACATIN para uso público los demás solo institucionales
Características Técnicas: Permite los estándares 802.11b/g/n
Categoría: Conectividad
Responsable: Tecnologías y Sistemas de la Información Infraestructura
Usuario objetivo: Sacatin (SSID INVITADOS SACATIN - HIPOCRATES), Belen (SSID METROSALUD), San Cristobal (SSID HIPOCRATES), CISAM
Horario prestación del servicio: 24 horas
Contacto de Soporte: Soporte al Servicio: Tecnología y Sistemas de la Información, Ext. 1911 opción 1 Email: mesadeayudasistemas@metrosalud.gov.co
Horario de soporte al servicio: lunes a jueves de 7:00 a.m. – 5:00 p.m. viernes de 7:00 a.m. – 4:00 p.m. Sábados y domingos 7:00 a.m. – 3:00 p.m.

Intranet

Descripción: Acceso a la red interna de la institución para el uso de recursos locales restringidos.
Características Técnicas: Permite el uso de impresoras, scanners, carpetas compartidas, telefonía IP interna, sistemas de información específicos como apoyo a los procesos, entre otros recursos.
Categoría: Conectividad
Responsable: Tecnologías y Sistemas de la Información Infraestructura
Usuario objetivo: Funcionarios y contratistas
Horario prestación del servicio: 24 horas

Contacto de Soporte: Soporte al Servicio: Tecnología y Sistemas de la Información, Ext. 1911 opción 1 Email: mesadeayudasistemas@metrosalud.gov.co
Horario de soporte al servicio: lunes a jueves de 7:00 a.m. – 5:00 p.m. viernes de 7:00 a.m. – 4:00 p.m. Sábados y domingos 7:00 a.m. – 3:00 p.m.

Conexión VPN

Descripción: Acceso seguro a la red interna de la institución desde cualquier lugar a través de internet..
Características Técnicas: La conexión por VPN o red privada virtual, establece una conexión cifrada de la información a través IPSec desde redes externas a la intranet institucional
Categoría: Conectividad
Responsable: Tecnologías y Sistemas de la Información Infraestructura (Proveedor TIGO – UNE)
Usuario objetivo: Funcionarios y contratistas
Horario prestación del servicio: 24 horas
Contacto de Soporte: Soporte al Servicio: Tecnología y Sistemas de la Información, Ext. 1911 opción 1 Email: mesadeayudasistemas@metrosalud.gov.co
Horario de soporte al servicio: lunes a jueves de 7:00 a.m. – 5:00 p.m. viernes de 7:00 a.m. – 4:00 p.m. Sábados y domingos 7:00 a.m. – 3:00 p.m.

B.COMUNICACIONES

Correo

Descripción: Servicio de correo web institucional como medio de comunicación electrónica para el intercambio de mensajes y documentos digitales.
Características Técnicas: Basado en Zimbra con un buzón de almacenamiento de 2 GB y acceso desde el cliente Microsoft Outlook o a través del navegador web.
Categoría: Comunicaciones
Responsable: Tecnologías y Sistemas de la Información Infraestructura (Proveedor TIGO - UNE)
Usuario objetivo: Funcionarios y programas institucionales
Horario prestación del servicio: 24 horas
Contacto de Soporte: Soporte al Servicio: Tecnología y Sistemas de la Información, Ext. 1911 opción 1 Email: mesadeayudasistemas@metrosalud.gov.co
Horario de soporte al servicio: lunes a jueves de 7:00 a.m. – 5:00 p.m. viernes de 7:00 a.m. – 4:00 p.m. Sábados y domingos 7:00 a.m. – 3:00 p.m.

Chat

Descripción: Servicio de mensajería instantánea para atención en línea de consultas e inquietudes de usuarios sobre información institucional.
Características Técnicas: Basado en Open Fire Cliente Servidor.
Categoría: Comunicaciones
Responsable: Tecnologías y Sistemas de la Información Infraestructura
Usuario objetivo: Funcionarios
Horario prestación del servicio: 24 horas
Contacto de Soporte: Soporte al Servicio: Tecnología y Sistemas de la Información, Ext. 1911 opción 1 Email: mesadeayudasistemas@metrosalud.gov.co

Horario de soporte al servicio: lunes a jueves de 7:00 a.m. – 5:00 p.m. viernes de 7:00 a.m. – 4:00 p.m. Sábados y domingos 7:00 a.m. – 3:00 p.m.

Telefonía

Descripción: Servicio de comunicaciones telefónicas entre usuarios internos y externos de la institución.
Características Técnicas: Telefonía Análoga e IP.
Categoría: Comunicaciones
Responsable: Tecnologías y Sistemas de la Información Infraestructura (Proveedor AXEDE)
Usuario objetivo: Funcionarios y Contratistas
Horario prestación del servicio: 24 horas
Contacto de Soporte: Soporte al Servicio: Tecnología y Sistemas de la Información, Ext. 1911 opción 1 Email: mesadeayudasistemas@metrosalud.gov.co
Horario de soporte al servicio: lunes a jueves de 7:00 a.m. – 5:00 p.m. viernes de 7:00 a.m. – 4:00 p.m. Sábados y domingos 7:00 a.m. – 3:00 p.m.

Redes sociales

Descripción: Servicio web para fortalecer la comunicación entre la institución y la comunidad universitaria a través de redes sociales.
Características Técnicas: Publicación y respuesta a comentarios a través de redes sociales Facebook, Twitter e Instagram.
Categoría: Comunicaciones
Responsable: Planeación Oficina de Comunicaciones
Usuario objetivo: Usuarios servicios de salud
Horario prestación del servicio: 24 horas
Contacto de Soporte: Comunicaciones Email: mesadeayudacomunicaciones@metrosalud.gov.co
Horario de soporte al servicio: lunes a jueves de 7:00 a.m. – 5:00 p.m. viernes de 7:00 a.m. – 4:00 p.m.

Teleconferencia

Descripción: Adecuación de auditorios con Video-Beam, sistema de altavoces, micrófono, Computador y software
Características Técnicas: Software Cisco Webex Meeting suministrado por Minsalud.
Categoría: Comunicación
Responsable: Tecnologías y Sistemas de la Información Infraestructura
Usuario objetivo: Todos los Servidores de Metrosalud
Horario prestación del servicio: 24 horas
Soporte al Servicio: Tecnología y Sistemas de la Información, Ext. 1911 opción 1 Email: mesadeayudasistemas@metrosalud.gov.co
Horario de soporte al servicio: lunes a jueves de 7:00 a.m. – 5:00 p.m. viernes de 7:00 a.m. – 4:00 p.m. Sábados y domingos 7:00 a.m. – 3:00 p.m.

C.SEGURIDAD

Seguridad Perimetral

Descripción: Gestión de la administración y configuración centralizada de la seguridad de la red institucional (internet, intranet y correo).
Características Técnicas: Sistema de seguridad contratado con TIGO-UNE conformado por: Firewall, VPN Client to Site, Web Control Filtering, IDS/IPS, App Control, Antivirus GateWay
Categoría: Seguridad
Responsable: Tecnologías y Sistemas de la Información Infraestructura (Proveedor TIGO - UNE)
Usuario objetivo: Todos los usuarios servicios TI
Horario prestación del servicio: 24 horas
Soporte al Servicio: Tecnología y Sistemas de la Información, Ext. 1911 opción 1
Email: mesadeayudasistemas@metrosalud.gov.co
Horario de soporte al servicio: lunes a jueves de 7:00 a.m. – 5:00 p.m. viernes de 7:00 a.m. – 4:00 p.m. Sábados y domingos 7:00 a.m. – 3:00 p.m.

Video Vigilancia

Descripción: Administración y mantenimiento del sistema de video vigilancia de las instalaciones de la institución
Características Técnicas: Compra, instalación, configuración, gestión de mantenimientos preventivos y correctivos de las diferentes cámaras ubicadas en los diferentes espacios de las sedes de Metrosalud
Categoría: Seguridad
Responsable: Tecnologías y Sistemas de la Información Infraestructura
Usuario objetivo: Todas las sedes de Metrosalud
Horario prestación del servicio: 24 horas
Soporte al Servicio: Tecnología y Sistemas de la Información, Ext. 1911 opción 1
Email: mesadeayudasistemas@metrosalud.gov.co
Horario de soporte al servicio: lunes a jueves de 7:00 a.m. – 5:00 p.m. viernes de 7:00 a.m. – 4:00 p.m. Sábados y domingos 7:00 a.m. – 3:00 p.m.

Software Antivirus

Descripción: Software Antivirus Kaspersky que detecta y elimina virus informáticos y muchos otros tipos de amenazas informáticas incluyendo el Ransomware.
Características Técnicas: Cliente instalado en todas las estaciones que se actualiza desde un servidor central
Categoría: Seguridad
Responsable: Tecnologías y Sistemas de la Información Infraestructura
Usuario objetivo: Todos los usuarios de PC en Metrosalud
Horario prestación del servicio: 24 horas
Soporte al Servicio: Tecnología y Sistemas de la Información, Ext. 1911 opción 1
Email: mesadeayudasistemas@metrosalud.gov.co
Horario de soporte al servicio: lunes a jueves de 7:00 a.m. – 5:00 p.m. viernes de 7:00 a.m. – 4:00 p.m. Sábados y domingos 7:00 a.m. – 3:00 p.m.

Software de Backup

Descripción: Software Veeam-Backup que realiza copias de todos servidores alojados en la nube privada de Metrosalud.
Características Técnicas: Software Veeam-Backup con copias Padre-Hijo-Abuelo

Categoría: Seguridad
Responsable: Tecnologías y Sistemas de la Información Infraestructura
Usuario objetivo: Todos los Servidores alojados en la nube privada de Metrosalud
Horario prestación del servicio: 24 horas
Soporte al Servicio: Tecnología y Sistemas de la Información, Ext. 1911 opción 1
Email: mesadeayudasistemas@metrosalud.gov.co
Horario de soporte al servicio: lunes a jueves de 7:00 a.m. – 5:00 p.m. viernes de 7:00 a.m. – 4:00 p.m. Sábados y domingos 7:00 a.m. – 3:00 p.m.

D. SOLUCIONES INFRAESTRUCTURA

Equipos de computo

Descripción: Adquisición, instalación, configuración y mantenimientos preventivos y correctivos de hardware y software de los equipos asignados a personal administrativo y operativo de la institución.
Características Técnicas: La administración de los equipos incluye la compra, instalación, configuración, gestión de mantenimientos preventivos, correctivos de hardware, software y garantías de los equipos de cómputo.
Categoría: Gestión de Soluciones infraestructura
Responsable: Tecnologías y Sistemas de la Información.
Usuario objetivo: Funcionarios y Contratistas
Horario prestación del servicio: 24 horas
Soporte al Servicio: Tecnología y Sistemas de la Información, Ext. 1911 opción 1
Email: mesadeayudasistemas@metrosalud.gov.co
Horario de soporte al servicio: lunes a jueves de 7:00 a.m. – 5:00 p.m. viernes de 7:00 a.m. – 4:00 p.m. Sábados y domingos 7:00 a.m. – 3:00 p.m.

Digiturnos

Descripción: Software y hardware para la gestión de turnos en los servicios de consulta externa y ayudas diagnósticas.
Características Técnicas: Televiso, mini-PC y software web (proveedor Dinámica y Desarrollo).
Categoría: Gestión de Soluciones infraestructura
Responsable: Tecnologías y Sistemas de la Información.
Usuario objetivo: Funcionarios y Contratistas
Horario prestación del servicio: 24 horas
Soporte al Servicio: Tecnología y Sistemas de la Información, Ext. 1911 opción 1
Email: mesadeayudasistemas@metrosalud.gov.co
Horario de soporte al servicio: lunes a jueves de 7:00 a.m. – 5:00 p.m. viernes de 7:00 a.m. – 4:00 p.m. Sábados y domingos 7:00 a.m. – 3:00 p.m.

Recursos de impresión y escaneo

Descripción: Administración y mantenimiento de impresoras, Escaner y suministros para el servicio de impresión por parte de las dependencias.
Características Técnicas: Impresoras multifuncionales departamentales (Proveedor Sertecopy) impresión POST infraestructura propia
Categoría: Gestión de Soluciones infraestructura
Responsable: Tecnologías y Sistemas de la Información y proveedor Sertecopy.

Usuario objetivo: Funcionarios y Contratistas
Horario prestación del servicio: 24 horas
Soporte al Servicio: Tecnología y Sistemas de la Información, Ext. 1911 opción 1
Email: mesadeayudasistemas@metrosalud.gov.co – Sertecopy 444 45 00 info@sertecopy.com
Horario de soporte al servicio: lunes a jueves de 7:00 a.m. – 5:00 p.m. viernes de 7:00 a.m. – 4:00 p.m. Sábados y domingos 7:00 a.m. – 3:00 p.m.

E. SOPORTE A USUARIOS

Soporte técnico hardware y software

Descripción: Brindar el servicio de soporte técnico de hardware y software a los requerimientos solicitados por las diferentes dependencias de la institución.
Características Técnicas: Gestión de solicitudes de reporte a través de la mesa de ayuda realizados por las diferentes dependencias.
Categoría: Soporte a usuarios
Responsable: Tecnologías y Sistemas de la Información y proveedor Sertecopy.
Usuario objetivo: Funcionarios y Contratistas
Horario prestación del servicio: 24 horas
Soporte al Servicio: Tecnología y Sistemas de la Información, Ext. 1911 opción 1
Email: mesadeayudasistemas@metrosalud.gov.co
Horario de soporte al servicio: lunes a jueves de 7:00 a.m. – 5:00 p.m. viernes de 7:00 a.m. – 4:00 p.m. Sábados y domingos 7:00 a.m. – 3:00 p.m.

Soporte Redes de datos

Descripción: Brindar el servicio de soporte técnico de las redes internas y la conectividad entre las sedes y a los requerimientos solicitados por las diferentes dependencias de la institución.
Características Técnicas: Gestión de las redes internas y los canales de comunicación de las sedes externa con proveedor contratado TIGO-UNE.
Categoría: Soporte a usuarios
Responsable: Tecnologías y Sistemas de la Información y proveedor TIGO-UNE.
Usuario objetivo: Funcionarios y Contratistas
Horario prestación del servicio: 24 horas
Soporte al Servicio: Tecnología y Sistemas de la Información, Ext. 1911 opción 1
Email: mesadeayudasistemas@metrosalud.gov.co
Horario de soporte al servicio: lunes a jueves de 7:00 a.m. – 5:00 p.m. viernes de 7:00 a.m. – 4:00 p.m. Sábados y domingos 7:00 a.m. – 3:00 p.m.

F. SISTEMAS DE INFORMACION

Software de Ofimática

Descripción: Soporte en las aplicaciones Word, Excel, Outlook, Power point y Access Acceso entre otros.
Categoría: Sistema de información.
Responsable: Tecnologías y Sistemas de la Información
Usuario objetivo: Funcionarios y Contratistas
Horario prestación del servicio: horas de oficina

Soporte al Servicio: Tecnología y Sistemas de la Información, Ext. 1911 opción 1
Email: mesadeayudasistemas@metrosalud.gov.co
Horario de soporte al servicio: lunes a jueves de 7:00 a.m. – 5:00 p.m. viernes de 7:00 a.m. – 4:00 p.m. Sábados y domingos 7:00 a.m. – 3:00 p.m.

Página web e intranet

Descripción: Sitio web institucional que integra información sobre noticias, eventos de interés, políticas, normatividad y acceso unificado a servicios como correo electrónico, sistemas de información, herramientas de apoyo a la gestión administrativa
Categoría: Sistema de información.
Responsable: Tecnologías y Sistemas de la Información
Usuario objetivo: Funcionarios y Contratistas
Horario prestación del servicio: 24 horas
Soporte al Servicio: Tecnología y Sistemas de la Información, Ext. 1911 opción 1
Email: mesadeayudasistemas@metrosalud.gov.co
Horario de soporte al servicio: lunes a jueves de 7:00 a.m. – 5:00 p.m. viernes de 7:00 a.m. – 4:00 p.m. Sábados y domingos 7:00 a.m. – 3:00 p.m.

Sistema de información ERP (Safix)

Descripción: Sistema de apoyo a la gestión administrativa y financiera compuesto por Admisiones, Facturacion, Gestión Hospitalaria, Cartera, Tesorería, Contabilidad, costos, activos fijos, Inventarios, Presupuesto, Nomina, Cuadro de turnos, Safix Web etc.
Categoría: Sistema de información.
Responsable: Tecnologías y Sistemas de la Información
Usuario objetivo: Funcionarios y Contratistas
Horario prestación del servicio: 24 horas
Soporte al Servicio: Tecnología y Sistemas de la Información, Ext. 1911 opción 2
Email: mesadeayudasistemas@metrosalud.gov.co
Horario de soporte al servicio: lunes a jueves de 7:00 a.m. – 5:00 p.m. viernes de 7:00 a.m. – 4:00 p.m. Sábados y domingos 7:00 a.m. – 3:00 p.m.

Sistemas de información Clínico (Safix)

Descripción: Sistema de información Clínico compuesto por los diferentes tipos de Historia clínica y Safix Web.
Categoría: Sistema de información.
Responsable: Tecnologías y Sistemas de la Información
Usuario objetivo: Funcionarios y Contratistas
Horario prestación del servicio: 24 horas
Soporte al Servicio: Tecnología y Sistemas de la Información, Ext. 1911 opción 2
Email: mesadeayudasistemas@metrosalud.gov.co
Horario de soporte al servicio: lunes a jueves de 7:00 a.m. – 5:00 p.m. viernes de 7:00 a.m. – 4:00 p.m. Sábados y domingos 7:00 a.m. – 3:00 p.m.

Software Sevenet

Descripción: Software para la gestión documental.
Categoría: Sistema de información.

Responsable: Tecnologías y Sistemas de la Información
Usuario objetivo: Funcionarios y Contratistas
Horario prestación del servicio: horas de oficina
Soporte al Servicio: Gestión documental, Ext. 1141 Email: mesadeayudagdocumental@metrosalud.gov.co
Horario de soporte al servicio: lunes a jueves de 7:00 a.m. – 5:00 p.m. viernes de 7:00 a.m. – 4:00 p.m.

Software Moodle

Descripción: Sistema de apoyo a los docentes a través del cual se crea un ambiente virtual que permite la publicación de contenidos, actividades, evaluaciones, foros, etc. Todos estos recursos en línea están soportados bajo la plataforma Moodle.
Categoría: Sistema de información.
Responsable: Tecnologías y Sistemas de la Información (técnico), Comunicaciones y Gestion Humana (contenido)
Usuario objetivo: Funcionarios y Contratistas
Horario prestación del servicio: 24 horas
Soporte al Servicio: Tecnología y Sistemas de la Información, Ext. 1911 opción 2 Email: mesadeayudasistemas@metrosalud.gov.co, mesadeayudacomunicaciones@metrosalud.gov.co, mesadeayudatalentohumano@metrosalud.gov.co
Horario de soporte al servicio: lunes a jueves de 7:00 a.m. – 5:00 p.m. viernes de 7:00 a.m. – 4:00 p.m. Sábados y domingos 7:00 a.m. – 3:00 p.m.

Directorio Activo

Descripción: Sistema de administración y gestión centralizada de las cuentas de usuarios, utilizadas para el acceso unificado a los distintos servicios y sistemas de información institucionales.
Categoría: Sistema de información.
Responsable: Tecnologías y Sistemas de la Información
Usuario objetivo: Funcionarios y Contratistas
Horario prestación del servicio: 24 horas
Soporte al Servicio: Tecnología y Sistemas de la Información, Ext. 1911 opción 1 Email: mesadeayudasistemas@metrosalud.gov.co
Horario de soporte al servicio: lunes a jueves de 7:00 a.m. – 5:00 p.m. viernes de 7:00 a.m. – 4:00 p.m. Sábados y domingos 7:00 a.m. – 3:00 p.m.

Software Mesa de ayuda

Descripción: Sistema para registro de solicitudes de soporte técnico al grupo de Tecnologías y Sistemas de información, Sistemas, Gestión Documental, Gestión Humana, comunicaciones etc.
Categoría: Sistema de información.
Responsable: Tecnologías y Sistemas de la Información
Usuario objetivo: Funcionarios y Contratistas
Horario prestación del servicio: 24 horas
Soporte al Servicio: Tecnología y Sistemas de la Información, Ext. 1911 opción 1 Email: mesadeayudasistemas@metrosalud.gov.co,

mesadeayudacomunicaciones@metrosalud.gov.co,
mesadeayudatalentohumano@metrosalud.gov.co,
mesadeayudagdocumental@metrosalud.gov.co ,
mesadeayudariesgos@metrosalud.gov.co,
mesadeayudaalmacen@metrosalud.gov.co
Horario de soporte al servicio: lunes a jueves de 7:00 a.m. – 5:00 p.m. viernes de 7:00 a.m. – 4:00 p.m. Sábados y domingos 7:00 a.m. – 3:00 p.m.

Sistema administración de equipos biomédicos AM

Descripción: Sistema de administración y gestión centralizada de los activos fijos hospitalarios, utilizadas para registrar la hoja de vida de los equipos biomédicos.
Categoría: Sistema de información.
Responsable: Tecnologías y Sistemas de la Información – Ingeniera Biomédica
Usuario objetivo: Funcionarios y Contratistas
Horario prestación del servicio: 24 horas
Soporte al Servicio: Tecnología y Sistemas de la Información, Ext. 1911 opción 1
Email: mesadeayudasistemas@metrosalud.gov.co
Horario de soporte al servicio: lunes a jueves de 7:00 a.m. – 5:00 p.m. viernes de 7:00 a.m. – 4:00 p.m. Sábados y domingos 7:00 a.m. – 3:00 p.m.

Software gestión SIG Almera

Descripción: Sistema Integrado de Gestión de Calidad.
Categoría: Sistema de información.
Responsable: Tecnologías y Sistemas de la Información – Planeacion
Usuario objetivo: Funcionarios y Contratistas
Horario prestación del servicio: 24 horas
Soporte al Servicio: Tecnología y Sistemas de la Información, Ext. 1911 opción 1
Email: mesadeayudasistemas@metrosalud.gov.co
Horario de soporte al servicio: lunes a jueves de 7:00 a.m. – 5:00 p.m. viernes de 7:00 a.m. – 4:00 p.m. Sábados y domingos 7:00 a.m. – 3:00 p.m.

Software Sivigila

Descripción: El Sistema de Salud Pública (SIVIGILA) tiene como responsabilidad el proceso de observación y análisis objetivo, sistemático y constante de los eventos en salud, el cual sustenta la orientación, planificación, ejecución, seguimiento y evaluación de la práctica de la salud pública.
Categoría: Sistema de información.
Responsable: Ministerio de Salud
Usuario objetivo: Funcionarios y Contratistas
Horario prestación del servicio: 24 horas
Soporte al Servicio: Tecnología y Sistemas de la Información, Ext. 1911 opción 1
Email: mesadeayudasistemas@metrosalud.gov.co
Horario de soporte al servicio: lunes a jueves de 7:00 a.m. – 5:00 p.m. viernes de 7:00 a.m. – 4:00 p.m. Sábados y domingos 7:00 a.m. – 3:00 p.m.

Software Paiweb

Descripción: El Sistema de Salud Pública (PIWEB) tiene como responsabilidad el programa ampliado de inmunización de salud pública.
Categoría: Sistema de información.
Responsable: Ministerio de Salud
Usuario objetivo: Funcionarios y Contratistas
Horario prestación del servicio: 24 horas
Soporte al Servicio: Tecnología y Sistemas de la Información, Ext. 1911 opción 1
Email: mesadeayudasistemas@metrosalud.gov.co
Horario de soporte al servicio: lunes a jueves de 7:00 a.m. – 5:00 p.m. viernes de 7:00 a.m. – 4:00 p.m. Sábados y domingos 7:00 a.m. – 3:00 p.m.

Ambientes de pruebas, desarrollo

Descripción: Ambientes de Prueba y desarrollo del Sistema de apoyo a la gestión administrativa, financiera y Clínica Safix.
Categoría: Sistema de información.
Responsable: Tecnologías y Sistemas de la Información
Usuario objetivo: Funcionarios y Contratistas
Horario prestación del servicio: 24 horas
Soporte al Servicio: Tecnología y Sistemas de la Información, Ext. 1911 opción 2
Email: mesadeayudasistemas@metrosalud.gov.co
Horario de soporte al servicio: lunes a jueves de 7:00 a.m. – 5:00 p.m. viernes de 7:00 a.m. – 4:00 p.m. Sábados y domingos 7:00 a.m. – 3:00 p.m.

Software de integración con otros sistemas Interoperabilidad

Descripción: Software y módulos de integración con otros sistemas de información como Savia, SERES (Dian), Living Lab, Omega (Laboratorio) etc.
Categoría: Sistema de información.
Responsable: Tecnologías y Sistemas de la Información
Usuario objetivo: Funcionarios y Contratistas
Horario prestación del servicio: 24 horas
Soporte al Servicio: Tecnología y Sistemas de la Información, Ext. 1911 opción 2
Email: mesadeayudasistemas@metrosalud.gov.co
Horario de soporte al servicio: lunes a jueves de 7:00 a.m. – 5:00 p.m. viernes de 7:00 a.m. – 4:00 p.m. Sábados y domingos 7:00 a.m. – 3:00 p.m.

G. GENERACION DE INFORMACION

Minería de Datos

Descripción: Plataforma de DataWare House en el que se puede realizar Inteligencia de negocios y minería de datos para apoyar la toma de decisiones de la alta gerencia
Categoría: Sistema de información.
Responsable: Tecnologías y Sistemas de la Información
Usuario objetivo: Funcionarios y Contratistas
Horario prestación del servicio: 24 horas
Soporte al Servicio: Tecnología y Sistemas de la Información, Ext. 1911 opción 2
Email: mesadeayudasistemas@metrosalud.gov.co

Horario de soporte al servicio: lunes a jueves de 7:00 a.m. – 5:00 p.m. viernes de 7:00 a.m. – 4:00 p.m. Sábados y domingos 7:00 a.m. – 3:00 p.m.

Tableros de Indicadores

Descripción: Apoyo a la generación y validación de indicadores de gestión para la medición de la operación del negocio
Categoría: Sistema de información.
Responsable: Tecnologías y Sistemas de la Información
Usuario objetivo: Funcionarios y Contratistas
Horario prestación del servicio: 24 horas
Soporte al Servicio: Tecnología y Sistemas de la Información, Ext. 1911 opción 2
Email: mesadeayudasistemas@metrosalud.gov.co
Horario de soporte al servicio: lunes a jueves de 7:00 a.m. – 5:00 p.m. viernes de 7:00 a.m. – 4:00 p.m. Sábados y domingos 7:00 a.m. – 3:00 p.m.

Diseño y Generación de Reportes

Descripción: Construcción de reportes y generación de informes para reporte a entes de control
Categoría: Sistema de información.
Responsable: Tecnologías y Sistemas de la Información
Usuario objetivo: Funcionarios y Contratistas
Horario prestación del servicio: 24 horas
Soporte al Servicio: Tecnología y Sistemas de la Información, Ext. 1911 opción 2
Email: mesadeayudasistemas@metrosalud.gov.co
Horario de soporte al servicio: lunes a jueves de 7:00 a.m. – 5:00 p.m. viernes de 7:00 a.m. – 4:00 p.m. Sábados y domingos 7:00 a.m. – 3:00 p.m.

ELABORADO POR:	
Jaime Alberto Henao Acevedo	Director Sistemas de Información
Jorge Adrián Ceballos Gallo	Analista
Angela Patricia Espinosa Pineda	Profesional Especializado

CONTROL DE ACTUALIZACIÓN

VERSIÓN	FECHA	DESCRIPCIÓN DEL CAMBIO O AJUSTE	RAZÓN DEL CAMBIO O AJUSTE	RESPONSABLE DEL CAMBIO O AJUSTE
1	30/10/2020	Se consolida en un solo documento los lineamientos institucionales en materia de seguridad de la información	Se realiza un documento para compilar diferentes instructivos y otros tipos de documentos no oficiales que orientan la operación de sistemas en condiciones seguras	Director de Sistemas de Información
2	28/09/2021	Se agrega anexo 15 con el Catálogo de servicios de Tecnologías de Información	Para dar cumplimiento a la Política de Gobierno Digital	Director de Sistemas de Información