

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. EDUCACIÓN Instituto para la Investigación Educativa y el Desarrollo Pedagógico</p>	<b>MANUAL PARA LA ADMINISTRACIÓN DE LA RED LAN DEL IDEP Y POLÍTICAS DE SEGURIDAD</b>	Código: MN-GT-12-07
		Versión: 2
		Fecha de Aprobación: 07/07/2023
		Página 1 de 19

<b>Firma de Autorizaciones</b>		
<b>Elaboró</b>	<b>Revisó</b>	<b>Aprobó</b>
César Linares Técnico Operativo - Oficina Asesora de Planeación	Ing. Julieta Yaver Licht Ingeniera Contratista OAP  Ing. Oscar Orlando Lozano Ingeniero Contratista OAP  Ing. Zulay García Ingeniera Contratista OAP	Jefe Oficina Asesora de Planeación
<b>Control de Cambios</b>		
<b>Fecha</b>	<b>Descripción</b>	
Julio de 2019	Creación del Documento	
Junio de 2023	Actualización del documento por cambio del Antivirus y futuro cambio del Firewall por uno en servicio FWAAS.	


 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. EDUCACIÓN Instituto para la Investigación Educativa y el Desarrollo Pedagógico</p>	<p><b>MANUAL PARA LA ADMINISTRACIÓN DE LA RED LAN DEL IDEP Y POLÍTICAS DE SEGURIDAD</b></p>	Código: MN-GT-12-07
		Versión: 2
		Fecha de Aprobación: 07/07/2023
		Página 2 de 19

## TABLA DE CONTENIDO

1.	OBJETIVO.	4
2.	ALCANCE.	4
3.	4	
4.	DOCUMENTOS ASOCIADOS.	4
5.	ADMINISTRACIÓN DE LA RED LAN.	4
5.1.	Administración de la red LAN del IDEP:	4
5.2.	Antivirus (Kaspersky Endpoint).	5
5.3.	Switches y routers inalámbricos.	6
5.4.	Dominio Windows – Directorio activo y DNS.	6
5.5.	Acceso a la red LAN de Servidores físicos y virtuales nuevos.	6
5.6.	Acceso a la red LAN de sistemas NAS (Network Attached Storage, por sus siglas en inglés).....	7
5.7.	Acceso al Centro de Datos y cuartos de comunicaciones de la red LAN.	7
5.8.	Sistema de control de acceso biométrico para las oficinas de la entidad.	7
5.9.	Sistema de cámaras de CCTV.	7
5.10.	Impresoras conectadas a la red LAN.	8
5.11.	Campañas de divulgación seguridad en la red LAN.	8
5.12.	Acceso a internet de dispositivos móviles de invitados y equipo portátiles de préstamo.	8
5.13.	Acceso a internet de computadores portátiles o de escritorio que no se pueden registrar en el Dominio Windows de la entidad.	8
6.	Políticas de seguridad de la red LAN.	8
6.1.	Computadores de escritorio y portátiles asignados al inventario de funcionarios y contratistas con sistema operativo Microsoft Windows.	9
6.2.	Computadores de escritorio y portátiles asignados al inventario de funcionarios y contratistas con sistema operativo MAC OS y Linux	9

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. EDUCACIÓN Instituto para la Investigación Educativa y el Desarrollo Pedagógico</p>	<p><b>MANUAL PARA LA ADMINISTRACIÓN DE LA RED LAN DEL IDEP Y POLÍTICAS DE SEGURIDAD</b></p>	Código: MN-GT-12-07
		Versión: 2
		Fecha de Aprobación: 07/07/2023
		Página <b>3</b> de <b>19</b>

6.3.	Computadores de escritorio y dispositivos móviles como celulares, tablets y portátiles de propiedad funcionarios y contratistas con cualquier sistema operativo.	10
6.4.	Computadores de escritorio y dispositivos móviles como celulares, tablets y portátiles de propiedad invitados con cualquier sistema operativo.	11
6.5.	Computadores portátiles de préstamo de la entidad con cualquier sistema operativo. .....	11
6.6.	Servidores físicos y virtuales de Windows y Linux.	11
6.7.	Sistema de cámaras de seguridad de CCTV.	13
6.8.	Sistema de control de acceso biométrico.	13
6.9.	NAS e Impresoras conectadas a la red LAN.	14
6.10.	Firewall.	14
6.11.	Acceso remoto desde la red de internet a la red LAN.	15
6.12.	Consola de antivirus.	17
6.13.	Hiperconvergencia.	17
6.14.	Switches y Routeres inalámbricos.	18
6.15.	Acceso al Centro de Datos y cuartos de comunicaciones de la red LAN.	19

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. EDUCACIÓN Instituto para la Investigación Educativa y el Desarrollo Pedagógico</p>	<p><b>MANUAL PARA LA ADMINISTRACIÓN DE LA RED LAN DEL IDEP Y POLÍTICAS DE SEGURIDAD</b></p>	Código: MN-GT-12-07
		Versión: 2
		Fecha de Aprobación: 07/07/2023
		Página 4 de 19

## 1. OBJETIVO.

Presentar el Manual para la administración de la red LAN del IDEP, que incluye las políticas de seguridad.

### ● 2. ALCANCE.

El presente manual hace parte del Proceso de Gestión Tecnológica y describe de manera general lo referente a la administración de la red LAN del IDEP, en el cual también se establecen políticas para garantizar el uso adecuado y la seguridad de esta.

## 3. REFERENCIAS NORMATIVAS.

Ver normativa del proceso de **Gestión Tecnológica** que puede ser consultado en el siguiente enlace: <https://www.idep.edu.co/directorio-transparencia>

## 4. DOCUMENTOS ASOCIADOS.

- PRO-GT-12-05 Mantenimiento de Infraestructura Tecnológica
- PRO-GT-12-07 Registro de Activos de Información tipo Software, Hardware y Servicios
- PRO-GT-12-08 Formulación y Seguimiento al PETI
- PRO-GT-12-10 Mesa de Servicios
- PRO-GT-12-12 Control de cambios de gestión tecnológica

## 5. ADMINISTRACIÓN DE LA RED LAN.


**5.1. Administración de la red LAN del IDEP:** se realiza sobre los equipos activos y dispositivos de red conectados a la red LAN y la red IDEP pública.

5.1.1. Firewall (Fortinet):

5.1.2. Verificar semanalmente si se encuentran actualizadas las firmas del Firewall (Firmware), esta actualización es automática en caso de no estar actualizada, realizar la actualización manualmente.

5.1.3. Verificar por lo menos una vez al año la fecha de expiración de las licencias de uso (Fortiguard), estas licencias se renuevan a través de un contrato de licenciamiento con el fabricante. Este contrato debe estar en el plan de adquisición anual de la entidad.

5.1.4. Verificar semanalmente el estado de la CPU, Disco duro, memoria RAM, sesiones, estadísticas de amenazas, consumo de ancho de banda, entre otros (Dashboard/widget), los porcentajes deben estar en un porcentaje por debajo del 80%. En caso de sobrepasar este porcentaje, el técnico

	<b>MANUAL PARA LA ADMINISTRACIÓN DE LA RED LAN DEL IDEP Y POLÍTICAS DE SEGURIDAD</b>	Código: MN-GT-12-07
		Versión: 2
		Fecha de Aprobación: 07/07/2023
		Página <b>5</b> de <b>19</b>

operativo de la Oficina Asesora de Planeación o quien haga sus veces debe contactar el soporte de fabricante para escalar el caso.


- 5.1.5. Atender por demanda las incidencias de los usuarios sobre el acceso a páginas y aplicativos WEB. Este proceso se realiza a través de la mesa de ayuda con el técnico operativo de la Oficina Asesora de Planeación o quien haga sus veces.
- 5.1.6. Realizar una depuración semestral sobre el uso de las políticas y objetos existentes en el Firewall. Este trabajo lo debe realizar el técnico operativo de la Oficina Asesora de Planeación o quien haga sus veces y se trata de identificar si las políticas y objetos existentes en el Firewall estén actualizados y funcionando de manera adecuada.
- 5.1.7. Realizar el registro en la base de datos de activos de información y/o en los diagramas de red, cuando se presente una modificación en la contratación, cableado estructurado, mapas de red, vlan, entre otros.
- 5.1.8. Realizar backup semanalmente al Firewall.

## **5.2. Antivirus (SOPHOS).**

- 5.2.1. Por motivo de que se cambió de antivirus (SOPHOS) y a la fecha de presentar este documento se encuentra en proceso de instalación, adecuación y puesta en marcha, todavía no hay un procedimiento para el mismo.

## **5.3. Switches y routers inalámbricos.**

- 5.3.1. Atender por demanda las incidencias de los usuarios que estén relacionadas con posible desconexión del punto de red. Este proceso se realiza a través de la mesa de ayuda con el técnico operativo de la Oficina Asesora de Planeación o quien haga sus veces.
- 5.3.2. Realizar la desconexión o desactivación de puntos de red que no se estén usando, esto con el fin de evitar posibles accesos no autorizados a la red LAN de la entidad.
- 5.3.3. Realizar el registro en la base de datos de activos de información y/o en los diagramas de red, cuando se presente una modificación en la contratación, cableado estructurado, mapas de red, vlan, entre otros.
- 5.3.4. Realizar backup en switches y routers por lo menos una vez al año o por demanda cada vez que se realice una modificación en la configuración o actualización de firmware. Este backup debe realizarse antes de aplicar cualquier cambio.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. EDUCACIÓN Instituto para la Investigación Educativa y el Desarrollo Pedagógico</p>	<p><b>MANUAL PARA LA ADMINISTRACIÓN DE LA RED LAN DEL IDEP Y POLÍTICAS DE SEGURIDAD</b></p>	Código: MN-GT-12-07
		Versión: 2
		Fecha de Aprobación: 07/07/2023
		Página 6 de 19

#### **5.4. Dominio Windows – Directorio activo y DNS.**

- 5.4.1. Crear o desactivar las cuentas de dominio Windows para funcionarios y contratistas, registrándolos en el grupo correspondiente del directorio activo.
- 5.4.2. Crear los registros de DNS (Domain Name Service por sus siglas en inglés) para equipos de cómputo de servidores físicos y virtuales.
- 5.4.3. Realizar el registro en la base de datos de activos de información y/o en los diagramas de red, cuando se presente una modificación en su configuración, hardware, software o sistema operativo.

#### **5.5. Acceso a la red LAN de Servidores físicos y virtuales nuevos.**

- 5.5.1. El acceso a equipos de cómputo tipo servidores físicos se realiza únicamente dentro del Centro de Datos del IDEP, se debe asignar un punto de red de los dispuestos para este fin en el Switch, se debe asignar una dirección IP para configurarla de manera estática en el servidor y se debe asignar un espacio físico en el rack de servidores. Para el caso de servidores virtuales se debe asignar una dirección IP para configurarla de manera estática en el servidor virtual. Este proceso lo realiza el técnico operativo de la Oficina Asesora de Planeación o quien haga sus veces.
- 5.5.2. Realizar el registro en la base de datos de activos de información y/o en los diagramas de red, cuando se presente una modificación en su configuración, hardware, software o sistema operativo.

#### **5.6. Acceso a la red LAN de sistemas NAS (Network Attached Storage, por sus siglas en inglés).**


Se realiza por demanda configurando en la NAS la dirección IP, para configurarla de manera estática. La configuración la realiza directamente el técnico operativo de la Oficina Asesora de Planeación.

#### **5.7. Acceso al Centro de Datos y cuartos de comunicaciones de la red LAN.**

Realizar el registro por demanda de los accesos al Centro de datos o a los cuartos de equipos, este registro debe quedar documentado en la mesa de ayuda por parte del técnico operativo de la Oficina Asesora de Planeación o quien haga sus veces.

#### **5.8. Sistema de control de acceso biométrico para las oficinas de la entidad.**

- 5.8.1. Atender por demanda las solicitudes para autorizar o denegar el ingreso a las oficinas de la entidad de funcionarios o contratistas en el sistema de acceso por biométrico. Este proceso se realiza a través de la mesa de

	<b>MANUAL PARA LA ADMINISTRACIÓN DE LA RED LAN DEL IDEP Y POLÍTICAS DE SEGURIDAD</b>	Código: MN-GT-12-07
		Versión: 2
		Fecha de Aprobación: 07/07/2023
		Página 7 de 19

ayuda con el técnico operativo de la Oficina Asesora de Planeación o quien haga sus veces.

- 5.8.2. Realizar el registro en la base de datos de activos de información y/o en los diagramas de red, cuando se presente una modificación en el cableado estructurado, mapas de red, entre otros.
- 5.8.3. Realizar backup al sistema de acceso biométrico por demanda o cuando haya cambios.

### **5.9. Sistema de cámaras de CCTV.**


- 5.9.1. Verificación diaria del estado de funcionamiento de las cámaras de seguridad CCTV, esta actividad la realiza el técnico operativo de la Oficina Asesora de Planeación o quien haga sus veces.
- 5.9.2. Atención por demanda de las incidencias del correcto funcionamiento que se presenten sobre las cámaras de seguridad, estas incidencias son escaladas para su atención al proveedor del contrato de mantenimiento de la infraestructura de tecnología.
- 5.9.3. Verificación por lo menos una vez al año de la capacidad ocupada del disco duro de almacenamiento de los videos de las cámaras de seguridad CCTV.
- 5.9.4. Realizar el registro en la base de datos de activos de información y/o en los diagramas de red, cuando se presente una modificación en el cableado estructurado, mapas de red, entre otros.

### **5.10. Impresoras conectadas a la red LAN.**

Se realiza por demanda configurando en la impresora la dirección IP que corresponde a la impresora de acuerdo a la oficina donde se encuentre ubicada, igualmente se debe configurar las credenciales de autenticación del dominio. La configuración la realiza directamente el técnico operativo de la Oficina Asesora de Planeación.

### **5.11. Campañas de divulgación de seguridad en la red LAN.**

- 5.11.1. Realizar por lo menos una vez al año campañas de divulgación presencial hacia funcionarios y contratistas de la entidad, sobre las políticas de seguridad en la red LAN.
- 5.11.2. Realizar por lo menos cuatro veces al año campañas de divulgación por correo hacia funcionarios y contratistas de la entidad, sobre las políticas de seguridad en la red LAN.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. EDUCACIÓN Instituto para la Investigación Educativa y el Desarrollo Pedagógico</p>	<p><b>MANUAL PARA LA ADMINISTRACIÓN DE LA RED LAN DEL IDEP Y POLÍTICAS DE SEGURIDAD</b></p>	Código: MN-GT-12-07
		Versión: 2
		Fecha de Aprobación: 07/07/2023
		Página 8 de 19

### **5.12. Acceso a internet de dispositivos móviles de invitados y equipo portátiles de préstamo.**

Se realiza por demanda configurando la contraseña de acceso a la red inalámbrica de internet de la red IDEP pública, esta red es el internet que ofrece el ADSL que tiene la entidad y que se encuentra totalmente separada de la red LAN. La configuración la realiza directamente el técnico operativo de la Oficina Asesora de Planeación. Los invitados no podrán tener acceso a la red LAN de la entidad.

### **5.13. Acceso a internet de computadores portátiles o de escritorio que no se pueden registrar en el Dominio Windows de la entidad.**

Se realiza por demanda registrando en el Firewall la dirección MAC en el Firewall de la tarjeta de red del computador para dar acceso a la red LAN de la entidad. Este es el caso de los computadores con sistemas operativos diferentes a Microsoft Windows, entre los que están Linux y MAC OS. Se deben realizar las excepciones en las políticas del Firewall para este tipo de equipos, esta configuración la realiza directamente el técnico operativo de la Oficina Asesora de Planeación.


## **6. Políticas de seguridad de la red LAN.**

Estas políticas son aplicadas a los equipos activos y dispositivos de red que haga uso de los servicios informáticos del IDEP, los funcionarios, contratistas y proveedores deberán tenerlas en cuenta para su cumplimiento.

### **6.1. Computadores de escritorio y portátiles asignados al inventario de funcionarios y contratistas con sistema operativo Microsoft Windows.**

- 6.1.1. Deben estar vinculados al dominio Windows, no debe trabajar con cuentas de usuario local.
- 6.1.2. Se les debe configurar una única cuenta de dominio de usuario final, con restricción de instalación de software y restricción a las funciones de ejecutar y panel de control que aparecen en el menú de inicio de Windows. Ningún otro funcionario o contratista podrá iniciar sesión con cuenta de dominio Windows en un equipo diferente al asignado.
- 6.1.3. Estos equipos deben tener el agente de red y el Kaspersky Endpoint instalado, el símbolo del Kaspersky en la barra de tareas del equipo no debe presentar ningún símbolo de advertencia o encontrarse deshabilitado (color gris), de presentarse esta situación el responsable del equipo debe abrir un ticket por mesa de ayuda para ser solucionada esta situación.
- 6.1.4. Deben estar asociados a un punto de red físico único, el cual debe ser entregado como parte del inventario al funcionario o contratista, para que




 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. EDUCACIÓN Instituto para la Investigación Educativa y el Desarrollo Pedagógico</p>	<p><b>MANUAL PARA LA ADMINISTRACIÓN DE LA RED LAN DEL IDEP Y POLÍTICAS DE SEGURIDAD</b></p>	Código: MN-GT-12-07
		Versión: 2
		Fecha de Aprobación: 07/07/2023
		Página <b>9</b> de <b>19</b>

haga custodia del uso adecuado del mismo. El funcionario o el contratista deberá avisar inmediatamente a los ingenieros de sistemas, si alguien no autorizado hace conexión de algún equipo al punto de red que tiene asignado.

- 6.1.5. El equipo debe estar con la contraseña de la cuenta de administrador local configurada para que únicamente el técnico operativo de la Oficina Asesora de Planeación preste el soporte. Igualmente para presentar soporte debe tener configurada la cuenta de dominio administrador global.
- 6.1.6. El equipo debe contar con contraseña de acceso a la BIOS y debe estar configurado en el BOOT de inicio como primer dispositivo el disco duro local.
- 6.1.7. Los funcionarios y contratistas son responsables del buen uso del equipo asignado, por tal motivo no deben permitir la manipulación del equipo diferente al técnico operativo de la Oficina Asesora de Planeación, en caso de que alguna persona manipule o pida el equipo prestado deberá ser validado primero por el técnico operativo de la OAP.
- 6.1.8. En estos equipos debe estar almacenada localmente solamente información institucional, la información personal deberá ser almacenada en memorias USB o discos externos propiedad de cada funcionario o contratista.

**6.2. Computadores de escritorio y portátiles asignados al inventario de funcionarios y contratistas con sistema operativo MAC OS y Linux.** Estos equipos no se pueden vincular al dominio Windows, por tal razón deben cumplir como mínimo con los siguientes aspectos:

- 6.2.1. Se les debe configurar una única cuenta local de usuario final, con restricción de instalación de software. Ningún otro funcionario o contratista podrá iniciar sesión con cuenta local en un equipo diferente al asignado.
- 6.2.2. Estos equipos deben tener el agente de red y el Kaspersky Endpoint instalado, el símbolo del Kaspersky en la barra de tareas del equipo no debe presentar ningún símbolo de advertencia o encontrarse deshabilitado (color gris), de presentarse esta situación el responsable del equipo debe abrir un ticket por mesa de ayuda para ser solucionada esta situación.
- 6.2.3. Deben estar asociados a un punto de red físico único, el cual debe ser entregado como parte del inventario al funcionario o contratista, para que haga custodia del uso adecuado del mismo. El funcionario o el contratista deberá avisar inmediatamente a los ingenieros de sistemas, si alguien no autorizado hace conexión de algún equipo al punto de red que tiene asignado.
- 6.2.4. El equipo debe estar con la contraseña de la cuenta de administrador local configurada para que únicamente el técnico operativo de la Oficina Asesora de Planeación preste el soporte. Esta contraseña debe cumplir con la

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. EDUCACIÓN Instituto para la Investigación Educativa y el Desarrollo Pedagógico</p>	<p><b>MANUAL PARA LA ADMINISTRACIÓN DE LA RED LAN DEL IDEP Y POLÍTICAS DE SEGURIDAD</b></p>	Código: MN-GT-12-07
		Versión: 2
		Fecha de Aprobación: 07/07/2023
		Página <b>10</b> de <b>19</b>

configuración de complejidad de mínimo de ocho caracteres usando mayúsculas, caracteres especiales, caracteres alfanuméricos, entre otros.


- 6.2.5. El equipo debe contar con contraseña de acceso a la BIOS y debe estar configurado en el BOOT de inicio como primer dispositivo el disco duro local.
- 6.2.6. Los funcionarios y contratistas son responsables del buen uso del equipo asignado, por tal motivo no deben permitir la manipulación del equipo diferente al técnico operativo de la Oficina Asesora de Planeación, en caso de que alguna persona manipule o pida el equipo prestado deberá ser validado primero por el técnico operativo de la OAP.
- 6.2.7. En estos equipos debe estar almacenada localmente solamente información institucional, la información personal deberá ser almacenada en memorias USB o discos externos propiedad de cada funcionario o contratista.

### **6.3. Computadores de escritorio y dispositivos móviles como celulares, tablets y portátiles de propiedad de funcionarios y contratistas con cualquier sistema operativo.**

Estos equipos por ningún motivo pueden tener conexión a la red LAN de la entidad, ni de forma física ni de forma inalámbrica, solamente podrán hacer uso de la red inalámbrica Wi-Fi IDEP pública. La red IDEP pública es una red totalmente aislada de la red LAN de la entidad, por esta razón solamente podrán hacer uso del servicio de Internet y no tendrá acceso a los recursos compartidos de la red LAN ni de las impresoras de la esta red. Tampoco se garantiza la seguridad sobre esta red, por esta razón el técnico operativo de la OAP deberá en el momento de configurar esta red en los equipos de las personas invitadas, informar que tomen las precauciones de seguridad sobre sus archivos o información almacenada en sus dispositivos para evitar pérdida de información o sustracción de información sensible.

### **6.4. Computadores de escritorio y dispositivos móviles como celulares, tablets y portátiles de propiedad invitadas con cualquier sistema operativo.**

Estos equipos por ningún motivo pueden tener conexión a la red LAN de la entidad, ni de forma física ni de forma inalámbrica, solamente podrán hacer uso de la red inalámbrica Wifi IDEP pública. La red IDEP pública es una red totalmente aislada de la red LAN de la entidad, por esta razón solamente podrán hacer uso del servicio de Internet y no tendrá acceso a los recursos compartidos de la red LAN ni de las impresoras de la esta red. Tampoco se garantiza la seguridad sobre esta red, por esta razón el técnico operativo de la OAP deberá en el momento de configurar esta red en los equipos de las personas invitadas, informar que tomen las precauciones de seguridad sobre sus archivos o información almacenada en sus dispositivos para evitar perdida de información o sustracción de información sensible.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. EDUCACIÓN Instituto para la Investigación Educativa y el Desarrollo Pedagógico</p>	<p><b>MANUAL PARA LA ADMINISTRACIÓN DE LA RED LAN DEL IDEP Y POLÍTICAS DE SEGURIDAD</b></p>	Código: MN-GT-12-07
		Versión: 2
		Fecha de Aprobación: 07/07/2023
		Página 11 de 19


▪

## 6.5. Computadores portátiles de préstamo de la entidad con cualquier sistema operativo.

- 6.5.1. Estos equipos por ningún motivo pueden tener conexión a la red LAN de la entidad, ni de forma física ni de forma inalámbrica, solamente podrán hacer uso de la red inalámbrica Wi-Fi IDEP pública o a la red física IDEP pública en la sala de juntas del piso 8 y al centro de documentación. La red IDEP pública es una red totalmente aislada de la red LAN de la entidad, por esta razón solamente podrán hacer uso del servicio de Internet y no tendrá acceso a los recursos compartidos de la red LAN ni de las impresoras de la esta red. Tampoco se garantiza la seguridad sobre esta red, por esta razón el técnico operativo de la OAP deberá en el momento de configurar esta red en los equipos de las personas invitadas, que tomen las precauciones de seguridad sobre sus archivos o información almacenada en memorias USB o discos externos para evitar pérdida de información o sustracción de información sensible.
- 6.5.2. En estos equipos no se debe realizar ningún tipo de almacenamiento en los discos duros de manera permanente, esta información será borrada una vez se haga la devolución al técnico operativo de la OAP.

## 6.6. Servidores físicos y virtuales de Windows y Linux.

- 6.6.1. Los servidores físicos deben estar alojados únicamente dentro del Centro de datos del IDEP, dentro del rack de servidores, por ninguna razón se deben tener equipos de cómputo tipo servidor en los puestos de trabajo de los funcionarios o contratistas. Esto con el fin de garantizar la restricción para el acceso al personal no autorizado.
- 6.6.2. Estos equipos servidores deben tener el agente de red y el Kaspersky Endpoint instalado, el Kaspersky no debe presentar ningún símbolo de advertencia o encontrarse deshabilitado (color gris), de presentarse esta situación el responsable del servidor debe verificar coordinado con el técnico operativo del OAP la solución pertinente.
- 6.6.3. Deben estar asociados a un punto de red físico único, el cual debe ser asignado por el técnico operativo de la OAP, de acuerdo a la distribución que se tenga en los Switches y VLANs para este fin.
- 6.6.4. El equipo debe estar con la contraseña de la cuenta de Root local configurada para que únicamente el técnico operativo de la Oficina Asesora de Planeación preste el soporte en conjunto con el responsable del equipo servidor. Esta contraseña debe cumplir con la configuración de complejidad de mínimo de ocho caracteres usando mayúsculas, caracteres especiales, caracteres alfanuméricos, entre otros.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. EDUCACIÓN Instituto para la Investigación Educativa y el Desarrollo Pedagógico</p>	<p><b>MANUAL PARA LA ADMINISTRACIÓN DE LA RED LAN DEL IDEP Y POLÍTICAS DE SEGURIDAD</b></p>	Código: MN-GT-12-07
		Versión: 2
		Fecha de Aprobación: 07/07/2023
		Página 12 de 19

- 6.6.5. El servidor debe contar con contraseña de acceso a la BIOS y debe estar configurado en el BOOT de inicio como primer dispositivo el disco duro local.
- 6.6.6. Los funcionarios y contratistas responsables de cada equipo servidor son responsables del buen uso del equipo asignado, por tal motivo no deben permitir la manipulación del equipo diferente al técnico operativo de la Oficina Asesora de Planeación.
- 6.6.7. En estos equipos debe estar almacenada localmente solamente información institucional, la información personal deberá ser almacenada en memorias USB o discos externos propiedad de cada funcionario o contratista.
- 6.6.8. Deben estar asociados a una dirección IP única, la cual deberá ser asignada por el técnico operativo de la OAP, de acuerdo a la distribución que se tenga en los segmentos de red para este fin.
- 6.6.9. Estos servidores de cómputo deben estar registrados en la base de datos de activos de información y en los diagramas de red de la entidad. Realizando el registro de las versiones de software que tienen instalados tales como el sistema operativo, controladores de dispositivos, software de aplicación, bases de datos, antivirus, proveedor de soporte, IP asignadas, entre otros. Así mismo realizar el registro de las configuraciones que a criterio del administrador del servidor de cómputo que se requiera para llevar a cabo una actualización, traslado, plan de contingencia, simulacro entre otros.
- 6.6.10. Los servidores de cómputo de la entidad deben estar incluidos en el plan de contingencia, plan de mantenimiento de infraestructura y debe tener contrato de soporte con el fabricante o proveedor del servicio.

## **6.7. Sistema de cámaras de seguridad de CCTV.**


- 6.7.1. El acceso por red al sistema de cámaras de seguridad de CCTV de la entidad, solamente estará en responsabilidad del técnico operativo del OAP, al igual de la configuración y videos almacenados en este sistema. Cualquier petición para el acceso a estos videos será autorizada exclusivamente por la alta dirección de la entidad.
- 6.7.2. El concentrador (DVR) de las cámaras de seguridad deberá estar ubicado exclusivamente dentro del Centro de datos de la entidad, con el fin de garantizar la restricción para el acceso al personal no autorizado.
- 6.7.3. Debe estar asociado a una dirección de red IP única, la cual deberá ser asignada por el técnico operativo de la OAP, de acuerdo a la distribución que se tenga en los segmentos de red para este fin.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. EDUCACIÓN Instituto para la Investigación Educativa y el Desarrollo Pedagógico</p>	<p><b>MANUAL PARA LA ADMINISTRACIÓN DE LA RED LAN DEL IDEP Y POLÍTICAS DE SEGURIDAD</b></p>	Código: MN-GT-12-07
		Versión: 2
		Fecha de Aprobación: 07/07/2023
		Página 13 de 19

- 6.7.4. El concentrador (DVR) de las cámaras de seguridad deberá estar registrado en la base de datos de activos de información y en los diagramas de red de la entidad. Realizando el registro de las versiones de software que tienen instalados tales como el sistema operativo, software de aplicación, interface de conexión, bases de datos, IP asignada, proveedor de soporte, entre otros. Así mismo realizar el registro de las configuraciones que a criterio del administrador del DVR que se requiera para llevar a cabo una actualización, traslado, plan de contingencia, simulacro entre otros.
- 6.7.5. Sistema de cámaras de seguridad de CCTV de la entidad deben estar incluidos en el plan de mantenimiento de infraestructura de la entidad.

## **6.8. Sistema de control de acceso biométrico.**

- 6.8.1. La administración del sistema de control de acceso biométrico para el acceso de los funcionarios y contratistas a las oficinas de la entidad, solamente estará en responsabilidad del técnico operativo del OAP, al igual de la configuración y base de datos de este sistema. Cualquier petición para el registro o desactivación en la base de datos se realizará mediante un ticket de la mesa de ayuda; para el caso de los funcionarios lo solicitará el profesional especializado de talento humano y para los contratistas lo solicitará el supervisor del contrato.
- 6.8.2. Los concentradores o Controladores Lógicos Programables (PLCs por sus siglas en inglés Programmable Logic Controller) del sistema biométrico deberán estar ubicado exclusivamente dentro del Centro de Datos de la entidad, con el fin de garantizar la restricción para el acceso al personal no autorizado.
- 6.8.3. Debe estar asociado a una dirección de red IP única, la cual deberá ser asignada por el técnico operativo de la OAP, de acuerdo a la distribución que se tenga en los segmentos de red para este fin.
- 6.8.4. Sistema de control de acceso biométrico deberá estar registrado en la base de datos de activos de información y en los diagramas de red de la entidad. Realizando el registro de las versiones de software que tienen instalados tales como software de aplicación, interface de conexión, bases de datos, proveedor de soporte, IP asignadas, entre otros. Así mismo realizar el registro de las configuraciones que a criterio del administrador del DVR que se requiera para llevar a cabo una actualización, traslado, plan de contingencia, simulacro entre otros.
- 6.8.5. Realizar backup cuando se realicen modificaciones a la base de datos, este backup se realizará previo a cualquier modificación.
- 6.8.6. Sistema de cámaras de seguridad de CCTV de la entidad deben estar incluidos en el plan de mantenimiento de infraestructura de la entidad.


 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. EDUCACIÓN Instituto para la Investigación Educativa y el Desarrollo Pedagógico</p>	<p><b>MANUAL PARA LA ADMINISTRACIÓN DE LA RED LAN DEL IDEP Y POLÍTICAS DE SEGURIDAD</b></p>	Código: MN-GT-12-07
		Versión: 2
		Fecha de Aprobación: 07/07/2023
		Página 14 de 19

## 6.9. NAS e Impresoras conectadas a la red LAN.

- 6.9.1. Para la administración se debe hacer la asignación de la dirección IP única por cada una de las impresoras y NAS que estén en servicio en la red LAN. Las cuales deberán ser asignadas por el técnico operativo de la OAP, de acuerdo a la distribución que se tenga en los segmentos de red para este fin.
- 6.9.2. Estos dispositivos de red deben estar asociados a un punto de red físico único, el cual debe ser asignado por el técnico operativo de la OAP, de acuerdo a la distribución que se tenga en los Switches y VLANs para este fin. Una vez asignados estos puntos de red, serán de uso exclusivo para su correspondiente impresora o NAS y no se deberán conectar equipos de cómputo a los mismos. El técnico operativo del OAP será el responsable del buen uso de estos puntos en cuanto al tema de seguridad para el acceso a la red LAN de la entidad.
- 6.9.3. Las NAS de la entidad deben estar alojadas únicamente dentro del Centro de datos del IDEP, dentro del rack de servidores, por ninguna razón se pueden tener operando en el puesto de trabajo de algún funcionario o contratista. Esto con el fin de garantizar la restricción para el acceso al personal no autorizado.
- 6.9.4. Las NAS de la entidad deben estar registradas en la base de datos de activos de información y en los diagramas de red de la entidad. Realizando el registro de las versiones de software que tienen instalados tales como el sistema operativo, interface de conexión, proveedor de soporte, IP asignada, entre otros. Así mismo realizar el registro de las configuraciones que a criterio del administrador de la NAS que se requiera para llevar a cabo una actualización, traslado, plan de contingencia, simulacro entre otros.
- 6.9.5. Las NAS y las impresoras de la entidad deben estar incluidos en el plan de mantenimiento de infraestructura de la entidad.

## 6.10. Firewall. Un Firewall o cortafuegos es el dispositivo de seguridad de la red que monitorea el tráfico de red entrante y saliente y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad.

- 6.10.1. El Firewall principal de la entidad debe estar alojado únicamente dentro del Centro de datos del IDEP, dentro del rack de servidores, por ninguna razón se puede tener operando en el puesto de trabajo de algún funcionario o contratista. Esto con el fin de garantizar la restricción para el acceso al personal no autorizado.
- 6.10.2. Debe estar asociado a las direcciones de red IP por cada subred existente en la red LAN, las cuales deberán ser asignadas por el técnico operativo de la OAP, de acuerdo a la distribución que se tenga en los segmentos de red para este fin.


 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. EDUCACIÓN Instituto para la Investigación Educativa y el Desarrollo Pedagógico</p>	<p><b>MANUAL PARA LA ADMINISTRACIÓN DE LA RED LAN DEL IDEP Y POLÍTICAS DE SEGURIDAD</b></p>	Código: MN-GT-12-07
		Versión: 2
		Fecha de Aprobación: 07/07/2023
		Página 15 de 19

- 6.10.3. Debe estar asociado a una dirección IP en la red Pública, la cual es asignada por el proveedor del servicio de internet y configurada por el técnico operativo de la OAP.
- 6.10.4. Debe estar con la contraseña de la cuenta de administrador local configurada para que únicamente el técnico operativo de la Oficina Asesora de Planeación preste el soporte. Esta contraseña debe cumplir con la configuración de complejidad de mínimo de ocho caracteres usando mayúsculas, caracteres especiales, caracteres alfanuméricos, entre otros.
- 6.10.5. Debe estar registrado en la base de datos de activos de información y en los diagramas de red de la entidad. Realizando el registro de las versiones de software que tienen instalados tales como el sistema operativo nativo, interface de conexión, proveedor de soporte, IP asignadas, entre otros. Así mismo realizar el registro de las configuraciones que a criterio del administrador del Firewall que se requiera para llevar a cabo una actualización, traslado, plan de contingencia, simulacro entre otros.
- 6.10.6. El Firewall de la entidad debe estar incluido en el plan de contingencia, plan de mantenimiento de infraestructura y debe tener contrato de soporte con el fabricante o proveedor del servicio.
- 6.10.7. Realizar backup cuando se realicen cualquier modificación o actualización, este backup se realizará previo a cualquier modificación o actualización.

▪

#### **6.11. Acceso remoto desde la red de internet a la red LAN.**

- 6.11.1. Todos los accesos remotos desde la red de internet a la red LAN de la entidad deben ser a través del servicio VPN (Virtual Private Network, por sus siglas en inglés), que es prestado por el Firewall de la entidad. VPN hace referencia a una red privada virtual, es una tecnología de red de computadoras que permite una extensión segura de la red de área local LAN sobre una red pública o no controlada como Internet.
- 6.11.2. Las solicitudes para tener acceso remoto desde internet a la red LAN de la entidad para los funcionarios y contratistas deben realizarse a través de la mesa de ayuda de la entidad. Para los funcionarios la debe realizar el jefe inmediato y para los contratistas la debe realizar el supervisor del contrato.
- 6.11.3. Las solicitudes para acceso por VPN debe tener creada una cuenta de usuario de Dominio. La cuenta de dominio y grupos funcionales se administran desde el Servidor de Dominio a través del Active Directory, en donde se controla lo concerniente a permisos y características de las cuentas de acceso y de los grupos funcionales.
- 6.11.4. Los funcionarios que tienen acceso a VNP son los que estén autorizados para Teletrabajo.
- 6.11.5. Los funcionarios o contratistas que requieran acceso a VNP y sean autorizados por el supervisor o Jefe inmediato. En caso de que la conexión se vaya a realizar en equipo de escritorio el técnico operativo realizará la

	<b>MANUAL PARA LA ADMINISTRACIÓN DE LA RED LAN DEL IDEP Y POLÍTICAS DE SEGURIDAD</b>	Código: MN-GT-12-07
		Versión: 2
		Fecha de Aprobación: 07/07/2023
		Página 16 de 19


instalación en la residencia del funcionario o contratista. En caso de que la conexión se realice en un equipo portátil debe traerlo al IDEP.

- 6.11.6. El técnico operativo debe instalar el Forticlient para acceso a VPN, que garantiza el acceso al equipo que tiene en uso el IDEP.
- 6.11.7. El horario de acceso a VPN será de lunes a viernes de 6:00 am a 6:00 pm, si requieren ingreso en horario diferente deberá dejarlo registrado en la solicitud inicial por mesa de ayuda.
- 6.11.8. El técnico operativo y los Ingenieros del proceso de Gestión Tecnológica tiene acceso a VPN con horario ilimitado para realizar acciones como la administración remota de servidores de cómputo de la entidad, monitoreo de los servicios informáticos de la entidad, administración de firewall, entre otros.
- 6.11.9. El proveedor del Sistema de Información GOOBI tiene acceso por VPN y el horario será de lunes a viernes de 6:00 am a 6:00 pm, si requieren ingreso en horario diferente deberá ser autorizado por el supervisor del contrato y debe quedar registrado en la mesa de ayuda de la entidad.
- 6.11.10. Los proveedores que presten servicios de soporte y mantenimiento a sistemas de información que tenga instalado el IDEP se les habilitará el acceso, una vez el supervisor del contrato remita correo electrónico al Jefe de la Oficina de Planeación y deberá quedar registrado en la mesa de ayuda de la entidad. El responsable del soporte de primer nivel de la entidad de cada Sistemas de Información valida la información, crea la cuenta de acceso e informa al proveedor las condiciones técnicas y de seguridad que debe cumplir la máquina a la cual se le dará el acceso.
- 6.11.11. Para el caso de soporte de fabricante de la Hiperconvergencia la conexión se realiza a través del aplicativo que tiene el fabricante para tal fin, será autorizado por el supervisor del contrato y deberá quedar registrado en la mesa de ayuda de la entidad.
- 6.11.12. Para la validación de los requisitos de la máquina de teletrabajo, se programa una visita donde se revisa que el equipo remoto cumpla con los requerimientos del Instituto llenando el formato FT-GTH-13-51 (Lista de verificación de condiciones técnicas mínimas de equipos para teletrabajo).
- 6.11.13. Las cuentas de Dominio y acceso VPN son personales e intransferibles, en caso se identificar préstamo o suplantación se denegará inmediatamente el servicio y se notificará al jefe inmediato o supervisor del contrato la novedad.

## 6.12. Consola de antivirus.

- 6.12.1. Por motivo de que se cambió de antivirus (SOPHOS) y a la fecha de presentar este documento se encuentra en proceso de instalación, adecuación y puesta en marcha, todavía no hay un procedimiento para el mismo. La consola de antivirus es vía Web y el responsable de la administración es el técnico



 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. EDUCACIÓN Instituto para la Investigación Educativa y el Desarrollo Pedagógico</p>	<p><b>MANUAL PARA LA ADMINISTRACIÓN DE LA RED LAN DEL IDEP Y POLÍTICAS DE SEGURIDAD</b></p>	Código: MN-GT-12-07
		Versión: 2
		Fecha de Aprobación: 07/07/2023
		Página 17 de 19


operativo de la oficina de planeación o uno de los ingenieros contratados para tal fin, que es designado por el jefe de la Oficina Asesora de Planeación del IDEP.

- 6.12.2. Debe estar registrada en la base de datos de activos de información de la entidad. Realizando el registro de la versión de software, servidor o computador donde está instalada, interface de conexión, proveedor de soporte, entre otros. Así mismo realizar el registro de las configuraciones que a criterio del administrador de la consola de antivirus que se requiera para llevar a cabo una actualización, traslado, plan de contingencia, entre otros.
- 6.12.3. Debe estar incluida en el plan de contingencia y debe tener contrato de soporte con el fabricante o proveedor del servicio.
- 6.12.4. Realizar backup cuando se realicen cualquier modificación o actualización, este backup se realizará previo a cualquier modificación o actualización.

### **6.13. Hiperconvergencia.**

Es el sistema de virtualización de la entidad, que permite tener los servidores de cómputo principales como máquinas virtuales, teniendo centralizada la gestión y administración en una misma aplicación de virtualización con recursos de almacenamiento y procesamiento con alta disponibilidad en los servicios informáticos institucionales.

- 6.13.1. La Hiperconvergencia de la entidad debe estar alojado únicamente dentro del Centro de datos del IDEP, dentro del rack de servidores, por ninguna razón se puede tener operando en el puesto de trabajo de algún funcionario o contratista. Esto con el fin de garantizar la restricción para el acceso al personal no autorizado.
- 6.13.2. Debe estar asociado a las direcciones de red IP por cada subred existente en la red LAN, las cuales deberán ser asignadas por el técnico operativo de la OAP, de acuerdo a la distribución que se tenga en los segmentos de red para este fin.
- 6.13.3. Deben estar asociados a un punto de red físico único, el cual debe ser asignado por el técnico operativo de la OAP, de acuerdo a la distribución que se tenga en los Switches y VLANs para este fin.
- 6.13.4. Los nodos de la Hiperconvergencia deben estar con la contraseña de la cuenta de administrador local configurada para que únicamente el técnico operativo de la Oficina Asesora de Planeación preste el soporte en conjunto con el responsable del equipo servidor. Esta contraseña debe cumplir con la configuración de complejidad de mínimo de ocho caracteres usando mayúsculas, caracteres especiales, caracteres alfanuméricos, entre otros.
- 6.13.5. Los nodos de la Hiperconvergencia deben contar con contraseña de acceso a la BIOS y debe estar configurado en el BOOT de inicio como primer dispositivo el disco duro local.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. EDUCACIÓN Instituto para la Investigación Educativa y el Desarrollo Pedagógico</p>	<p><b>MANUAL PARA LA ADMINISTRACIÓN DE LA RED LAN DEL IDEP Y POLÍTICAS DE SEGURIDAD</b></p>	Código: MN-GT-12-07
		Versión: 2
		Fecha de Aprobación: 07/07/2023
		Página 18 de 19


- 6.13.6. Debe estar registrada en la base de datos de activos de información y en los diagramas de red de la entidad. Realizando el registro de las versiones de software que tienen instalados tales como el sistema operativo nativo, interface de conexión, proveedor de soporte, IP asignadas, entre otros. Así mismo realizar el registro de las configuraciones que a criterio de la Hiperconvergencia que se requiera para llevar a cabo una actualización, traslado, plan de contingencia, simulacro entre otros.
- 6.13.7. Debe estar incluido en el plan de contingencia, plan de mantenimiento de infraestructura y debe tener contrato de soporte con el fabricante o proveedor del servicio.
- 6.13.8. Realizar backup cuando se realicen cualquier modificación o actualización, este backup se realizará previo a cualquier modificación o actualización.

#### **6.14. Switches y Routeres inalámbricos.**

- 6.14.1. Para la administración se debe hacer la asignación de la dirección IP única por cada Switch y Router que estén en servicio en la red LAN. Las cuales deberán ser asignadas por el técnico operativo de la OAP, de acuerdo a la distribución que se tenga en los segmentos de red para este fin.
- 6.14.2. Los Switches y Routeres de la entidad deben estar alojadas únicamente dentro del Centro de datos o cuartos de comunicaciones del IDEP, dentro del rack de comunicaciones, por ninguna razón se pueden tener operando en el puesto de trabajo de algún funcionario o contratista. Esto con el fin de garantizar la restricción para el acceso al personal no autorizado.
- 6.14.3. Deben estar con la contraseña de la cuenta de administrador local configurada para que únicamente el técnico operativo de la Oficina Asesora de Planeación preste el soporte. Esta contraseña debe cumplir con la configuración de complejidad de mínimo de ocho caracteres usando mayúsculas, caracteres especiales, caracteres alfanuméricos, entre otros.
- 6.14.4. Deben estar registradas en la base de datos de activos de información y en los diagramas de red de la entidad. Realizando el registro de las versiones de software que tienen instalados tales como interface de conexión, proveedor de soporte, IP asignada, entre otros. Así mismo realizar el registro de las configuraciones que a criterio del administrador de los Switches y Routeres que se requiera para llevar a cabo una actualización, traslado, plan de contingencia, simulacro entre otros.
- 6.14.5. Debe estar incluido en el plan de contingencia, plan de mantenimiento de infraestructura y debe tener contrato de soporte con el fabricante o proveedor del servicio.

#### **6.15. Acceso al Centro de Datos y cuartos de comunicaciones de la red LAN.**

- 6.15.1. El acceso al Centro de Datos y Cuartos de comunicaciones de la red LAN de la entidad deben estar restringidos a personas no autorizadas a través

	<b>MANUAL PARA LA ADMINISTRACIÓN DE LA RED LAN DEL IDEP Y POLÍTICAS DE SEGURIDAD</b>	Código: MN-GT-12-07
		Versión: 2
		Fecha de Aprobación: 07/07/2023
		Página <b>19</b> de <b>19</b>

de la protección perimetral física como son divisiones, muros y puertas de acceso.

- 6.15.2. Los sistemas de acceso como son biométricos o llaves deben estar en custodia del personal autorizado del grupo de sistema y soporte de la infraestructura.
- 6.15.3. El Centro de Datos debe estar monitoreado por cámara de seguridad CCTV que tenga grabación por movimiento 7x24.
- 6.15.4. El Centro de Datos debe tener sensor de humo para detección de incendios y activación de alarmas visuales y audibles.