HISTÓRICO DE CAMBIOS		
VERSIÓN	**FECHA DE EMISIÓN**	**CAMBIOS REALIZADOS**
1	28/12/2023	Emisión inicial

Elaboró	Revisó	Aprobó	Avaló
Jorge Enrique Ramírez Rodríguez Contratista OAP-TI	**María Cristina Herrera Calderón** Contratista OAP-TI	**Daniel Sánchez Rojas** Jefe de la Oficina Asesora de Planeación y Tecnologías de la Información	**Daniel Sánchez Rojas** Jefe de la Oficina Asesora de Planeación y Tecnologías de la Información
Jorge Alberto Farigua Gutiérrez Contratista OAP-TI			

1. OBJETIVO

Establecer los lineamientos para garantizar la administración y seguridad de los servicios de red, de conectividad y de la información del IDARTES.

2. ALCANCE

El protocolo inicia con la identificación de las redes y los servicios de red y culmina con la administración de la información que en ellos se contiene.

3. RESPONSABLES

Equipo de tecnologías de la información de la Oficina Asesora de Planeación y Tecnologías de la Información.

4. DEFINICIONES Y ABREVIATURAS

TÉRMINO	DEFINICIÓN
ANS	Acuerdos de niveles de servicio.
ANTIVIRUS	Programa diseñado para identificar, aislar o eliminar un virus del computador.
ALMACENADO TRANSACCIONAL	Un procedimiento almacenado de modificación en el que los cambios en la base de datos realizados por el procedimiento se encapsulan en su propia transacción.
APLICACIÓN VAULT	Herramienta que hace parte de la Suite de Google Apps para almacenamiento y consulta de copias de seguridad de cuentas de correo de licenciamiento Basic.
BASE DE DATOS DISTRIBUIDA	Una base de datos en la que los datos se distribuyen entre varias computadoras o dispositivos (nodos), lo que permite que varias computadoras accedan simultáneamente a los datos que residen en nodos separados.
BASE DE DATOS INCRUSTADA	Un base de datos incrustada es la combinación de una base de datos y el software de la base de datos que normalmente reside dentro de una aplicación. La base de datos contiene información y el software controla la base de datos para acceder o almacenar información.
BACKUP	Copia de respaldo de la información realizada en medio magnético.
BACKUP COMPLETO O FULL	se refiere al proceso de copiar todo aquello que fue previamente considerado importante y que no puede perderse. Esta copia de seguridad

TÉRMINO	DEFINICIÓN
	es la primera y la más consistente, ya que puede ser realizada sin la necesidad de herramientas adicionales.
BACKUP PROGRESIVO O INCREMENTAL	Este proceso de copia exige un nivel de control mucho mayor sobre las distintas etapas del backup, realiza la copia los archivos teniendo en cuenta los cambios que sufrieron desde el último respaldo.
BACKUP DIFERENCIAL	El diferencial tiene la estructura básica del backup progresivo, es decir, hace copias de seguridad solo de los archivos que sufrieron alguna modificación o que son nuevos, el cambio en este modelo de backup está en que todos los archivos creados después del backup completo siempre serán copiados nuevamente.
CATALOGAR	Un repositorio para la forma legible por computadora de la definición de datos de una base de datos metadatos. A veces se llama catálogo del sistema o simplemente syscat.
CATEGORÍA	Se asigna una categoría (que puede estar a su vez subdividida en más niveles) dependiendo del tipo de incidente o del grupo de Trabajo responsable de su resolución. Se identifican los servicios afectados por el incidente.
CACHE	La memoria de la computadora que se reserva para contener una parte de los datos de la base de datos a los que el programa de aplicación de la base de datos ha accedido más recientemente.
CENTROS CREA	Centros de formación artística orientados a la comunidad, dependientes de la Subdirección de Formación.
CONEXION	Los medios de comunicación entre un cliente y un servidor. Un proceso puede tener múltiples conexiones abiertas, cada una en su propio hilo, a una o más bases de datos a la vez.
CORREO ELECTRÓNICO	Es un servicio que permite el intercambio de mensajes a través de sistemas de comunicación electrónicos.
ESCALABILIDAD	Un sistema de software es escalable cuando su rendimiento y el rendimiento general del sistema continúan mejorando a medida que se ponen a disposición más recursos informáticos para su uso. Esto generalmente viene en forma de la cantidad de CPU y núcleos disponibles en la computadora en la que se ejecuta el sistema de software.
GLPI	Herramienta que gestiona las incidencias o solicitudes de soporte de los usuarios de la entidad. Su sigla, traducidas de francés a español, significan

TÉRMINO	DEFINICIÓN
	Gestión Libre del Parque informático.
GOOGLE DRIVE	Servicio de herramientas colaborativas de la Suite de Google Apps para almacenamiento en nube y ofimática online.
HARDWARE	Componentes eléctricos, dípticos, electrónicos, electromecánicos y mecánicos que conforman un instrumento o sistema de computador.
INSTANCIA DE BASES DE DATOS	Una base de datos independiente que comparte el mismo esquema que otra base de datos. Usado solo en RDM.
INFORMACIÓN	Agrupación de datos con un significado específico.
LICENCIAMIENTO BÁSIC DE GMAIL	Tipo de cuenta de Gmail con opciones limitadas en cuanto a seguridad y respaldo.
LICENCIAMIENTO BUSINESS DE GMAIL	Tipo de cuenta de Gmail con opciones avanzadas en cuanto a seguridad y respaldo reservada para directivos y jefes de área.
MODELO RELACIONAL	Una base de datos en la que las relaciones entre tablas se organizan principalmente a través de columnas de datos comunes, que definen una relación de uno a muchos entre una fila del Clave primaria tabla y una o más filas de la coincidencia clave externa mesa. Equi-joins relacionan tablas que tienen valores de clave primaria / externa coincidentes, pero se pueden definir otras comparaciones (relaciones).
SINCRONIZACION	El método de implementación (con frecuencia semáforos) mediante el cual la ejecución simultánea de múltiples subprocesos o procesos informáticos puede acceder de forma segura y actualizar los datos compartidos.
SOFTWARE	Programas que se ejecutan en el computador para realizar una función determinada.
SERVIDOR DE APLICACIONES	Un servidor que procesa operaciones de bases de datos específicas de la aplicación realizadas desde programas cliente de aplicaciones.
SERVIDOR CLIENTE	Un servidor es un programa que se ejecuta en una computadora que administra directamente la base de datos. Un cliente es un programa (o proceso) separado que se comunica con el servidor de la base de datos a través de algún tipo de llamada a procedimiento remoto (RPC) para realizar operaciones de base de datos específicas de la aplicación.
TIPOS DE DATOS	El tipo básico de datos que se pueden almacenar en una columna. Los tipos de datos que están disponibles en RDM SQL son: carbonizarse, wchar,

TÉRMINO	DEFINICIÓN
	varchar, wvarchar, binario, varbinary, booleano, diminuto, pequeño, entero, Empezando, verdadero, flotador, doble, fecha, hora, marca de tiempo, varbinary largo, varchar largo, y largo wvarchar.
USUARIO	Servidor público que tiene a su cargo un computador y/o una cuenta de correo por medio de los cuales puede acceder a los recursos y servicios que ofrece una red.
USUARIO ADMINISTRADOR	Usuarios con privilegios para instalación y configuración de software y hardware en el equipo asignado que por sus deberes funcionales requieren este perfil.
VISOR DE BASE DE DATOS	Nombre original de 1984 para el producto Raima DBMS ahora llamado RDM.

5. DIRECTRICES A IMPLEMENTAR

1. Revisión de los derechos de acceso de usuarios: Los responsables de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.

Para el caso de los accesos de los usuarios, el IDARTES cuenta con el controlador de dominio que permite llevar un control periódico, definiendo tiempos de actividad y caducidad para los usuarios y el acceso que estos deben tener de cara a sistemas de información, inicio de sesión en estaciones de trabajo y autenticación en equipos NAS. Una vez la cuenta del usuario expira o ha culminado su relación contractual con el IDARTES, la cuenta inmediatamente es desactivada perdiendo acceso a los sistemas previamente autorizados.

2. Retiro o ajuste de los derechos de acceso: Los derechos de acceso de todos los colaboradores y de usuarios externos a la información y a las instalaciones de procesamiento de información, se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.

3. Perímetro de seguridad física: Se deben definir y usar perímetros de seguridad, para proteger áreas que contengan información sensible o crítica, e instalaciones de manejo de información.

Para el aseguramiento de los centros de procesamiento como los son centros de cableado, centros de datos, y lugares de almacenamiento donde reposan elementos de tecnología, todos se encuentran separados de las áreas comunes con las que cuenta la entidad, así como también cuentan con protección de acceso a través de llave, que solo son otorgadas a personal autorizado de la entidad en donde se realiza acompañamiento por parte de la OAP-TI y se supervisa que no se intervengan equipos adicionales a los indicados.

Para el acceso a estos espacios se llevará una bitácora digital donde reposan las actividades realizadas, así como un registro de la duración de la visita, con el escaneo de un código QR.

4. Controles físicos de entrada: Las áreas seguras se deben proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.

Dichos controles se describen a continuación:

a) Tener un registro de la fecha y hora de entrada y salida de los visitantes, y todos los visitantes deben ser supervisados a menos que su acceso haya sido aprobado

previamente; solo se les debe otorgar acceso para propósitos específicos autorizados y se deben emitir instrucciones sobre los requisitos de seguridad del área y de los propósitos de emergencia. La identidad de los visitantes se debe autenticar por los medios apropiados.

b) Establecer que el acceso a las áreas en las que se procesa o almacena información confidencial se debería restringir a los individuos autorizados solamente mediante la implementación de controles de acceso apropiados, (mediante la implementación de un mecanismo de autenticación de dos factores, tales como una tarjeta de acceso y un PIN secreto).

c) Mantener y hacer seguimiento de un libro de registro (physical log book) físico o un rastro de auditoría electrónica de todos los accesos.

d) Definir que todos los empleados, contratistas y partes externas deben portar algún tipo de identificación visible, y se deben notificar de inmediato al personal de seguridad si se encuentran visitantes no acompañados, y sin la identificación visible.

e) Establecer que el personal de servicio de soporte de la parte externa se le debería otorgar acceso restringido a áreas seguras o a instalaciones de procesamiento de información confidencial solo cuando se requiera; este acceso se debe autorizar y se le debe hacer seguimiento.

f) Definir los derechos de acceso a las áreas seguras se deben revisar y actualizar regularmente, y revocar cuando sea necesario.

5. Servicios de suministro: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.

El IDARTES cuenta en todos sus espacios con equipos responsables de garantizar el suministro eléctrico en caso de pérdida de potencia por diferentes causas externas.

Estos equipos especializados son las UPS, que cuentan con pruebas de potencia que permiten suplir por un periodo determinado la estabilidad de los equipos especiales como son servidores, switches, SAN, NAS, etc, en dado caso que el suministro eléctrico no pueda ser restablecido a la menor brevedad, las sedes del IDARTES y el edificio principal cuentan con planta eléctrica que permitirá darle continuidad al funcionamiento de los equipos.

Ilustración 1. UPS

Fuente. Tercer piso de la sede principal del IDARTES

6. Seguridad del cableado: El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información, debe estar protegido contra interceptación, interferencia o daño.

Respecto a cableado estructurado, la entidad en todas sus sedes tiene separado el cableado eléctrico del cableado de datos, así, como también cuenta dispositivos pasivos para la correcta gestión de la red Patch Panel, organizadores de cableado y marquillado de los puntos de red dentro de un armario que cumple con las normas técnicas para este servicio.

Ilustración 2. Rack modelo

Fuente. Tercer piso de la sede principal del IDARTES

7. Mantenimiento de equipos: Los equipos deben mantenerse correctamente para asegurar su disponibilidad e integridad continua.

Para el mantenimiento de equipos de red y servidores se agendan anualmente dos tareas de mantenimiento preventivo, que se ejecutan una en cada semestre del año, durante estas actividades se realiza una limpieza de los elementos, así, como una revisión de su software en busca de actualizaciones que mejoren su rendimiento y seguridad.

Este proceso se lleva a cabo y se documenta en la hoja de vida de cada elemento, en donde una vez se finaliza la actividad se valida el correcto funcionamiento de los elementos intervenidos.

Ilustración 3. Mantenimiento servidores

Fuente. Elaboración propia

8. Separación de los ambientes de desarrollo, pruebas y producción: Se debe separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados en el ambiente de producción.

Se describen a continuación cada uno de los ambientes:

• **Desarrollo:** Ambiente en donde los ingenieros de desarrollo pueden llevar a cabo pruebas sobre nuevas funcionalidades o revisar cambios necesarios sobre los ambientes de producción, son desplegados sobre la plataforma de virtualización OVM.

• **Pruebas:** Ambiente expuesto al equipo de QA quienes realizan las diferentes pruebas funcionales de los aplicativos que allí reposan, estos ambientes son desplegados sobre la plataforma de virtualización OVM.

- **Producción:** Ambiente de cara a los usuarios finales, que solo es modificado una vez se ha llevado y expuesto al comité de cambios y ha recibido el visto bueno tanto de infraestructura, seguridad, QA y jefatura del área, en la plataforma VmWare.

Como se señaló previamente, todos estos ambientes están separados tanto físicamente, como de manera virtual, ya que los ambientes productivos reposan en la infraestructura VmWare y los ambientes de desarrollo y de pruebas sobre el cluster de virtualización OVM.

La separación de los ambientes contempla las siguientes consideraciones:

a) Definir y documentar las reglas para la transferencia de software del estatus de desarrollo al de producción.

b) Definir que los cambios en los sistemas operativos y aplicaciones se deben probar en un entorno de pruebas antes de aplicarlos a los sistemas operacionales.

c) Definir que las pruebas no se deben llevar a cabo en los sistemas operacionales, solamente en circunstancias excepcionales.

d) Establecer que los compiladores, editores y otras herramientas de desarrollo o utilitarios del sistema no debe ser accesibles desde sistemas operacionales cuando no se requiere.

e) Establecer que los usuarios deben usar diferentes perfiles de usuario para sistemas operacionales y de pruebas, y los menús deben desplegar mensajes de identificación apropiados para reducir el riesgo de error.

f) Definir que los datos sensibles no se deben copiar en el ambiente de pruebas, a menos que se suministren controles.

9. Creación de una máquina virtual: A través de la mesa de servicios se generará la solicitud y será validada y aprobada por el jefe de la Oficina Asesora de Planeación y Tecnologías de la Información. En la solicitud debe especificar:

- Justificación de la necesidad
- Tipo de sistema operativo
- Cantidad memoria RAM
- Cantidad VCPU
- Capacidad y tipo de almacenamiento

- Requerimiento de IP Pública
- Creación de subdominio en idartes.gov.co o crea.gov.co

Una vez aprobada la creación, el administrador de infraestructura realizará la configuración, parametrización y la creación de las credenciales de acceso a la máquina virtual.

Una vez la máquina virtual es creada, su acceso, independientemente del ambiente en el que se encuentre para la conexión SSH, será a través del cliente VPN, esta regla de conexión será configurada de manera conjunta por el ingeniero de seguridad y el ingeniero de conectividad e infraestructura, para que de cara a internet, solo queden habilitadas las conexiones por HTTPS, cualquier puerto o protocolo adicional deberá ser expuesto ante el comité de cambios, quien evaluará los riesgos asociados y la necesidad de tener un puerto diferente.

Para el caso en que los aplicativos a evaluar, requieran una conexión site to site con otra entidad u organización, será el desarrollador quien informará al ingeniero de seguridad y al de conectividad e infraestructura esta necesidad e indicará los contactos técnicos con quienes se deberán realizar estas conexiones, al igual que con las publicaciones web se validarán puertos y protocolos requeridos por ambas partes y el impacto acompañado de la necesidad del requerimiento.

10. Controles de redes: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.

La gestión de redes LAN, WAN, WLAN estará a cargo del ingeniero de conectividad e infraestructura, quien supervisará los permisos, comportamientos y registro de eventos en la red del IDARTES, así como la disponibilidad de los enlaces principales y secundarios de las sedes según sea el caso.

El IDARTES actualmente cuenta con tres controladoras de red wifi que administran las redes inalámbricas de diferentes escenarios de la siguiente manera:

1. Cisco Meraki: Castillo de las Artes
2. Unifi: Edificio principal, centro CREA, y escenarios
3. OMADA TPlink: TJEG, teatro El Ensueño, y centros CREA

En estas controladoras reposan dos SSID:

1. IDARTES_LAN: Red corporativa para equipos portátiles y demás propiedad del IDARTES, con acceso red LAN de la entidad.
2. IDARTES_MOVILES: Red de acceso gratuito para funcionarios y visitantes, con acceso limitado a las redes LAN de la entidad.

Las políticas de navegación para el caso de Unifi y OMADA son administradas directamente desde el equipo firewall Fortinet de la entidad.

Desde el firewall Fortinet se registra la sesión del usuario, los intentos de logueo, así, como también sitios visitados.

11. Seguridad de los servicios de red: Se debe identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.

Las redes de la entidad se encuentran separadas en diferentes VLAN que segmentan el tráfico que pasa por ellas, es necesario una autenticación al momento de conectarse a la red cableada de la entidad o de intentar acceder a la red corporativa, allí se cifra la comunicación y mediante los controles que tiene establecido el firewall de autenticación a través de LDAP, y los controles de seguridad en la navegación, se limita el acceso a ciertas páginas web no autorizadas, garantizando la seguridad.

12. Monitorear los registros de logs y eventos de los respaldos en caso de encontrar alguna alarma o error del backup, para esto, se debe hacer seguimiento con el fin de corregir las fallas detectadas.

A través de las herramientas de monitoreo solarwinds y zabbix se lleva un registro de los eventos de los equipos de red, caídas, bloqueos, consumo de recursos, etc.

13. Todos los cambios realizados sobre la infraestructura de servidores, equipos de conectividad o revisiones que se realicen a estos, deben ser registrados en el documento Bitacora Datacenter.xlsx.

6. GESTIÓN DE LA SEGURIDAD DE LAS REDES

Controles de redes			
CONTROL	**DIRECTRICES**	**ACTORES**	**SOPORTE A DIRECTRICES**
Gestionar y controlar las redes para proteger la información en sistemas y aplicaciones	Administrar y gestionar la red del IDARTES.	Oficina Asesora de Planeación y Tecnologías de la Información	Log Fortigate
	Establecer los controles lógicos para el acceso a los diferentes recursos informáticos, con el fin de mantener los niveles de seguridad apropiados.		Log Fortigate
	Proporcionar a los colaboradores y terceros todos los recursos tecnológicos de conectividad necesarios para que puedan desempeñar las funciones y actividades laborales.		Log Fortigate, y log Orion SolawWinds
	Monitorear la funcionalidad de las redes a través del uso de analizadores de red.		Log Fortigate, y log Orion SolawWinds
	No es permitido conectar a las estaciones de trabajo o a los puntos de acceso de la red corporativa, elementos de red (tales como switches, enrutadores, módems, etc.) que no sean autorizados por la OAPTI.	Todos los colaboradores y terceros del IDARTES	No aplica

Seguridad de los servicios de red			
CONTROL	**DIRECTRICES**	**ACTORES**	**SOPORTE A DIRECTRICES**
Identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se	Dar el acceso a internet exclusivamente a través de la red establecida para ello, es decir, por medio del sistema de seguridad con Firewall incorporado en la misma.	Oficina Asesora de Planeación y Tecnologías de la Información	Log del Firewall
	Administrar la habilitación y/o bajas de los dispositivos móviles (computadoras portátiles, Ipad, celulares, etc.) propiedad del IDARTES y de los usuarios que hayan sido solicitados a través de la mesa de ayuda de tecnología.		Log del Firewall
	Utilizar el acceso a la red, internet, exclusivamente para el desarrollo de las	Todos los colaboradores	No aplica

Seguridad de los servicios de red			
CONTROL	**DIRECTRICES**	**ACTORES**	**SOPORTE A DIRECTRICES**
contraten externamente	actividades propias de las funciones desempeñadas en el IDARTES.	del IDARTES	
	Usar la red inalámbrica del IDARTES, para lo cual necesariamente deberá estar dentro del dominio del IDARTES.		No aplica
	El acceso de los colaboradores a la red debe realizarse a través de la red inalámbrica definida como (IDARTES_moviles) o mediante la red cableada.		No aplica
	Conectarse única y exclusivamente a la red inalámbrica (Invitados) del IDARTES a internet, sin la necesidad de algún tipo de cableado. La red inalámbrica de invitados le permitirá utilizar los servicios de internet, en las zonas de cobertura del IDARTES.	Clientes, proveedores, visitantes del IDARTES	No aplica
	Los usuarios que accedan a través de la red invitados no tendrán acceso a los servicios, sistemas de información, etc., del IDARTES ni a ningún recurso de uso privado del IDARTES.		Log Cisco

Separación en las redes			
CONTROL	**DIRECTRICES**	**ACTORES**	**SOPORTE A DIRECTRICES**
Separar en las redes los grupos de servicios de información, usuarios y sistemas de información	Establecer un esquema de segregación de redes, con el fin de controlar el acceso a los diferentes segmentos de red y buscar que se preserve la confidencialidad, integridad y disponibilidad de la información del IDARTES.	Oficina Asesora de Planeación y Tecnologías de la Información	Logs switches
	Establecer parámetros técnicos para la conexión segura de la red con los servicios de red.		Logs switches
	Establecer mecanismos de autenticación seguros para el acceso a la red.		Log Fortigate
	Separar las redes inalámbricas públicas de las redes internas, para preservar los principios de la seguridad de la		Log Fortigate

Separación en las redes			
CONTROL	**DIRECTRICES**	**ACTORES**	**SOPORTE A DIRECTRICES**
	información.		

Documento 20234300692433 firmado electrónicamente por:

DANIEL SÁNCHEZ ROJAS, Jefe Oficina Asesora de Planeación y Tecnologías de la Información, Oficina Asesora de Planeación, Fecha firma: 28-12-2023 12:41:18
JORGE ALBERTO FARIGUA GUTIERREZ, , Oficina Asesora de Planeación, Fecha firma: 28-12-2023 14:02:55
MARIA CRISTINA HERRERA CALDERON, , Oficina Asesora de Planeación, Fecha firma: 28-12-2023 13:19:26
JORGE ENRIQUE RAMIREZ RODRIGUEZ, Contratista, Área de Tecnología, Fecha firma: 28-12-2023 12:43:05

Proyectó: SANDRA PATRICIA MORENO BOHORQUEZ - Técnico Administrativo - Área de Tecnología

Anexos: 1 folios

eda1e4e3f8f043f592838d80e366e95f690b5c51659ddc9a06d1956e315d83d6
Codigo de Verificación CV: 6f637 Comprobar desde: