PORTADA

A) HISTORIAL DE CAMBIOS

VERSIÓN	FECHA	JUSTIFICACIÓN DE LA MODIFICACIÓN
1	30/11/2016	Lanzamiento del procedimiento
2	11/12/2018	Actualización de la normatividad del procedimiento
3	30/09/2021	1. Incluir en el desarrollo del procedimiento las temáticas: • Documentación de TI • Gestión de la capacidad • Separación de ambientes • Sincronización de relojes • Usuarios restringidos • Análisis de vulnerabilidades • Ventanas de mantenimiento • Seguridad de las comunicaciones 2. Actualizar la lista de distribución 3. Redefinir el objetivo y el alcance 4. Cambiar el titulo marco legal por marco de referencia 5. Cambiar el nombre del procedimiento, antes: "ADMINISTRACIÓN DE TECNOLOGIAS DE INFORMACIÓN (TI)" 6. Inclusión de los controles del mapa de riesgos relacionados con el procedimiento.
4	28/04/2023	Se incluye en el capítulo 7 desarrollo del procedimiento el numeral: 7.10 GESTIÓN DE MONITOREO Y SUS REGISTROS
5	02/04/2024	• Cambia el nombre del numeral 7.7 SEGURIDAD DE LAS REDES Y COMUNICACIONES • En el numeral 7.7 se agrega la actividad 12 • En el numeral 7.7 se agrega la actividad 13 • En el numeral 7.7 se edita la actividad 3 • Se agrega el numeral 7.11 PROTECCIÓN DE ACTIVOS DE INFORMACIÓN DURANTE PRUEBAS DE AUDITORÍA • Se agrega el numero 7.12 ELIMININACIÓN SEGURA DE INFORMACIÓN • Se modifica la actividad 6 del numeral 7.8 TRANSFERENCIA DE INFORMACIÓN • Se modifican las actividades 1,2 y se elimina la actividad 3 del numeral 7.5 ANÁLISIS DE VULNERABILIDADES • Se agrega el numeral 7.14 DISPOSICIÓN SEGURA DE EQUIPOS • Se cambia el objetivo, alcance, responsables, marco de referencia • Se cambia la forma de presentación de los capítulos • Se modifican las actividades 2,3,4,5 y 6 el capítulo 7.6 VENTANAS DE MANTENIMIENTO • Se modifica la actividad 4 del capítulo 7.8 TRANSFERENCIA DE INFORMACIÓN • Se cambia el contexto del numeral 8. Controles, alineado con la norma ISO 27001:2022 • Se cambia el numeral 9. Formatos y anexos

B) REVISIONES Y APROBACIONES DEL DOCUMENTO

ELABORÓ	REVISÓ	APROBÓ
Nombre: Jesús Goyes Alvarado	Nombre: German Armando Correa Amado	Nombre: Francisco Alvaro Ramírez Rivera
Cargo: Contratista Asesor Planeación y Sistemas	Cargo: Jefe Oficina Asesora de Planeación y Sistemas	Cargo: Director General
Fecha: 26/03/2024	Fecha: 01/02/2024	Fecha: 02/04/2024

REVISÓ
Nombre: Oscar Herrera Isaza
Cargo: Contratista Asesor Sistemas de Gestión
Fecha: 27/03/2024

C) LISTA DE DISTRIBUCIÓN

N°	NOMBRE Y CARGO
1	Jefe Oficina Asesora de Planeación y Sistemas.
2	Profesional Oficina Asesora de Planeación y Sistemas
3	Profesional Especializada Oficina Asesora de Planeación y Sistemas.
4	Técnico Oficina Asesora de Planeación y Sistemas
5	Profesional Oficina Asesora de Planeación y Sistemas

1. OBJETIVO

Definir la línea base para la gestión de las operaciones tecnológicas de la Entidad

2. ALCANCE

Inicia con una documentación detallada de la plataforma tecnológica y a partir de ello continua con el monitoreo y la aplicación de tareas preventivas y correctivas sobre la operación tecnológica, tanto a nivel de infraestructura de servidores, comunicaciones, almacenamiento, como también de los sistemas de información y demás servicios de TI en el punto final, de forma que se garanticen niveles aceptables de disponibilidad.

3. RESPONSABLES

El responsable de ejecutar este procedimiento es el equipo de trabajo perteneciente a la oficina asesora de planeación y sistema y su proceso de Gestión Tecnológica

4. MARCO DE REFERENCIA

- *Ley 1581 de 2012, para la protección de datos personales.*
- *Resolución 409 del 10 de agosto de 2018 expedida por el Fondo de Previsión Social del Congreso de la República y que se refiere a la revisión y aprobación de procedimientos.*
- *Política de tratamiento de datos personales de Fonprecon*
- *Políticas de seguridad y privacidad de la información*

5. DEFINICIONES

- **TI**: Todos los factores tecnológicos que, en conjunto, posibilitan una adecuada disponibilidad, acceso y control de la información, entre los cuales, se puede mencionar las redes de comunicación interna y externa, sistemas de información, hardware, software, etc.
- **Eficiencia**: Utilizar menos recursos para lograr un mismo objetivo o lograr más objetivos con los mismos o menos recursos.
- **Eficacia**: Capacidad para lograr objetivos.

6. POLÍTICAS Y CONDICIONES GENERALES

6.1 Mantener los componentes de hardware, software y comunicaciones de red, plenamente identificados en un catálogo.

6.2 Mantener en condiciones de operación aceptables y requeridas por la Entidad todos los componentes de TI.

7. DESARROLLO DEL PROCEDIMIENTO

7.1 DOCUMENTACIÓN

Responsables**:** Administradores de la plataforma tecnológica – Jefe de la Oficina Asesora de Planeación y Sistemas

N°	ACTIVIDAD	DOCUMENTO REGISTRO Y OBSERVACIONES
1	Registrar y mantener actualizado información de la plataforma tecnológica referente a la gestión de TI: • Roles para administración de TI • Guía de monitoreo, precisando los aspectos más relevantes para seguimento • Vigencia domínio Fonprecon.gov.co • Unidades de red por GPO AD • Contactos Soporte, de provedores de TI • Mesa de ayuda, niveles de servicio • Objetivos estratégicos de TI • Estructura organizacional de TI • PETI Proyectos • Configuraciones	Documentación tecnológica F01-PRO-GTC-002

2	Registrar y mantener actualizado información de la plataforma tecnológica referente a los diferentes catálogos de TI:
	• bases de datos
	• Copias de seguridade - Cintas
	  • Bases de datos
	  • Certificados SSL
	  • Sistemas de información
	  • Servicios Tecnológicos
	  • Software Licencias
	  • Renovaciones ciclo de vida
	  • Infraestructura
	  • Cintas LTO7
	  • Estaciones de trabajo y perifericos
	  • Marco Normativo (Políticas, normas y legislación)
	  • Componentes SGSI : Seguridad y privacidad, ciberseguridad, datos personales
	  • Bases de datos personales - RNBD - SIC
		Documentación tecnológica F01-PRO-GTC-002

7.1 DOCUMENTACIÓN

Responsables**:** Administradores de la plataforma tecnológica – Jefe de la Oficina Asesora de Planeación y Sistemas

N°	ACTIVIDAD	DOCUMENTO REGISTRO Y OBSERVACIONES
	• Microsoft 365 - Buzones de correo - FUNCIONARIOS • Ciclo de vida software • Manuales • Vencimiento servicios, acuerdos, licencias • Microsot 365 - Flujos y aplicaciones • Repositorios compartidos • Nivel de servicio canales de internet • Garantías vigencia	
3	Registrar y mantener actualizado información de la plataforma tecnológica referente a los diferentes indicadores de TI: • Atención requerimientos • Mantenimiento • Transmisión • Seguridad de la información - Incidentes - SGSI • Seguridad de la información - Sensibilización - SGSI • Seguridad de la información - Impacto Ataques - SGSI • Seguridad de la información - Pruebas - SGSI • Seguridad de la información - RTO - SGSI • Disponibilidad operación servicios TI – SGSI	Documentación tecnológica F01-PRO-GTC-002
4	Registrar y mantener actualizado información de la plataforma tecnológica referente al centro de datos: • Protocolo ON/OFF • Mapa tablero eléctrico regulado • Certificación RETILAP RETIE • Vigencia garantias • Almacenamiento iSCSI • Plataforma Virtualización • Incidentes HW • Segmentos de red • Registros DNS • Almacenamiento servidores	Documentación tecnológica F01-PRO-GTC-002

7.1 DOCUMENTACIÓN

Responsables**:** Administradores de la plataforma tecnológica – Jefe de la Oficina Asesora de Planeación y Sistemas

N°	ACTIVIDAD	DOCUMENTO REGISTRO Y OBSERVACIONES
5	Registrar y mantener actualizado información de la plataforma tecnológica referente al diseño: • Centro de datos - General • Red General • Red Detallado • Roles Servidores • Gabinete Servidores y redes • Aprovechamiento TI	Documentación tecnológica F01-PRO-GTC-002
6	Registrar y mantener actualizado información de la plataforma tecnológica referente a la seguridad: • Respaldo servidores • Respaldo bases de datos • Respaldo Carpetas • Monitoreo y Logs • Registro de novedades • Copia de estaciones de trabajo	Documentación tecnológica F01-PRO-GTC-002

7.2 GESTIÓN DE LA CAPACIDAD

Responsables: Administradores de la plataforma tecnológica - Oficina de Planeación y Sistemas

N°	ACTIVIDAD	DOCUMENTO REGISTRO Y OBSERVACIONES
1	Documentar la capacidad de almacenamiento por cada servidor del centro de datos, incluyendo las unidades tipo iSCSI	Documentación tecnológica F01-PRO-GTC-002
2	Registrar y mantener actualizado el inventario de bases de datos, lugar de almacenamiento y plan de respaldo.	Documentación tecnológica F01-PRO-GTC-002
3	Revisar con frecuencia mensual, el estado de la capacidad de almacenamiento, frente al tamaño ocupado y disponible	Software de inventario de hardware y software

7.2 GESTIÓN DE LA CAPACIDAD **Responsables:** Administradores de la plataforma tecnológica - Oficina de Planeación y Sistemas		
N°	**ACTIVIDAD**	**DOCUMENTO REGISTRO Y OBSERVACIONES**
4	Revisar la proyección y estimación de la capacidad de almacenamiento requerida para 5 años, en servicios críticos como servidores de bases de datos, gestión documental, correo, aplicaciones y demás que se consideren relevantes	Documentación tecnológica F01-PRO-GTC-002
5	Administrar el almacenamiento, agregando o quitando según las necesidades y la disponibilidad del mismo, mediante estrategias de unidades de almacenamiento tipo ISCSI, local, desde dispositivos tipo NAS	Servidores de almacenamiento
6	Mantener el control documentado de almacenamientos para ambientes de pruebas y otros propósitos temporales, de forma que se puedan liberar lo antes posible.	Documentación tecnológica F01-PRO-GTC-002
7	Revisar periódicamente y mantenga controlada la acumulación de logs, a fin de no ocupar el 100% del almacenamiento con esta información, para ello, aplique configuraciones automáticas de borrado de logs mediante la solución de copias de seguridad tanto para SQL server como para Exchange.	Servidores del centro de datos
8	Borrar información temporal como instaladores y otros recursos que no son necesarios para la operación de un sistema	Servidores del centro de datos
9	Revisar el estado de alertas de umbrales de almacenamiento mediante los reportes de este propósito en el software de inventario *Lansweeper*	Software de inventario *Lansweeper*

7.3 SEPARACIÓN DE AMBIENTES **Responsables:** Administradores de la plataforma tecnológica - Oficina de Planeación y Sistemas		
N°	**ACTIVIDAD**	**DOCUMENTO REGISTRO Y OBSERVACIONES**
1	**Ambiente de desarrollo y pruebas:** • Mantener disponible un ambiente de pruebas, con un servidor físico que admita recursos virtualizados HyperV, redes virtuales aisladas del ambiente de producción para realizar pruebas con copias de servidores. • Mantener una instancia de pruebas y desarrollo para bases	Documentación tecnológica F01-PRO-GTC-002

7.3 SEPARACIÓN DE AMBIENTES **Responsables:** Administradores de la plataforma tecnológica - Oficina de Planeación y Sistemas		
N°	**ACTIVIDAD**	**DOCUMENTO REGISTRO Y OBSERVACIONES**
1	de datos SQL Server, requeridas por aplicaciones en desarrollo y pruebas. • Mantener en operación un segmento de red diferente al de servidores de producción y de estaciones de trabajo, para la zona desmilitarizada DMZ, que permita la ubicación de servicios que son publicados en internet **Ambiente de producción:** • Se basa en segmentos de red específicos y documentados • Los equipos del ambiente de producción alojados en el centro de datos se configuran con direccionamiento IP fijas. • Las estaciones de trabajo de este ambiente, se configuran con direccionamiento IP dinámico DHCP.	

7.4 SINCRONIZACIÓN DE RELOJES **Responsable:** Administradores de la plataforma tecnológica		
N°	**ACTIVIDAD**	**DOCUMENTO REGISTRO Y OBSERVACIONES**
1	Fuentes de referencia de tiempo: • Las estaciones de trabajo y servidores del centro de datos diferentes a los controladores de dominio, sincronizan con los servidores de la red LAN conocidos como controladores de dominio, mediante aplicación de GPO para este propósito denominada Hora NTP. • Los controladores de dominio, toman la referencia de tiempo del servidor NTP de la hora legal en Colombia y redundancia en servidores org de la zona horaria para Colombia, mediante configuración específica en el registro de Windows, por lo cual, estos servidores no reciben la GPO • Los controladores de dominio requieren permisos de salida a internet para consultar la hora legal de Colombia y zona horaria org para Colombia	Servidores con el rol de controlador de dominio y directorio activo

	• Los sistemas de información tienen como fuente de referencia de tiempo, los servidores donde se alojan o estaciones de trabajo donde se ejecuta la aplicación para el caso de aplicaciones cliente servidor.	

7.5 ANÁLISIS DE VULNERABILIDADES **Responsables:** Administradores de la plataforma tecnológica - Oficina de Planeación y Sistemas		
N°	**ACTIVIDAD**	**DOCUMENTO REGISTRO Y OBSERVACIONES**
1	***Activos de la red LAN:*** • *Realizar análisis de vulnerabilidades de forma periódica, haciendo uso de la solución Kali Linux, con licencia de libre uso* • *Actualizar las definiciones de Kali Linux, en cada uso.* ***Activos como servicios en internet:*** • *Gestión de la plataforma online security scorecard provista por Super intendencia financiera de Colombia*	Registro de vulnerabilidades en cada plataforma
2	*Usar los resultados de vulnerabilidades para:* • *Planear y aplicar correctivos de forma controlada ya sea desde el alcance de gestión tecnológica o desde un tercero de acuerdo con los niveles de acuerdo de servicios del caso o alcance contractual* • *Informar y escalar con el nivel administrativo apropiado o en el comité de seguridad de la información, aquellos correctivos que requieren inversión* • *Reportar métricas a la Superintendencia Financiera de Colombia con periodicidad trimestral, en cumplimiento de circular externa 033 de 2020*	Métricas Formato 408 Acciones de remediación

7.6 VENTANAS DE MANTENIMIENTO **Responsables:** Administradores de la plataforma tecnológica - Oficina de Planeación y Sistemas		
N°	**ACTIVIDAD**	**DOCUMENTO REGISTRO Y OBSERVACIONES**
1	• Establecer de forma clara:	Documentos de planeación de la

7.6 VENTANAS DE MANTENIMIENTO **Responsables:** Administradores de la plataforma tecnológica - Oficina de Planeación y Sistemas		
N°	**ACTIVIDAD**	**DOCUMENTO REGISTRO Y OBSERVACIONES**
	• Alcance y resultados esperados de la actividad • Fechas y horarios • Alcance de la indisponibilidad • Cronograma y responsables de cada actividad • Estrategia de roll back • Permisos de ingreso a la sede • Registro de ingreso y salida de equipos y personal • Solicitar al proveedor relación de personal y parafiscales	actividad
2	*Establecer consenso con líderes de proceso acerca de fechas y horarios con menos impacto en la operación misional,*	Correo electrónico
3	*Solicitar autorización a la dirección general para la fecha y hora acordados con el proceso y responsables de las actividades*	Reunión
4	*Solicitar autorización de ingreso a la sede a través de la coordinación de bienes y servicios*	Correo electrónico
5	*Informar y reiterar a través de correo electrónico a los funcionarios, contratistas, proveedores y terceros acerca de la ventana de mantenimiento, incluyendo horario, detalle de los servicios que no estarán disponibles y las recomendaciones del caso.*	Correo electrónico
6	*Informe del resultado de las actividades*	Correo electrónico

7.7 SEGURIDAD DE LAS REDES Y COMUNICACIONES Responsables: Profesional y Contratista Asesor Oficina de Planeación y Sistemas		
N°	**ACTIVIDAD**	**DOCUMENTO REGISTRO Y OBSERVACIONES**
1	Revisar y gestionar el estado de ocupación del ancho de banda de los canales de internet, mediante la interfaz web de seguimiento del proveedor.	Reporte de firewall. *Reporte de la* Herramienta de monitoreo del proveedor de conectividad
2	Revisar y gestionar la reputación (listas negras) de domínio fonprecon.gov.co. ip públicas y mail.fonprecon.gov.co, mediante herramientas gratuitas online como mxtoolbox	Reporte de plataforma gratuita de monitoreo online.
3	*Mantener la segmentación de la red para estaciones de trabajo*	

	y periféricos, equipos del centro de datos, DMZ, VPN, direcciones ip públicas *Identificación de redes de confianza y opcionales en las reglas del firewall de borde y firewall de equipos de punto final*	
4	Direccionar el tráfico de red de servicios disponibles en internet, mediante reglas de firewall y NAT.	
5	En las reglas de firewall que lo permitan, habilitar control georreferenciado, filtro de aplicaciones, spam, IPS, APT	
6	Los servicios tecnológicos disponibles en internet como el sitio web, certificados en línea, entre otros, deben incluir un certificado SSL	
7	Todas las reglas de firewall debe incluir registro de logs	
8	El firewall a nivel de sistema operativo, debe estar habilitado y afinado según se requiera en casos específicos como el sitio web	
9	El servicio de internet corporativo debe suministrarse a través de un canal dedicado y contar con redundancia.	
10	La red WIFI gratis para la gente, no usa credenciales y su uso es responsabilidad del visitante. Su disponibilidad e instrucciones se informan de manera visible en el área de atención al usuario.	
11	La red WIFI corporativa está restringida por clave de acceso y permisos de conectividad mediante MAC y dirección IP reservada. Los equipos que no son propiedad de Fonprecon, deben someterse a revisión de cumplimiento de requisitos como sistema operativo y antivirus actualizado y en ciclo de vida vigente del fabricante	
12	*Ante un cambio de proveedor de internet, Informar las direcciones IP públicas por las cuales salen las comunicaciones de Fonprecon hacia internet a las áreas de: Subdirección Administrativa y financiera, contabilidad, sub dirección de prestaciones económicas, historia laboral y afiliaciones, a fin de que dichas direcciones IP sean informadas y autorizadas en las diferentes entidades financieras y otros que por seguridad restringen sus servicios a las direcciones IP públicas de internet de las entidades.*	*Trazabilidad en correo electrónico*
13	*Los cables que transportan energía, datos, voz o servicios de información de apoyo deben estar protegidos contra la interceptación, las interferencias o los daños, mediante la disposición y uso de tableros eléctricos y centro de cableado en*	

	una zona aislada y controlada. *La distribución del cableado al punto final debe realizarse mediante el uso de canaleta y tomas de conexión documentadas de acuerdo con el circuito eléctrico al que pertenece en el tablero y el puerto del path panel en el caso del cableado de voz y datos.*	*Documentación del cableado*

7.8 TRANSFERENCIA DE INFORMACIÓN			
N°	**ACTIVIDAD**	**RESPONSABLE**	**DOCUMENTO REGISTRO Y OBSERVACIONES**
1	La información de bases de datos es transmitida y consultada, por acciones exclusivas de funcionarios, contratistas o proveedores para quien intermedia: • Autorización de credenciales de acceso con los niveles de acceso requeridos • Acuerdo de confidencialidad firmado entre las partes	Funcionarios, contratistas y terceros	Control de acceso Acuerdo de confidencialidad
2	Para compartir documentos con terceros, se realiza mediante: • Correo electrónico, cuando el tamaño adjunto lo permite • Mediante el recurso de nube Microsoft 365, cuando el tamaño de los documentos supera la capacidad de adjuntos de un correo electrónico, para lo cual, se configura el acceso temporal mediante enlace web que caduca en una fecha y clave de acceso • Funcionarios con licencia de Microsoft 365	Funcionarios	Trazabilidad de la actividad
3	Para reportar estadísticas, informes y otros ante entes de control, se hace en las plataformas dispuestas para ello y que otorgan trazabilidad	Profesional y Contratista Asesor Oficina de Planeación y Sistemas	Trazabilidad de la plataforma
4	*La entrega o solicitud de copias de*	*Profesional*	*Formato de entrega o*

7.8 TRANSFERENCIA DE INFORMACIÓN			
N°	**ACTIVIDAD**	**RESPONSABLE**	**DOCUMENTO REGISTRO Y OBSERVACIONES**
	seguridad en cintas magnéticas alojadas en bodega externa, se transportan bajo las directrices y alcance de contrato vigente, acuerdos de niveles de servicio y acuerdo de confidencialidad relativo al contrato	*administrador de copias de seguridad Oficina de Planeación y Sistemas*	*solicitud de cintas en custodia*
5	La tercerización de servicios en la nube, prevé las recomendaciones de la circular 005 de 2019 de la *Superintendencia Financiera de Colombia*, así como la protección de los datos personales.	Profesional y Contratista Asesor Oficina de Planeación y Sistemas	
6	*Aplicar filtrado web mediante reglas de la gestión unificada de amenazas UTM, en la seguridad de borde, para:* • *Aplicaciones no deseadas y contenido malicioso* • *Restricción según clasificación de contenido o servicio* • *Perfiles de navegación en internet en los usuarios del directorio activo* • *Geolocalización* • *SPAM* • *Antivirus* *Filtros en la solución de correo, mediante:* • *Reglas para contenido específico en el flujo de correo* • *SPAM* • *Configuraciones de Microsoft defender* • *Reglas SPF, DKIM y DMARC* • *Listas negras de remitentes* • *Antivirus*	Profesional y Contratista Asesor Oficina de Planeación y Sistemas	

7.8 TRANSFERENCIA DE INFORMACIÓN			
N°	**ACTIVIDAD**	**RESPONSABLE**	**DOCUMENTO REGISTRO Y OBSERVACIONES**
7	La información en transporte, pasa por el dispositivo de seguridad unificada de borde, que filtra el contenido según privilegios de los usuarios, reglas y acciones de seguridad (spam, ips, apt, antivirus, entre otros) para bloquear estas comunicaciones o permitirlas bien sea hacia destinos en internet o en la red LAN	Profesional y Contratista Asesor Oficina de Planeación y Sistemas	

7.9 USUARIOS RESTRINGIDOS			
N°	**ACTIVIDAD**	**RESPONSABLE**	**DOCUMENTO REGISTRO Y OBSERVACIONES**
1	Los usuarios de red se configuran en las estaciones de trabajo, con el menor privilegio, que le permita el uso de recursos compartidos y ejecución de software. En ningún caso debe configurar permisos elevados para tareas administrativas o instalación de software	Personal de gestión tecnológica con tareas de soporte técnico	
2	Las tareas administrativas, soporte, mantenimiento, traslado e instalación de software, lo realiza el personal autorizado de Gestión Tecnológica-Mesa de Ayuda o en su defecto realiza la supervisión cuando el servicio lo presta un tercero	Personal de gestión tecnológica con tareas de soporte técnico	
3	Los usuarios con privilegios elevados para actividades administrativas de la plataforma tecnológica se gestionan y custodian según el procedimiento de custodia de credenciales para gestión de TI	Oficina de Planeación y Sistemas Gestión tecnológica	
4	El usuario Administrador local de las estaciones de trabajo con sistema operativo Windows, está habilitado y su contraseña se actualiza paródicamente	Personal de gestión tecnológica con tareas de soporte técnico	

7.9 USUARIOS RESTRINGIDOS			
N°	**ACTIVIDAD**	**RESPONSABLE**	**DOCUMENTO REGISTRO Y OBSERVACIONES**
	y se almacena de forma automática en el directorio activo, lo cual, se consulta con el nombre del pc.		
5	Controles del procedimiento • Automatización en la recolección de logs y las alertas de los sistemas operativos, correo y otros. • Reportes de herramienta de software para inventario de activos de TI. • Reportes en tiempo real de las alertas de fallas en la conectividad de red. • Reglas de control perimetral para comunicaciones de red, mediante el firewall de borde. • Segmentación de la red • Control de credenciales con privilegios administrativos.	Profesional y Contratista Asesor Oficina de Planeación y Sistemas	Las actividades son controles y se encuentran en el capítulo 8 controles existentes

7.10 GESTIÓN DE MONITOREO Y SUS REGISTROS			
N°	**ACTIVIDAD**	**RESPONSABLE**	**DOCUMENTO REGISTRO Y OBSERVACIONES**
1	Mantener operativos los siguientes sistemas de monitoreo Realizar seguimiento y remediación de alertas: • **Uptime Robot:** Servicio en internet con licenciamiento básico para monitorear en tiempo real los servicios web así como los canales ISP, con alertas de caída del servicio reportando a cuentas de correo electrónico de personal de TI • **CheckMK:** Servicio en la red LAN para monitoreo de los activos (hardware) del centro de datos,	Profesionales, técnicos y contratista Asesor Oficina de Planeación y Sistemas	Gestión de incidentes según hallazgos o alertas de estas herramientas

7.10 GESTIÓN DE MONITOREO Y SUS REGISTROS			
N°	**ACTIVIDAD**	**RESPONSABLE**	**DOCUMENTO REGISTRO Y OBSERVACIONES**
1	activado con licencia community sobre Linux, con interface de seguimiento de alertas y estado • **Windows Admin Center:** Alternativa para gestión y administración de plataforma de virtualización y servidores físicos GUI y CORE • **Plataformas ISP:** interfaces en línea para monitoreo de canales de internet, provisto por los prestadores del servicio de canales de internet • **Watchguard Dimension:** Servicio en la red LAN para gestión de logs derivados de la solución UTM de borde para seguridad y ciberseguridad • **LanSwepper:** Sistema de información licenciado anualmente para gestión y trazabilidad del inventario (hardware, garantía, seriales, usuarios, software instalado, logs, almacenamiento, reportes personalizados, etc) de hardware en las redes de comunicación de la Entidad, incluye equipos del centro de datos, estaciones de trabajo, impresoras y demás activos conectados a la red • **Integrated Lights-Out (iLO):** Interfaces de acceso remoto y gestión de servidores Hewlett Packard • **Integrated Dell Remote Access Controller (iDRAC):** Interfaces de acceso remoto y gestión de servidores DELL	Profesionales, técnicos y contratista Asesor Oficina de Planeación y Sistemas	

7.11 PROTECCIÓN DE ACTIVOS DE INFORMACIÓN DURANTE PRUEBAS DE AUDITORÍA

Responsables: jefe Oficina Asesora de Planeación y Sistemas, administrador del activo de información, jefe del proceso auditado, líder de auditoría

N°	*ACTIVIDAD*	*DOCUMENTO REGISTRO Y OBSERVACIONES*
1	*Identificar el activo objetivo de la auditoría*	*Trazabilidad documentada*
2	*Solicitar y revisar el plan de auditoria y retroalimentar los afinamientos o aclaraciones del caso*	*Trazabilidad documentada*
3	*Acordar con los interesados, el tipo de acceso (roles, permisos, consulta, transformación, procesamiento)*	*Trazabilidad documentada*
4	*Activar ambiente de pruebas para un acceso con alcance de transformación y procesamiento de información*	*Trazabilidad documentada*
5	*Crear las credenciales, roles y permisos de acceso*	*Trazabilidad documentada*
6	*Citar a los interesados requeridos a las sesiones de auditoría*	*Trazabilidad documentada*
7	*Eliminar ambiente de pruebas al finalizar la actividad*	*Trazabilidad documentada*
8	*Desactivar accesos al finalizar la actividad*	*Trazabilidad documentada*

7.12 ELIMININACIÓN SEGURA DE INFORMACIÓN

Responsables: jefe Oficina Asesora de Planeación y Sistemas, administrador del activo de información, jefe del proceso dueño del activo, coordinador de gestión documental

N°	*ACTIVIDAD*	*DOCUMENTO REGISTRO Y OBSERVACIONES*
1	*Identificar el activo de información*	*Trazabilidad documentada*
2	*Seleccionar y justificar la causa para la eliminación de la información:* • *Información innecesaria* • *Baja de equipo obsoleto* • *Reutilización de medios de almacenamiento* • *Fin de retención se acuerdo con tablas de retención según alcance de gestión documental* • *Liberar espacio de almacenamiento* • *Otras*	*Trazabilidad documentada*

7.12 ELIMININACIÓN SEGURA DE INFORMACIÓN

Responsables: jefe Oficina Asesora de Planeación y Sistemas, administrador del activo de información, jefe del proceso dueño del activo, coordinador de gestión documental

N°	ACTIVIDAD	DOCUMENTO REGISTRO Y OBSERVACIONES
3	*Determinar la necesidad y alcance de retención de copia de seguridad*	*Trazabilidad documentada*
4	*Realizar copia de seguridad de acuerdo con la necesidad y alcance*	*Trazabilidad documentada*
5	*Realizar el borrado seguro de acuerdo con las acciones documentadas en el procedimiento denominado:* ***gestión de equipos, software y redes de punto final***	*Formatos del procedimiento indicado*
6	*Generar informe y socializar con los interesados*	*Trazabilidad documentada*

7.13 SEGREGACIÓN DE DEBERES

Responsables: jefe Oficina Asesora de Planeación y Sistemas, jefe del proceso dueño del activo

N°	ACTIVIDAD	DOCUMENTO REGISTRO Y OBSERVACIONES
1	*Identificar el activo de información, sus roles y permisos de acceso*	*Trazabilidad documentada*
2	*Identificar los roles y alcance de funciones o actividades contractuales de las personas que administran el activo*	*Trazabilidad documentada*
3	*Asignar de manera segregada, los roles y permisos para:* • *Administradores de sistemas de información, identidades y gestión de acceso* • *Administradores de bases de datos, redes, seguridad y ciberseguridad, centro de datos* *Estos roles no deberían concentrarse en una sola persona*	*Trazabilidad documentada*
4	*Generar informe y socializar con los interesados*	*Trazabilidad documentada*

7.14 DISPOSICIÓN SEGURA DE EQUIPOS

Responsables: jefe Oficina Asesora de Planeación y Sistemas, coordinador de bienes y servicios, coordinador de almacén, ingenieros de gestión tecnológica

N°	***ACTIVIDAD***	***DOCUMENTO REGISTRO Y OBSERVACIONES***
1	***Equipos del centro de datos****:* • *Identificación mediante serial, modelo, marca, placa de inventario de almacén, unidad de rack* • *Asignación de responsable del inventario del activo* • *Identificar los equipos de terceros* • *Disposición de equipos en gabinetes separados según rol de comunicaciones, servidores, voz, energía, aire, otros* • *Disposición de equipos servidores con anclaje seguro en rieles* • *Disposición de equipos de comunicación con anclaje mediante tornillos en las unidades del rack respectivo* • *Cables de red documentados en sus extremos* • *Disposición de equipos en zona exclusiva con control acceso restringido para personal autorizado con huella y tarjeta de proximidad* ***Equipos de punto final:*** • *Identificación mediante serial, modelo, marca, placa de inventario de almacén* • *Asignación de responsable del inventario del activo* • *Identificar los equipos de terceros* • *Disposición de puestos de trabajo según condiciones de seguridad y salud en el trabajo y que soporten el peso de los equipos asignados* • *Disposición de equipos en el puesto de trabajo* • *Disposición de impresoras y escáner en una base solida que soporte el peso del activo* • *Conexiones de red y energía mediante las tomas de canaleta haciendo uso de cables en buen estado en la categoría apropiada*	*Documentación actualizada desde al alcance de gestión tecnológica y almacén*

8. CONTROLES

Norma técnica colombiana NTC-ISO 27001:2022 Anexo A:

- ***5.3 Segregación de deberes:*** *Los deberes y áreas de responsabilidad en conflicto deberían segregarse*
- ***5.7 Inteligencia de amenazas****: La información relativa a las amenazas a la seguridad de la información se debe recopilar y analizar para producir inteligencia de las amenazas*
- ***5.37 Procedimientos operativos documentados:*** *Los procedimientos operativos de las instalaciones de procedimiento de la información de debe documentar y poner a disposición del personal que los necesite*
- ***6.7 Trabajo remoto:*** *Las medidas de seguridad se deben implementar cuando el personal trabaje de forma remota para proteger la información a la que se accede, procesa o almacena fuera de las instalaciones de la organización*
- ***7.10 Medios de almacenamiento:*** *Los medios de almacenamiento deben gestionarse a lo largo de su ciclo de vida de adquisición, uso, transporte y disposición de acuerdo con el esquema de clasificación y los requisitos de manipulación de la organización*
- ***7.12 Seguridad del cableado:*** *Los cables que transportan energía, datos o servicios de información de apoyo deben estar protegidos contra la interceptación, las interferencias o los daños*
- ***7.14 Disposición o reutilización segura de los equipos****: Los elementos de los equipos que contengan medios de almacenamiento se deben verificar para asegurarse de que los datos sensibles y el software con licencia se han eliminado o sobrescrito de forma segura antes de su disposición o reutilización*
- ***8.1 Dispositivos de punto final de usuario:*** *Se debe proteger la información almacenada, procesada o accesible a través de los dispositivos de punto final del usuario*
- ***8.6 Gestión de la capacidad:*** *EL uso de los recursos se debe monitorear y ajustar en función de las necesidades de capacidad actuales y previstas*
- ***8.8 Gestión de vulnerabilidades técnicas****: Se debe obtener información sobre las vulnerabilidades técnicas de los sistemas de información en uso, se debe evaluar la exposición de la organización a dichas vulnerabilidades y se debe adoptar las medidas apropiadas*
- ***8.9 Gestión de la configuración:*** *Las configuraciones, incluidas las configuraciones de seguridad, de hardware, software, servicios y redes se deben establecer, documentar, implementar, monitorear y revisar*
- ***8.10 Eliminación de información:*** *La información almacenada en los sistemas de información, dispositivos o en cualquier otro medio de almacenamiento se debe eliminar cuando ya no se necesario*
- ***8.15 Registro:*** *Los registros que guarden actividades, excepciones, fallas y otros eventos pertinentes se deben producir, almacenar, proteger y analizar*

- ***8.16 Actividades de seguimiento:*** *Se debe monitorear el comportamiento anómalo de las redes, los sistemas y las aplicaciones y se deben adoptar las medidas adecuadas para evaluar posibles incidentes de seguridad de la información*
- ***8.17 Sincronización de reloj:*** *Los relojes de los sistemas de procesamiento de información utilizados por la organización se deben sincronizar con las fuentes de tiempo aprobadas*
- ***8.20 Seguridad de redes:*** *Las redes y los dispositivos de red deben estar asegurados, gestionados y controlados para proteger la información de los sistemas y las aplicaciones*
- ***8.21 Seguridad de los servicios de red:*** *Se deben identificar, implementar y monitorear los mecanismos de seguridad, los niveles de servicio y los requisitos de servicio de los servicios de red*
- ***8.22 Segregación de redes:*** *Los grupos de servicios de información, los usuarios y los sistemas de información deben estar segregados en las redes de la organización*
- ***8.23 Filtrado web:*** *El acceso a sitios web externos se debe gestionar para reducir la exposición de contenido malicioso*
- ***8.31 Separación de entornos de desarrollo, evidencia y producción:*** *Los entornos de desarrollo, ensayo y producción deben estar separados y protegidos*
- ***8.34 Protección de los sistemas de información durante las pruebas de auditoría:*** *Las pruebas de auditoría y otras actividades de aseguramiento que impliquen la evaluación de los sistemas operativos se deben planificar y acordar conjuntamente entre el aprobador y la dirección adecuada*

9. FORMATOS Y ANEXOS

Hoja de cálculo: Administración TI. Código F01-PRO-GTC-002