1. OBJETIVO

Establecer un proceso formal y estructurado para definir, implementar, monitorear y mantener las configuraciones seguras de todos los activos de tecnología de la información de la Superintendencia de Sociedades. Esto tiene como fin minimizar las vulnerabilidades, prevenir cambios no autorizados y asegurar la integridad, disponibilidad y confidencialidad de la información.

2. ALCANCE

Este procedimiento es aplicable a toda la infraestructura tecnológica de la entidad, lo que incluye, pero no se limita a:

- **Hardware:** Servidores, estaciones de trabajo, equipos portátiles, dispositivos de red (switches, routers) y dispositivos móviles.
- **Software:** Sistemas operativos, bases de datos, servidores de aplicaciones y software base.
- **Servicios en la nube:** Plataformas IaaS, PaaS y SaaS, con especial énfasis en Microsoft 365.
- **Redes:** Configuraciones de seguridad de la red, VLANs, reglas de firewall y servicios de red.

3. RESPONSABLES

Coordinadores Grupos de la DTIC: Definir y mantener actualizadas las líneas base de configuración de la plataforma tecnológica, apoyar la implementación de las líneas base y monitorear su funcionamiento
Gestores de Cambios: Presentar los cambios a la configuración realizados en la reunión de aprobación de cambios y realizar monitoreo de su funcionalidad
Líderes Técnicos / Administradores de Sistemas: Implementar las líneas base definidas para los elementos que forman parte de la Infraestructura, definir y solicitar al grupo GSAT la inclusión de la información de configuración para realizar el respectivo backups y pruebas de restauración.

4. DEFINICIONES

Gestión de la Configuración: Proceso para identificar, documentar, controlar y auditar los elementos de configuración de las VPN.
Evento: Una alerta o notificación creada por algún componente de la plataforma tecnológica de la información o herramienta de monitoreo.
Incidente: Es un evento o serie de eventos de seguridad de la información no deseado o no planeado, que afecte la prestación del servicio o reduzca la calidad de la prestación del servicio o que tenga una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Infraestructura tecnológica: Es parte de la plataforma tecnológica Software, Hardware, Microcomputadores, Portátiles, redes LAN (cableado y equipos activos), redes WAN (regionales e Internet), Firewall (seguridad perimetral, alta disponibilidad), administración de ancho de banda, servidor de comunicaciones, telefonía (voz local y con regionales), video, Wireless, servidor de Bases de Datos, servidor de aplicaciones, aplicaciones (página Web, Intranet), Correo electrónico (Exchange), etc.
Log: Es el registro de las acciones y de los acontecimientos que ocurren en un sistema computacional cuando un usuario o proceso está activo y sucede un evento que está configurado para reportar. Rastro de lo que se está ejecutando sobre la plataforma tecnológica.
Software base: Corresponde al sistema operativo y software que soporta la infraestructura tecnológica de la Entidad incluyendo el software embebido en el hardware.
VPN SSL (Secure Sockets Layer): Mecanismo que permite el acceso remoto seguro de usuarios mediante autenticación y cifrado TLS/SSL.
VPN Site-to-Site: Conexión segura establecida entre sedes de la organización o con terceros autorizados, mediante túneles IPsec.

5. CICLO DE VIDA DE LA GESTIÓN DE LA CONFIGURACIÓN

5.1. LINEAMIENTOS GENERALES

- Monitorizar frecuentemente, si los componentes de la plataforma tecnológica requieren ser actualizados, y realizar las actualizaciones, si aplica, garantizando la prestación del servicio.
- Las actualizaciones de las versiones de software y hardware deben ser presentadas y aprobadas en el comité de cambios.
- Una vez se realicen las actualizaciones requeridas se deben aplicar pruebas y dejar operando la plataforma actualizada.
- Cuando se implementa un nuevo proyecto en la infraestructura, servicios, redes, se debe garantizar que su ejecución se lleve a cabo siguiendo las buenas prácticas recomendadas por el fabricante.
- Cuando sea necesario realizar ajustes o modificaciones debido a cambios en la infraestructura, identificación de mejoras tras auditorías, recomendaciones del fabricante, o para abordar nuevas amenazas se debe seguir lo establecido en el Procedimiento GTI-PR-006_CambiosAmbienteProductivo.
- Toda configuración aplicada debe formar parte del respaldo lógico (exportación de políticas o snapshots de configuración cuando sea posible), y debe ser documentada en los repositorios designados por la Dirección de Tecnología.

- Cuando se implemente un producto y/o servicio de un tercero el Coordinador de Sistemas y arquitectura de Tecnología o el responsable del proyecto debe garantizar que las configuraciones sean documentadas y almacenadas.
- Cuando se contrate un servicio de terceros o se integren aplicaciones externas a Microsoft 365 (por ejemplo, conectores, apps en Teams, herramientas de firma electrónica, etc.), el **Coordinador de Sistemas y Arquitectura de Tecnología** o el responsable del proyecto deberá garantizar que:

    - Las configuraciones y permisos asignados estén documentados.
    - Se almacene dicha documentación como parte del expediente del proyecto.
    - Se evalúe el cumplimiento de las políticas de seguridad antes de su habilitación.

El proceso de gestión de la configuración se desarrollará en cinco fases cíclicas para asegurar una mejora continua.

5.2. Fase 1: Definición y Documentación de Configuraciones Seguras (Línea Base)

Propósito: Establecer plantillas o "líneas base" de configuración segura para los tipos de activo tecnológico. Estas líneas base son el estándar autorizado contra el cual se medirán todos los sistemas, por tratarse de información clasificada deben ser mantenidos por cada uno de los administradores de la plataforma.

Actividades:

5.2.1. Catálogo de Infraestructura

Se debe contar con un catálogo actualizado de cada uno de los elementos que conforman la plataforma tecnológica de la entidad, este catálogo debe tener como mínimo la siguiente información: Código del elemento, tipo de elemento (bases de datos, servidores físicos, servidores virtuales, sistemas operativos y licenciamiento, dispositivos de red, entre otros), nombre del elemento, descripción del elemento, especificación técnica, versión, identificación de licencia, tipo de servicio (SaaS, IaaS), sistemas que impacta, ambiente de trabajo que soporta (producción, pruebas, desarrollo) y otra información técnica que corresponda.

Deben existir planes de mantenimiento preventivo y correctivo sobre los elementos que conforman el catálogo de infraestructura de TI.

5.2.2. Definir Configuraciones Estándar

Crear y documentar las configuraciones seguras para cada categoría de activo. Estas deben basarse en:

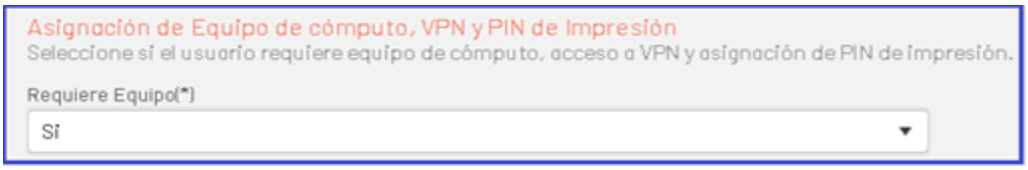
- Las recomendaciones del fabricante.
- Las buenas prácticas de la industria.
- Los lineamientos específicos detallados en el Anexo 1 de este documento allí se incluyen parámetros para:
  - Bases de Datos (p. ej., cambio de puertos, roles, deshabilitación de xp_cmdshell).
  - Servidores (p. ej., protección contra malware, políticas de cuentas y contraseñas).
  - Redes y Comunicaciones (p. ej., deshabilitar Telnet, configurar VLANs, actualizar firmware).
  - Servidores de Aplicaciones (WildFly/WAS).
  - Microsoft 365 (p. ej., políticas de Exchange Online, Teams, Entra ID).
  - Seguridad en la Nube y Endpoints.

5.2.3. Asignación, Alistamiento y Sincronización de Equipos

La asignación y alistamiento de equipos de cómputo se gestiona a través de la herramienta ITSM institucional mediante el servicio Formato 46001, específicamente a través de las categorías Aprovisionamiento de Usuario y Modificar Permisos.



Durante el registro de la solicitud, cuando se requiera la entrega o reasignación de un equipo de cómputo, el solicitante deberá seleccionar el tipo de usuario correspondiente (funcionario, contratista, judicante, practicante laboral o proveedor) y marcar la opción "Sí" en el campo "Requiere Equipo".



Una vez registrada la solicitud, la herramienta gestionará automáticamente el flujo de aprobación correspondiente ante el directivo responsable de la dependencia solicitante.

Posteriormente, una vez obtenida la aprobación jerárquica de la solicitud, la herramienta generará las tareas:

• Asignación de Equipo de Cómputo, responsable: Coordinador del Centro de Servicios Tecnológicos (CST).

• Configuración de Equipo y Perfil de Usuario, responsable: Agentes Nivel 1 del Centro de Servicios Tecnológicos (CST).

- **Sincronización de dispositivo en plataformas Microsoft**, responsable: Administrador de plataformas Microsoft designado.

La tarea "Asignación de Equipo de Cómputo" tiene como propósito validar la disponibilidad de equipos y determinar el tipo de dispositivo que puede ser asignado de acuerdo con el perfil del usuario solicitado. Así mismo, permite controlar la aprobación de la entrega o reasignación del activo tecnológico.

La tarea **"Configuración de Equipo y Perfil de Usuario"** tiene como propósito ejecutar las actividades de alistamiento definidas en la presente guía, registrar la gestión realizada durante su ejecución y generar las evidencias correspondientes del proceso.

Una vez el Coordinador del Centro de Servicios Tecnológicos (CST) haya gestionado la tarea **"Asignación de Equipo de Cómputo"** y definido el equipo que será **asignado al usuario**, el Agente Nivel 1 del CST deberá verificar que se encuentren dadas las condiciones necesarias para iniciar el proceso de configuración del equipo, de conformidad con el procedimiento establecido por la entidad.

Durante la ejecución de la tarea, el agente deberá documentar en tiempo real la gestión realizada, registrando las actividades ejecutadas y las novedades identificadas, con el fin de garantizar la trazabilidad del proceso desde el inicio del alistamiento hasta su finalización.

Una vez identificado el equipo que será objeto de configuración, el agente deberá actualizar el campo **Asunto** de las tareas **"Configuración de Equipo y Perfil de Usuario"** y **"Sincronización de dispositivo en plataformas Microsoft"**, registrando el número de placa del equipo asignado. Este registro permitirá identificar el activo tecnológico durante todo el flujo de atención y facilitar la generación de consultas, reportes y la trazabilidad de la información registrada en la herramienta ITSM.

Así mismo, el agente deberá mantener actualizada la información registrada en ambas tareas, incorporando las actividades realizadas, las novedades identificadas y cualquier información requerida durante la gestión, con el fin de garantizar la continuidad del proceso de sincronización del dispositivo por parte del Administrador de Plataformas Microsoft.

Finalizadas las actividades de configuración y alistamiento, el agente deberá diligenciar el formato **GTI-FM-033 Verificación de Alistamiento de Equipos**, adjuntarlo a la tarea **"Configuración de Equipo y Perfil de Usuario"** y registrar la finalización de la gestión realizada.

La tarea "**Sincronización de dispositivo en plataformas Microsoft**" tiene como propósito realizar el registro del dispositivo en las plataformas Microsoft administradas por la entidad, utilizando la información documentada durante el proceso de alistamiento.

El Administrador de Plataformas Microsoft deberá verificar la información registrada por el Agente Nivel 1 del Centro de Servicios Tecnológicos (CST) y ejecutar las actividades de sincronización del dispositivo en **Microsoft Entra ID**, **Microsoft Intune** y **Microsoft Defender**, garantizando la incorporación del dispositivo a las plataformas de administración, gestión y protección definidas por la entidad.

Aunque las tareas son generadas de manera simultánea por la herramienta ITSM, las actividades de configuración y alistamiento únicamente podrán iniciarse una vez el Coordinador del CST haya gestionado la tarea "Asignación de Equipo de Cómputo" y definido el equipo que será asignado al usuario.

Las actividades descritas a continuación corresponden a las actividades técnicas que deben ejecutarse durante la gestión de la tarea **"Configuración de Equipo y Perfil de Usuario"**.

5.2.3.1 Preparación Inicial del Equipo

La preparación inicial tiene como propósito garantizar que el equipo cumpla con los estándares técnicos, de seguridad y conectividad definidos por la entidad antes de ser entregado al usuario final.

Como parte de esta actividad, el agente responsable deberá:

- Instalar o verificar que el equipo cuente con el sistema operativo autorizado por la entidad en la versión vigente y compatible con los servicios y plataformas institucionales.

- Verificar y aplicar las actualizaciones disponibles del sistema operativo, controladores y demás componentes del equipo, utilizando las herramientas o mecanismos definidos por la entidad, hasta garantizar que el dispositivo se encuentre actualizado y apto para su operación.

- Verificar la existencia y configuración de la cuenta de administración local definida por la entidad para la gestión y soporte de los equipos. Cuando se trate de una instalación limpia o reinstalación del sistema operativo, deberá realizar la configuración correspondiente.

- Verificar que la configuración de almacenamiento del equipo cumpla con los lineamientos definidos por la entidad.

  Para ello, deberá confirmar la existencia de las siguientes particiones:

  • C: destinada al sistema operativo y aplicaciones.
  • D: destinada a la sincronización de la información institucional del usuario mediante OneDrive.

  Cuando la partición D: no exista, el agente deberá realizar la configuración correspondiente antes de continuar con las actividades de alistamiento.

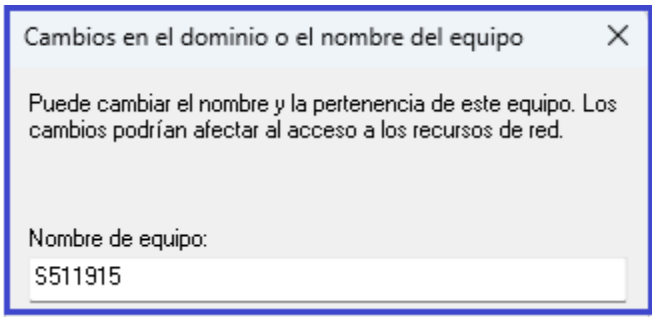
- Gestionar el traslado del equipo a la Unidad Organizativa (OU) definida por la entidad para los equipos de usuario final, mediante los mecanismos establecidos por la entidad para la atención de

requerimientos de Directorio Activo, garantizando la correcta aplicación de las políticas institucionales.

- Configurar el Control de Cuentas de Usuario (UAC) de acuerdo con los parámetros definidos para la administración y soporte de los equipos de cómputo, esta configuración se aplica desde una directiva.

5.2.3.2 Nombramiento de Equipo

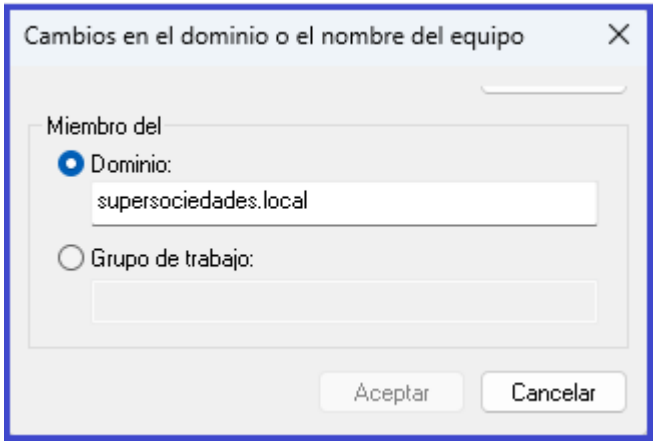
El agente responsable deberá asignar al equipo el nombre definido por la entidad para la identificación y administración de los activos tecnológicos, de acuerdo con la convención institucional vigente.



5.2.3.3 Unión al dominio

El agente responsable deberá integrar el equipo al dominio institucional definido por la entidad.

Una vez realizada la unión al dominio, deberá reiniciar el equipo para aplicar la configuración y continuar con las actividades de alistamiento.



5.2.3.4 Configuración del perfil de usuario

Solicitar al usuario asignado que inicie sesión en el equipo utilizando sus credenciales institucionales. Este proceso permitirá la creación del perfil de usuario y la validación del acceso al equipo.

Una vez realizado el inicio de sesión, se deberá verificar que el acceso se haya efectuado correctamente antes de continuar con la configuración del software base.

5.2.3.5 Proceso: Configuración de Software Base

Como parte del proceso de alistamiento, el agente responsable deberá garantizar que la línea base de software institucional para estaciones de trabajo se encuentre instalada, configurada y funcionando correctamente antes de la entrega del equipo al usuario.

Cuando alguno de los componentes de la línea base no se encuentre disponible en el equipo, el agente deberá realizar su instalación y configuración de acuerdo con los lineamientos definidos por la entidad.

Con el fin de optimizar los tiempos de entrega del equipo, el agente deberá realizar previamente las actividades que no requieran autenticación con las credenciales institucionales del usuario. Posteriormente, una vez el usuario haya iniciado sesión y se haya creado su perfil, deberá completar las configuraciones asociadas a su cuenta institucional.

La entidad define la siguiente línea base de software para estaciones de trabajo, la cual deberá ser verificada, instalada cuando aplique y configurada durante el proceso de alistamiento del equipo:

Línea base de software para estaciones de trabajo

- **Agente de ITSM:** Instalar y verificar la correcta ejecución del servicio.
- **Gestor Documental (GeDeSS):** Verificar los parámetros de configuración del editor en línea.

- **Lector de PDF (Acrobat Reader):** Verificar que se encuentre establecido como aplicación predeterminada y funcionando correctamente para la visualización de documentos PDF.

- **Compresor de archivos (7-ZIP):** Verificar que se encuentre instalado.

- **Aplicaciones de Microsoft 365:**

  - **Outlook:** Configurar la cuenta institucional y anclar a la barra de tareas.
  - **Teams:** Configurar la cuenta institucional y anclar a la barra de tareas.
  - **OneDrive:** Sincronizar con la cuenta institucional en la partición D: del equipo.

- **Navegadores Web:**

  - **Microsoft Edge:** Verificar actualización, sincronizar con la cuenta institucional y anclar a la barra de tareas.
  - **Google Chrome:** Verificar actualización y anclar a la barra de tareas.

- **Cola de impresión:** Instalar los controladores correspondientes desde el servidor de impresión, seleccionando la cola de impresión que corresponda de acuerdo con las necesidades del usuario.

- **Software adicional:** En caso de que el usuario solicite la instalación de software diferente al definido como software base de alistamiento, este deberá ser registrado en el campo correspondiente de la lista de verificación GTI-FM-033 Verificación de Alistamiento de Equipos, indicando el software solicitado.

5.2.3.6 Comprobaciones

Una vez finalizada la configuración del equipo, el agente responsable deberá realizar las validaciones necesarias para garantizar su correcto funcionamiento.

- **Perfiles de usuario en Windows:** Verificar en la ruta **C:\Usuarios** que únicamente se encuentren los perfiles correspondientes al usuario administrador autorizado y al usuario asignado al equipo.

- **Actualizaciones del sistema operativo:** Realizar una validación final para confirmar que el sistema operativo se encuentre actualizado de acuerdo con las actualizaciones disponibles para su versión.

- **Antivirus:** Verificar que Windows Defender se encuentre activado y actualizado.

- **Navegación a Internet:** Confirmar el acceso a Internet desde el navegador.

- **Agente de ITSM:** Validar que el equipo aparezca registrado en la consola de administración de dispositivos (ADM) de ITSM.

- **Asistencia Rápida:** Verificar que la aplicación se encuentre disponible y anclada a la barra de tareas.

- **Escritorio Remoto:** Verificar que la opción "Permitir conexiones remotas al equipo" se encuentre habilitada y que el usuario asignado esté incluido dentro de los usuarios autorizados, cuando aplique.

- **Información de conexión remota:** Cuando se configure el acceso mediante Escritorio Remoto, suministrar al usuario el número de placa y la dirección IP asignada al equipo, así como las indicaciones básicas para establecer futuras conexiones remotas cuando se encuentre fuera de las instalaciones de la entidad.

- **Intranet Institucional:** Validar el acceso correcto a la intranet de la entidad.

5.2.3.7 Diligenciamiento de la Lista de Verificación para el Alistamiento de Equipos.

La Lista de Verificación para el Alistamiento de Equipos constituye el mecanismo de control utilizado para evidenciar el cumplimiento de las actividades ejecutadas durante el proceso de alistamiento.

El agente responsable deberá diligenciar completamente el formato GTI-FM-033 VerificaciónAlistamientodeEquipos.xls y adjuntarlo a la tarea "Configuración de Equipo y Perfil de Usuario" gestionada en la herramienta ITSM.

El formato GTI-FM-033 VerificaciónAlistamientodeEquipos.xls debidamente diligenciado constituirá la evidencia del proceso de alistamiento realizado sobre el equipo.

5.2.3.8 Conexión a las redes Inalámbricas (WiFi)

Tal como se ilustra en la Figura 1, la red Wifi está protegida por el Firewall.

IMAGEN CLASIFICADA

Figura 1 – Topología de red Wifi

Se cuenta con 3 SSID: INVITADOSSUPERSOC, INTRANETSUPERSOC_BOG e INTRANETSUPERSOC_REG.

- SSID INVITADOSSUPERSOC: Creado en la sede principal de la Entidad en Bogotá, es una red abierta y está destinada para brindar acceso gratuito a los Ciudadanos que visitan la compañía. Esta red se ubica en un segmento externo que NO permite acceso ni enrutamiento de tráfico al interior de la Entidad, solo hacia Internet.

  Este control de acceso y protección se hace a través del Firewall. Además, por políticas de la Entidad, NO se permite redes sociales ni servicio de streaming como Facebook, Instagram, Whatsapp, Youtube, Netflix, etc.

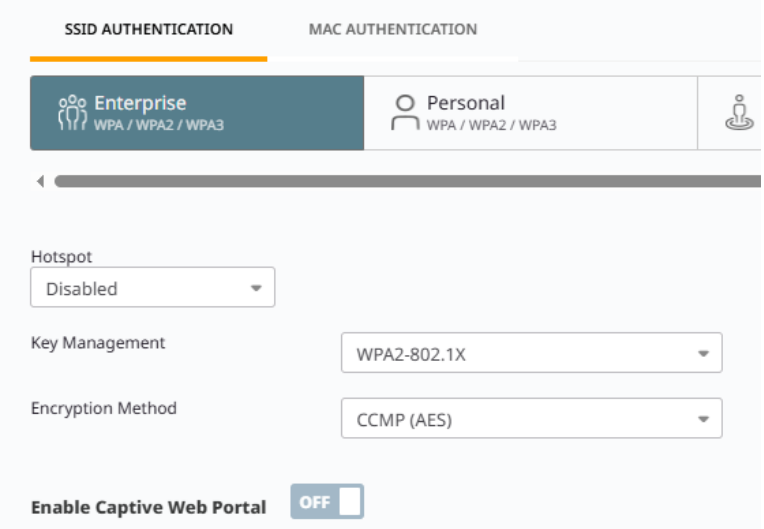
  El acceso a esta red es abierto y no se requiere dar alguna clave. Permite máximo 512 usuarios.

- SSID INTRANETSUPERSOC_BOG e INTRANETSUPERSOC_REG: Estos 2 SSIDs están creados para el uso de equipos y usuarios de red autorizados por los diferentes Coordinadores o Directivos de la Entidad. El primer SSID está disponible para la sede principal en Bogotá y el segundo para todas las Intendencias Regionales.

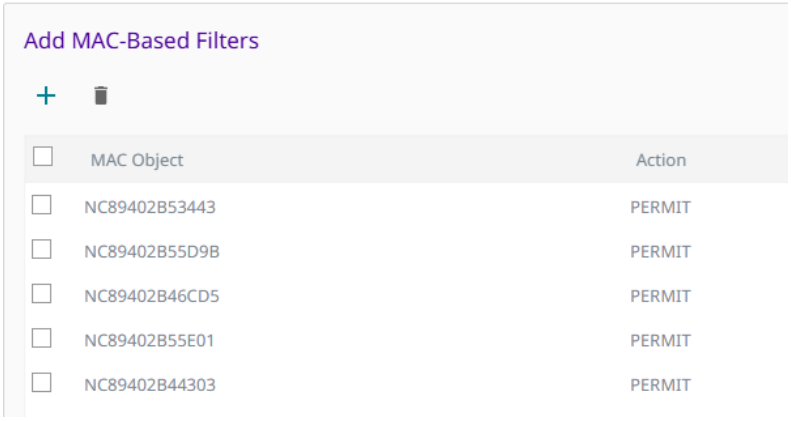
  Estas redes permiten acceso a Internet, a servicios internos como la Intranet y otros servicios como GeDeSS y demás sistemas de información disponibles para los funcionarios.

El control de seguridad se realiza mediante la autenticación del usuario y la validación de su dispositivo autorizado. El usuario es autenticado usando el servicio de RADIUS y la validación del usuario en el Directorio Activo, tal como se ilustra en la Figura 1.

Como doble factor de seguridad, el dispositivo como el portátil, PC o móvil celular es autenticado por su dirección física o MAC. Para la autenticación de usuarios se usa el protocolo WPA Enterprise WPA2-802.1X y un método de cifrado CCMP (AES):



Para la autenticación de los equipos se valida en la "lista blanca" de direcciones físicas del dispositivo o MAC:



Esta gestión se realiza a través de la herramienta de administración centralizada en la nube entregada por el proveedor.

5.2.3.9 Conexiones VPN SSL y VPN Site-to-Site

Las conexiones de VPN aplican para todos los equipos y dispositivos de red que soportan la funcionalidad de VPN SSL y VPN Site-to-Site, el personal de la DTIC responsable de la administración, monitoreo y soporte de las VPN y proveedores externos autorizados con acceso a la infraestructura a través de VPN.

Estas conexiones deben tener los siguientes controles:

- Cifrado robusto (AES-256, SHA-2, DH14 o superior) en Site-to-Site.
- Prohibición de cuentas genéricas.
- Revisión periódica de usuarios activos.
- Revisión semestral de políticas y accesos.
- Cumplimiento de la Política de Seguridad de la Información y normativa colombiana (Ley 1581/2012, Decreto 1377/2013).

El procedimiento para la asignación de las VPN incluye:

- Identificación de configuraciones iniciales.
- Control de Cambios: registro y aprobación en la Reunión de Aprobación de Cambios.
- Revisión Periódica: revisión semestral de políticas y accesos.

Todo cambio debe ser registrado para garantizar trazabilidad y control.

Responsables

- Administrador de Seguridad Perimetral: Configuración, documentación y monitoreo.
- Oficial de Seguridad de la Información: Validar cumplimiento de políticas.
- Jefe de la DTIC: Aprobar cambios de alto impacto.
- Usuarios Finales: Uso responsable de la VPN bajo los lineamientos establecidos.

5.2.3.10 Gestión de Logs y Registros de Auditoría

Permite a la entidad llevar a cabo investigaciones especiales, garantizar el cumplimiento de normativas, verificar eventos de seguridad, alertar sobre posibles ataques informáticos y riesgos de ciberseguridad, entre otros aspectos. Estos deben implementarse conforme a los lineamientos del dominio de Arquitectura de Seguridad, establecidos en la Arquitectura Empresarial V3.

Todos los sistemas de información, aplicaciones, sistemas operativos, bases de datos, dispositivos de comunicación, dispositivos de seguridad y servidores deben contar con logs o rastros de auditoría que registren las actividades de los usuarios, así como excepciones, fallas y eventos de seguridad.

En los proyectos de desarrollo de sistemas, se debe cumplir con el modelo 2.19 *Modelo de Gestión de Rastros de Auditoría* para la correcta generación de archivos de auditoría (*logs*).

Además, debe mantenerse un inventario actualizado de los registros de auditoría existentes en las plataformas tecnológicas y sistemas de información, incluyendo su nombre y ubicación.

Responsables:

- Los Coordinadores de la Dirección de Tecnología de la Información y las Comunicaciones

3. **Repositorio Central**

Todas las plantillas de configuración segura deben ser versionadas y almacenadas en el repositorio central, accesible para el personal autorizado.

Responsables:

- Coordinador Grupo de Sistemas y Arquitectura de Tecnología.
- Coordinador Grupo de Seguridad e Informática Forense.

5.3. Fase 2: Implementación y Aplicación de Configuraciones

Propósito: Asegurar que todos los sistemas, tanto nuevos como existentes, se ajusten a las líneas base de configuración definidas.

Actividades:

1. **Nuevos Activos**

Todo nuevo activo desplegado en el ambiente productivo debe ser configurado utilizando las plantillas aprobadas. El diligenciamiento de la "Lista de Verificación para el Alistamiento de Equipos" es la evidencia para las estaciones de trabajo.
Todos los componentes de la plataforma tecnológica deben estar sincronizados con la hora oficial colombiana y los permisos de acceso de deben aplicar con base en el principio de menor privilegio posible.

2. **Automatización**

Utilizar mecanismos automáticos para aplicar y forzar las configuraciones, como las plantillas a nivel de Directorio Activo y Endpoints mencionadas en el Anexo 1 de este documento, y las políticas de Microsoft Intune para Microsoft 365.

3. Respaldo Inicial

Una vez que un sistema está configurado según su línea base, se debe generar una copia de respaldo de su configuración. Así mismo, coordinar el plan de respaldo de información que incluya los logs de auditoria por medio de la herramienta de backups.

En caso de contar con un Centro de Operaciones de Seguridad (SOC), se deben establecer directrices de retención, respaldo y recuperación de los logs y registros de auditorías de los componentes de la plataforma tecnológica. El Coordinador de Seguridad e Informática Forense debe coordinar con el SOC las directrices de retención, respaldo y recuperación, y Cuando estas directrices se cumplan, aplicar un backup histórico y realizar el borrado en las plataformas tecnológicas y sistemas de información, de los registros de logs consolidados en el backup histórico. Adicionalmente, se debe emitir y revisar trimestralmente los informes generados por la herramienta de respaldo y realizar pruebas de restauración regularmente de acuerdo con el procedimiento GTI-PR-001RESPALDO Y RECUPERACION DE DATOS DE LA INFRAESTRUCTURA TECNOLÓGICA.

4. Operación de la infraestructura

- Se debe realizar las actividades técnicas requeridas para mantener la operación normal de los servicios de TI de acuerdo con la naturaleza de cada componente.

- Deben existir planes de mantenimiento preventivo sobre las plataformas tecnológicas con el objetivo de mantener su funcionamiento.

- Se debe garantizar que el software instalado este debidamente licenciado y con autorización de uso por parte de la entidad.

- Se debe mantener actualizada la información de los usuarios para los diferentes componentes de tecnología, conforme a las novedades y actualizaciones que sean informadas por el área de Talento humano.

- Monitorear frecuentemente, si los componentes de la plataforma tecnológica - requieren ser actualizados, y realizar las actualizaciones, si aplica, garantizando la prestación del servicio.

- Las actualizaciones de las versiones de software base deben ser presentadas y aprobadas de acuerdo con el procedimiento GTI-PR-006 GESTION DE CAMBIOS AMBIENTE PRODUCTIVO.

Una vez se realicen las actualizaciones requeridas se deben aplicar pruebas y dejar operando la plataforma actualizada.

Responsables:

- Administradores de las diferentes plataformas y servicios instalados.
- El Coordinador de Seguridad e Informática Forense
- El Coordinador de Sistemas y Arquitectura Tecnológica
- Responsables de proyectos tecnológicos.

5.4. Fase 3: Gestión de Cambios en la Configuración

Propósito: Controlar estrictamente cualquier modificación a las configuraciones aprobadas para prevenir desviaciones no autorizadas.

Actividades:

1. **Proceso Formal de Cambios**

Cualquier modificación a una configuración de un sistema en producción debe seguir el procedimiento **GTI-PR-006_CambiosAmbienteProductivo**.

2. **Solicitud y Aprobación**

El cambio debe ser solicitado, justificado, evaluado en su impacto y riesgo, y finalmente aprobado en la Reunión de aprobación de cambios de acuerdo con el procedimiento **GTI-PR-006_CambiosAmbienteProductivo**.

3. **Documentación del Cambio**

Se debe documentar el estado de la configuración "antes" y "después" del cambio.

4. **Respaldo Pre-Cambio**

Antes de aplicar un cambio, se debe realizar un respaldo de la configuración actual del activo.

Responsables:

- Gestores de cambio.
- Reunión de Aprobación de Cambios.
- Personal técnico Administradores o implementadores.

5.5. Fase 4: Monitoreo, Verificación y Auditoría

Propósito: Detectar desviaciones de la línea base y verificar continuamente el cumplimiento de las políticas de configuración.

Actividades:

1. **Monitoreo de Desviaciones**

   Los Grupos de la Dirección de Tecnología de Información y las Comunicaciones deben monitorear el estado de los sistemas, su operación, funcionamiento constante y validar la integridad de las configuraciones. Cualquier cambio no autorizado se debe notificar a servicios.tecnologicos@supersociedades.gov.co.

2. **Revisión de Logs**

   Revisar periódicamente los registros (logs) de los sistemas para identificar cambios de configuración, intentos de acceso no autorizados o errores. Los logs deben ser activados en toda la infraestructura y, de ser posible, centralizados en un SIEM.

   En caso de contar con un Centro de Operaciones de Seguridad (SOC), el Coordinador de Seguridad e Informática Forense será el responsable de la definición de los logs que ingresarán al sistema de monitoreo (SIEM Security Information Event Management) y el Coordinador de Sistemas y Arquitectura de Tecnología será el responsable de asignar el funcionario encargado de entregar los datos para la conexión de los logs a esta herramienta. Generar correo o acta de entrega de información de logs.

   El Coordinador de Sistemas y Arquitectura de Tecnología será el responsable de autorizar permisos de acceso a la herramienta que se utilice para el respaldo de logs de auditoría, para efectos de revisiones e investigaciones.

   En caso de presentarse incidentes o eventos que generen indisponibilidad de las plataformas tecnológicas y sistemas de información se deben revisar los

registros acerca de las actividades de los usuarios, excepciones, fallas, y eventos de seguridad de la información.

3. **Herramientas de monitoreo y alertamiento**

   Si existe una herramienta de monitoreo y alertamiento, es responsabilidad de los líderes técnicos de infraestructura y sistemas de información, estar atentos a los eventos de seguridad que se alerten y establecer las correcciones requeridas.

   Para el caso de la herramienta de monitoreo de la red WiFi mencionada en el numeral "Conexión a las redes Inalámbricas (WiFi)", se exportan informes de manera quincenal y en ellos se evidencia el estado real de operación de los componentes de la red.

4. **Análisis de Vulnerabilidades**

   Realizar escaneos periódicos para identificar configuraciones que puedan ser explotadas, alineado con la sección de "Gestión de Parches y Vulnerabilidades" del anexo 1 de este documento.

5. **Auditorías Periódicas**

   Crear un calendario de auditorías técnicas internas focalizadas en plataformas críticas (incluyendo VMware).

   Realizar revisiones y auditorías internas para verificar formalmente que los activos de la infraestructura cumplen con sus líneas base de configuración documentadas.

Responsables:

- Coordinador Grupo de Seguridad e Informática Forense.
- Administradores de sistemas y plataformas.

5.6. Fase 5: Remediación y Gestión de Desviaciones

Propósito: Corregir cualquier configuración que no cumpla con la línea base establecida, ya sea por un cambio no autorizado o un error.

Actividades:

1. **Notificación de Incidentes:**

Un cambio no autorizado en una configuración se debe reportar a través del Centro de Servicios tecnológicos a la cuenta servicios.tecnologicos@supersociedades.gov.co y se debe gestionar como un **incidente de seguridad de la información**. Por ello se debe dejar registro por parte del CST- Centro de servicios tecnológicos a través de la categoría: Disponibilidad, Tipo de Incidente: Mala configuración de la taxonomía de incidentes que hace parte de la GTI-GU-006 Guía Gestión de Incidentes, de las fallas que se presenten en la operación y funcionamiento de la infraestructura tecnológica.

2. **Análisis y Corrección**

Investigar la causa de la desviación. Utilizar los respaldos de configuración para restaurar el sistema a su estado autorizado y seguro.

3. **Análisis de Causa Raíz:**

Determinar por qué ocurrió la desviación y aplicar medidas correctivas para evitar su recurrencia.

4. **Documentación**: Mantener evidencia de los Informes de revisión técnica realizados, hallazgos identificados y acciones correctivas tomadas.

Responsables:

- Equipo de Respuesta a Incidentes.
- Administradores de sistemas.

6. CONTROL DE CAMBIOS

Versión	Fecha	Descripción del Cambio
001	24-02-2014	Creación del documento
002	01/11/2017	Actualización incluido seguridad física de acceso al centro de cómputo.
003	23/12/2021	Se adecua a los nombres de los grupos de tecnología actuales. Se modifica el parámetro de historial de la contraseña de 24 a 12 meses. Se modifica la duración de bloqueo de cuenta de 15 a 30 minutos por errores sucesivos en la digitación de acceso. Se exige la existencia de VPN para accesos remotos.

004	14/02/2025	Actualización de logos se modifica el parámetro del cumplimiento del control A.8.20 Seguridad de la red, A. 8.21 Seguridad de los servicios de red, de la norma ISO27001:2022
005	25/04/2025	Se actualiza a nueva plantilla de documentos, se incluye parámetros de seguridad para bases de datos, servidores, redes y comunicaciones, servidores de aplicaciones, Microsoft 365, la Nube, Seguridad de Endpoints y Dispositivos Móviles y gestión de parches y vulnerabilidades y Eliminación segura de información.
006	24/10/2025	Se actualiza el nombre del procedimiento, se incluyen actividades para la gestión de los parámetros de configuración
007	11/09/2026	Se incorporan actividades de monitoreo sobre la red inalámbrica, controles recurrentes para identificar equipos fuera de línea, analizar causas y gestionar su normalización.

Elaboró	Revisó	Aprobó
Nombre: Leidy Clavijo Cargo: Contratista - GSIF Fecha: 31 de agosto de 2026	Nombre: Diego Alejandro Franco García Cargo: Profesional Grupo de Sistemas y Arquitectura de Tecnología. Fecha: 31 de agosto de 2026	Nombre: Ricardo Fernelix Ríos Cargo: director de Tecnología de la Información y las Comunicaciones Fecha: 11 de septiembre 2026

7. ANEXO No.1 PARÁMETROS DE CONFIGURACIÓN

CONFIGURACION DE BASES DE DATOS

Parámetro o Componente	Descripción
Puertos Bases de Datos	De ser posible, cambie los puertos predeterminados utilizados por el motor de Base de Datos. En caso de realizar este cambio, debería modificar la configuración de los aplicativos que tienen acceso a la base de datos para reflejar el ajuste de puerto.
Filtrado de puertos por un firewall	Todos los puertos TCP y UDP utilizados por el motor de Base de Datos deben ser filtrados por un firewall (de host y/o de red) para que únicamente permita el acceso a este recurso a los equipos autorizados.
Acceso a base de datos	Se debería prevenir el acceso no autorizado a las bases de datos.
Particiones Separadas	Cree volúmenes o particiones de disco separando los archivos de programa del motor de Base de Datos y los datos.
Actualización SQL Server Último SP / CU	Determinar el nivel de parches actual y el nivel de parche objetivo a nivel de Motor de BD SQL Server.
Características y servicios SQL Server	Deshabilitar las características y servicios de SQL Server que no sean requeridas (SQL Browser Deshabilitado) Deshabilitar protocolos de SQL Server que no son utilizados (Shared Memory, Named Pipes, etc)
Autenticación	Configurar la autenticación desde Directorio activo siempre y cuando sea posible
Grupos y roles	Crear contenedores, como grupos o roles, y asignarles permisos para acceder a los recursos. Luego haga que las cuentas sean miembros de esos grupos de roles (Cero asignaciones explicita de privilegios directamente a cuentas de usuario).
Reglas Firewall	Habilitar firewall y abrir solo puertos que son estrictamente necesarios
Instancia SQL Server	Ocultar la instancia de SQL Server
Acceso backups	Restringir el acceso a las carpetas de backup de SQL Server
Cuenta SA	Cambiar contraseña de cuenta la cuenta SA (contraseña fuerte), renombrar y deshabilitar cuenta
Cuentas de servicio	Configuración de cuentas de servicio requeridas para SQL Server - Cuentas de servicio separadas (contraseñas fuertes y diferentes

Parámetro o Componente	Descripción
	x servicio, managed service account o Domain user account aplicando el principio del menor privilegio)
Cuenta de lecturas	Crear cuenta de solo lectura para ejecutar consultas y tareas básicas como backups bd, backup procedimiento
Store procedure	Deshabilitar store procedure xp_cmdshell
Restricción de acceso	Restringir el acceso a los archivos de base de datos y configuración de SQL Server
Eliminación grupo	Eliminar el grupo BUILTIN\Administrators de los inicios de sesión de SQL Server
Perfilar cuentas	Perfilar usuarios con privilegios elevados (aplicar principio del menor privilegio)

CONFIGURACIÓN DE SERVIDORES

Parámetro o Componente	Descripción
Protección contra amenazas y malware	Aplicar bloqueos de procesos, ejecutables y herramientas, así como habilitar tareas de análisis, protección y monitoreo y deshabilitar otras
Restricciones a Aplicaciones (Office, Adobe, Scripts)	Aplicar bloqueos sobre aplicaciones
Autenticación, cuentas y contraseñas	Aplicar configuraciones para cuentas de administración, con privilegios e invitados, así como de contraseñas y accesos remotos
Actualizaciones y programaciones de seguridad	Habilitar y deshabilitar configuraciones respecto de actualizaciones, fuentes de actualización, análisis e instalación
Supervisión y escaneo	Habilitar y deshabilitar configuraciones respecto a supervisión, eliminación de archivos, así como puntos de restauración y análisis de red
Conectividad y Red	Aplicar protecciones de red, deshabilitar enrutamiento de origen IP, recursos compartidos anónimos, puentes de red y ejecución de auto run
Políticas de interfaz, almacenamiento y experiencia del usuario	Deshabilitar almacenamiento de credenciales, administrador de contraseñas, autoplay para unidades y no permitir que los administradores locales personalicen permisos

CONFIGURACION REDES Y COMUNICACIONES

Parámetro o Componente	Descripción
Servicios inseguros deshabilitados	Los switches solo aceptan protocolos SSH y SFTP para la gestión.
Servicios del router y switch que deben ser protegidos de accesos no permitidos	Los accesos no permitidos se protegen mediante la implementación de reglas en el Firewall, donde solo se les permite a los servidores Bastión autorizados el acceso a los switches. A su vez el acceso a estos servidores también está restringido solo a la sub-red de la DTIC y VPN, además que los usuarios que ingresan vía RDP hace parte del grupo de administradores en el Directorio Activo. También se controla el horario de acceso, para NO permitir el ingreso en horas no hábiles ni festivos, con la excepción de los usuarios autorizados en el Directorio Activo.
Puertos predeterminados	Solo se permite tráfico SSH y SFTP via los servidores Bastión. Se habilita HTTP en el puerto 8080.
Cifrado	Se utiliza los mecanismos de cifrado que usan los protocolos SSH, SFTP y SSL, que incluyen un único algoritmo de cifrado (como AES) para cifrar y descifrar los datos durante la sesión.
Servicio remoto	Solo se puede tener acceso los dispositivos vía servidores Bastión los cuales están protegidos por el Firewall. Para accesos remotos autorizados se realiza a través de la VPN y a usuarios autorizados incluidos en los respectivos Grupos de Seguridad en el Directorio Activo.
Acceso SSH	Solo se permite acceso SSH desde los servidores Bastion. Este acceso está restringido y protegido a través del Firewall, lo que protege a la infraestructura de ser administrada desde cualquier punto interno o externo de la red.
Cambio de credenciales	Cambiar los usuarios por defecto, así como las contraseñas por defecto
Banner o mensajes de pre-autenticación y pos-autenticación	Se debe configurar un mensaje que alerte que está ingresando a un equipo de comunicación crítica y de acceso restringido
Time out sesiones por consola	El time out es por defecto 60 segundos.
Telnet	Deshabilitar el acceso via Telnet

Parámetro o Componente	Descripción
Reglas de Password local	Configurar el dispositivo para permitir reglas o requerimientos de complejidad de password y habilitar la encripción de password
Nombre	Configurar el nombre del dispositivo
Protocolos SMNP	Deshabilitar, así como los servicios que no sean requeridos
Configuración de tiempo de eventos y retención de logs	El periodo de retención de logs es de 24 horas. El sistema no permite una mayor retención.
Syslog	Configurar el syslog
VLAN	Configurar VLAN de gestión y VLAN de usuarios de acuerdo a la segmentación que tenga la Entidad
Puertos	Deshabilitar puertos que no estén siendo utilizados
NTP	Configurar al menos 2 server NTP
Zona horaria	Configurar la zona horaria -5 Bogotá
Actualización Firmware	Actualizar firmware a la última versión estable disponible y de acuerdo con la recomendación de fabrica
Antispoofing	Configurar los parámetros para evitar el spoofing
Broadcast	Configurar parámetros para evitar tormenta de broadcast
Backup configuración	Configurar programación de backups automaticamente o generar uno manual periódicamente y cuando se generen cambios
Bloqueo de IP	Configurar bloqueo de IP sobre intentos fallidos de logueo
Estaciones de cómputo de escritorio	Desactivar para los equipos de escritorio que se tengan en operación dentro de las instalaciones de la Entidad la tarjeta de red inalámbrica, de tal manera que solo se puedan conectar con la red alámbrica. Para los equipos portátiles no aplica la desactivación de la tarjeta de red inalambrica.

SERVIDORES DE APLICACIONES WILDFLY

Parámetro o Componente	Descripción
Acceso	Restringir acceso a la interface de administración
HTTPS/TLS	Habilitar HTTPS/TLS en todos los servicios expuestos, utilizando certificados institucionales.
Cambio de credenciales	Cambiar los usuarios por defecto, así como las contraseñas por defecto

Parámetro o Componente	Descripción
Parámetros dinámicos	Externalizar los parámetros dinámicos usando archivos properties
Credenciales	Utilizar bóvedas para credenciales e información sensible
Autenticación	Configurar autenticación y autenticación basada en roles RBAC integrado con el directorio activo
Logs y monitoreo	Configurar los logs y monitoreo para eventos de seguridad
Usuarios, grupos y mapeo roles	Configuración de usuarios, grupos y mapeo roles
Instancia como servicio	Configurar como servicio la ejecución de la instancia bajo cuentas dedicadas con mínimos privilegios
Syslog	Configurar el syslog
Página de bienvenida	Deshabilitar todas la paginas de bienvenida por defecto
Conectores	Deshabilitar todos lo conectores que no sean necesarios
Servicio remoto	Solo se puede tener acceso vía servidores Bastión los cuales están protegidos por el Firewall. Para accesos remotos autorizados se realiza a través de la VPN y a usuarios autorizados incluidos en los respectivos Grupos de Seguridad en el Directorio Activo.
Backup configuración	Configurar programación de backups automáticamente o generar uno manual periódicamente y cuando se generen cambios
Certificados digitales	Almacenar los certificados digitales en los almacenes de confianza Truststores
Keystore	Cambiar las credenciales por defecto del Keystore

WAS

Parámetro o Componente	Descripción
Acceso	Restringir acceso a la interface de administración
HTTPS/TLS	Habilitar HTTPS/TLS en todos los servicios expuestos, utilizando certificados institucionales.
Cambio de credenciales	Cambiar los usuarios por defecto, así como las contraseñas por defecto

Parámetro o Componente	Descripción
Parámetros dinámicos	Externalizar los parámetros dinámicos usando archivos properties
Credenciales	Configurar encripción de password personalizada
Acceso consola	Configurar el acceso seguro a la consola de administración
Roles	Configurar roles de seguridad administrativos integrados con el directorio activo para administrador, auditor, monitor, deployer y operador
Logs y monitoreo	Configurar los logs en una unidad de disco diferente a la del sistema operativo, así como el monitoreo para eventos de seguridad
Puertos	Cambio de puertos por defecto tanto para gestión como para el servicio de aplicaciones
Usuarios, grupos y mapeo roles	Configuración de usuarios, grupos y mapeo roles
Syslog	Configurar el syslog
Página de bienvenida	Deshabilitar todas la paginas de bienvenida por defecto
Conectores	Deshabilitar todos lo conectores que no sean necesarios
Servicio remoto	Solo se puede tener acceso vía servidores Bastión los cuales están protegidos por el Firewall. Para accesos remotos autorizados se realiza a través de la VPN y a usuarios autorizados incluidos en los respectivos Grupos de Seguridad en el Directorio Activo.
Backup configuración	Configurar programación de backups automáticamente o generar uno manual periódicamente y cuando se generen cambios
Certificados digitales	Almacenar los certificados digitales en los almacenes de confianza Truststores
Keystore	Cambiar las credenciales por defecto del Keystore

MICROSOFT 365

Para gestionar la configuración de la plataforma **Microsoft 365**, se han implementado **perfiles de configuración y políticas de seguridad** a través de herramientas como **Microsoft Intune**, **Microsoft Entra ID (anteriormente Azure AD)**, y el **Centro de cumplimiento y seguridad**. Estas configuraciones se aplican a **grupos específicos de usuarios** mediante asignaciones dinámicas o manuales,

garantizando la aplicación uniforme de controles, previniendo accesos no autorizados y asegurando el cumplimiento de las Políticas de Seguridad de la Información.

Parámetro o Componente	Descripción
Exchange Online	Se debe Asegurar de que los usuarios que instalan complementos de Outlook no están permitidos
Exchange Online	Se debe Asegurar de que el uso compartido externo de calendarios no esté disponible
Exchange Online	Se debe Asegurar de que las sugerencias de correo electrónico estén habilitadas para los usuarios finales
Exchange Online	Se debe Asegurar de que los proveedores de almacenamiento adicionales estén restringidos en Outlook en la Web
Microsoft Teams	Configurar qué usuarios pueden presentar en reuniones de Teams
Microsoft Teams	Limitar el control de los participantes externos en una reunión de Teams
Microsoft Teams	Limitar que los usuarios anónimos se unan a las reuniones
Microsoft Teams	Se debe Asegurar que solo los usuarios invitados deben ser admitidos automáticamente en las reuniones de Teams
Microsoft Information Protection	Se debe Asegurar de que las directivas de clasificación de datos de etiquetado automático están configuradas y usadas
Microsoft Information Protection	Se debe extender el etiquetado de confidencialidad de M365 a los recursos del mapa de datos de Microsoft Purview
Microsoft Information Protection	Se Deberia Publicar directivas de clasificación de datos de etiquetas de confidencialidad de M365
Microsoft Entra ID	Se debe Asegurar de que "Administración de Microsoft Azure" esté limitado a roles administrativos
Microsoft Entra ID	Se debe Asegurar de que la autenticación multifactor esté habilitada para todos los usuarios
Microsoft Entra ID	Se debe Asegurar de que la autenticación multifactor esté habilitada para todos los usuarios en roles administrativos
Microsoft Entra ID	Se debe Asegurar de que se usan las listas de contraseñas prohibidas personalizadas
Defender for Office	Se debe Asegurar de que no se permita ningún dominio remitente para las directivas contra el correo no deseado
Defender for Office	Se debe Asegurar de que todos los formularios de reenvío de correo estén bloqueados o deshabilitados
Defender for Office	Se debe establecer el umbral de nivel de correo electrónico de suplantación de identidad (phishing) en 2 o más

Defender for Office	No agregar direcciones IP permitidas en la directiva de filtro de conexión

ACCESO FÍSICO A ÁREAS DE PLATAFORMA TECNOLÓGICA.

Parámetro o Componente	Descripción
Área de seguridad	Se debe prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la superintendencia de sociedades.
Perímetro de seguridad física	El centro de cómputo debe estar en un área o perímetro de seguridad, que permita proteger la plataforma tecnológica que contenga información sensible o crítica, e instalaciones almacenamiento, procesamiento y transporte de la información sensible de la superintendencia de sociedades.
Controles físicos de entrada	El centro de cómputo de Supersociedades debe protegerse con controles de entrada físicos como puertas con sistemas de control de acceso automatizado que aseguren que solamente se permite el acceso a personal autorizado. Para esto se debe: - Actualizar la base de datos del sistema de control de acceso únicamente con los usuarios autorizados por el coordinador del Grupo de Sistemas y Arquitectura Tecnológica. - Tener diferentes medios de control de acceso de tal manera que si falla uno los otros permitan ingresar (Tarjeta de proximidad, contraseña de acceso, lector biométrico). En caso de mantenimientos preventivos o correctivos en los cuales se deba dejar las puertas abiertas durante algún tiempo prudencial, se deben realizar acciones como: - Colocar avisos de la actividad de mantenimiento, que indiquen la restricción de acceso solo a personal autorizado. - En lo posible solicitar vigilancia al área administrativa. - Colocar restricciones físicas como cordeles, conos, cintas de seguridad. Para todo acceso de personal diferente al autorizado, se debe dejar registro de acceso al centro de cómputo o alguna de sus áreas restringidas, anotando en las listas de control de acceso, la fecha, hora de entrada y salida, nombre y firma del visitante, razón del acceso, entidad a la que pertenece y funcionario que autorizo.
Registros de acceso	- Para todo acceso de personal diferente al autorizado, se debe dejar registro de acceso al centro de cómputo o alguna de sus

Parámetro o Componente	Descripción
	áreas restringidas, anotando en las listas de control de acceso, la fecha, hora de entrada y salida, nombre y firma del visitante, razón del acceso, entidad a la que pertenece y funcionario que autorizo. - Se debe instalar cámaras de vigilancia que registren acceso y estado del centro de cómputo. Se debe realizar revisiones al azar de los registros de las cámaras contra la lista de registro de acceso al centro de cómputo, sobre todo en horarios no hábiles. - Los contratistas deben portar carné de visitante y/o de la entidad a la que pertenecen.
Protección contra amenazas externas y ambientales	Se debe contar con dispositivos de alertamiento ante amenazas de incendio, inundación, subidas de temperatura, y demás amenazas ambientales.

Seguridad en la Nube (Cloud Security): Estas recomendaciones aplican a todos los servicios cloud utilizados en la organización, ya sea en modelos IaaS, PaaS o SaaS, incluyendo nubes públicas, privadas o híbridas, contratadas por la entidad o integradas a través de terceros.

Parámetro o Componente	Descripción
Selección y evaluación de proveedores	• Validar que el proveedor de servicios en la nube cumpla con estándares de seguridad reconocidos (ISO/IEC 27001, SOC 2, CSA STAR). • Verificar que el proveedor garantice la ubicación geográfica de los datos (jurisdicción legal aplicable). • Evaluar el cumplimiento del proveedor con la ley de protección de datos personales (Ley 1581 de 2012) y otras normativas aplicables.
Contratos y acuerdos	• Incluir cláusulas de seguridad en los contratos • Nivel de cifrado. • Tiempo de retención y borrado de datos. • Planes de continuidad del proveedor. • Notificación de incidentes de seguridad. • Formalizar acuerdos de nivel de servicio (SLA) que incluyan métricas de disponibilidad, respuesta ante incidentes y soporte técnico.

Parámetro o Componente	Descripción
Gestión de identidades y accesos (IAM)	• Aplicar el principio de mínimo privilegio en la asignación de roles. • Integrar el acceso cloud con el sistema central de autenticación institucional (por ejemplo, Azure AD, Entra ID). • Habilitar autenticación multifactor (MFA) en todos los accesos a consolas administrativas y paneles de gestión. • Realizar revisiones periódicas de permisos y accesos concedidos.
Cifrado y protección de datos	• Asegurar el uso de cifrado en tránsito (TLS 1.2 o superior) y en reposo. • Gestionar adecuadamente las claves de cifrado, ya sea por el proveedor (KMS) o internamente (BYOK – Bring Your Own Key). • Clasificar la información antes de almacenarla en entornos cloud.
Seguridad operacional	• Activar los mecanismos de registro y auditoría de accesos, cambios y eventos (logs). • Integrar estos registros con las herramientas de monitoreo y análisis de eventos institucionales (SIEM). • Definir planes de respaldo y restauración para los datos y configuraciones almacenados en la nube.
Respuesta a incidentes	• Establecer procedimientos para gestionar incidentes en entornos cloud. • Exigir al proveedor reportar eventos de seguridad relevantes dentro de los tiempos acordados. • Definir un canal de comunicación para la gestión de crisis conjunta con el proveedor.
Integración con el modelo Zero Trust	• Asegurar que el acceso a recursos en la nube esté basado en políticas dinámicas de confianza. • Validar constantemente la identidad, el dispositivo y el contexto de conexión antes de permitir el acceso a servicios cloud. • Restringir accesos por ubicación geográfica, horario y dispositivo de conexión.

Seguridad de Endpoints y Dispositivos Móviles: Estas recomendaciones aplican a todos los dispositivos de usuario final —corporativos o autorizados por la organización— que tengan acceso a sistemas, aplicaciones, datos institucionales o servicios en la nube.

Parámetro o Componente	Descripción
Configuración segura (hardening)	Establecer una imagen base institucional con configuraciones seguras para todos los equipos. Deshabilitar servicios innecesarios, puertos vulnerables y componentes de red que no se utilicen. Usar cuentas con privilegios mínimos para operaciones cotidianas; restringir cuentas administrativas.

Parámetro o Componente	Descripción
Protección contra malware	Instalar y mantener actualizado un software antivirus / antimalware gestionado centralmente. Habilitar funciones de protección en tiempo real y escaneos automáticos periódicos. Integrar la protección de endpoints con el sistema de monitoreo de eventos (SIEM/SOC).
Control de dispositivos extraíbles	Restringir el uso de memorias USB, discos externos y otros medios removibles no autorizados. El usuario autorizado debe realizar el etiquetado a la información, de acuerdo con la clasificación de la información que se almacene en dichos medios. Mantener el registro de la autorización de uso de estos medios.
Cifrado de disco	Habilitar cifrado completo de disco en todos los equipos portátiles En lo posible, usar cifrado gestionado desde la consola central de TI (ej. BitLocker, FileVault, MDM).
Seguridad en dispositivos móviles	Registrar todos los dispositivos móviles autorizados en una plataforma de gestión de dispositivos móviles (MDM). Prohibir el uso de redes Wi-Fi públicas para conexiones a sistemas institucionales sin VPN. Habilitar políticas de bloqueo automático, borrado remoto y autenticación biométrica o por PIN.
Accesos y autenticación	Forzar el uso de contraseñas robustas o autenticación biométrica para desbloquear dispositivos. Aplicar autenticación multifactor (MFA) para el acceso a servicios institucionales desde cualquier endpoint. Deshabilitar sesiones inactivas y establecer tiempos de bloqueo automático.
Parcheo y actualizaciones	Configurar la instalación automática de actualizaciones del sistema operativo y aplicaciones críticas. Establecer un proceso de gestión de parches que contemple pruebas, priorización y tiempos de aplicación.

Gestión de Parches y Vulnerabilidades: Estas recomendaciones aplican a:

- Sistemas operativos de servidores y estaciones de trabajo.
- Equipos de red, almacenamiento y telecomunicaciones.
- Aplicaciones institucionales (propias o de terceros).
- Plataformas en la nube bajo responsabilidad compartida.
- Herramientas de desarrollo, bases de datos y middleware.

Parámetro o Componente	Descripción

Identificación de vulnerabilidades	• Utilizar herramientas automáticas de escaneo de vulnerabilidades (como OpenVAS, Nessus, Qualys, etc.). • Monitorear fuentes oficiales de vulnerabilidades y parches (CVE, NVD, Microsoft, Red Hat, etc.). • Establecer una periodicidad para escaneos internos (ej. mensual o trimestral) y tras cambios significativos.
Evaluación y clasificación	• Evaluar cada vulnerabilidad detectada según su severidad (CVSS), criticidad del activo afectado y probabilidad de explotación. • Priorizar el tratamiento de vulnerabilidades críticas y de alto riesgo en plazos máximos establecidos (ej. ≤72 horas).
Aplicación de parches	• Aplicar parches de seguridad de forma controlada, validada y documentada. • Para entornos de producción, realizar pruebas en entornos de staging o laboratorio antes de aplicar los cambios. • Documentar cada parche aplicado y actualizar la bitácora técnica o sistema de tickets.
Seguimiento y verificación	• Verificar que los parches fueron aplicados correctamente y que el sistema sigue funcionando adecuadamente. • Repetir escaneos de validación posterior a la corrección.

Eliminación Segura de la Información: Aplica a todos los activos de información almacenados en Equipos de cómputo y servidores locales, Dispositivos móviles y medios extraíbles, Sistemas de almacenamiento de red (NAS, SAN), Plataformas de virtualización y servicios en la nube (IaaS, PaaS, SaaS), Bases de datos y aplicaciones institucionales que contengan información clasificada o reservada

Parámetro o Componente	Descripción
Criterios para la eliminación segura	Se debe eliminar de forma segura toda la información que: • Haya cumplido su ciclo de vida según tablas de retención documental. • Esté almacenada en medios o sistemas que serán reutilizados, desincorporados o retirados. • Responda a una solicitud del titular (en cumplimiento con la Ley 1581 de 2012).
Métodos de eliminación segura en infraestructura local	• Sobreescritura de datos con herramientas certificadas (Ej. DBAN, Blancco). • Desmagnetización para medios magnéticos, solo en entornos controlados. • Destrucción física como trituración, incineración o perforación, preferiblemente por empresas certificadas. • Formateo seguro debe incluir varias pasadas y verificación posterior.

Parámetro o Componente	Descripción
Eliminación segura en entornos cloud	• Verificar que el proveedor implemente mecanismos de borrado lógico irreversible y sanitización conforme a normativas como NIST 800-88. • Solicitar evidencia documental o confirmación de borrado seguro para servicios de almacenamiento, máquinas virtuales y bases de datos. • Para SaaS, hay que asegurar que los datos sean eliminados del ambiente activo y de las copias de respaldo en un plazo definido (ej. 30-90 días).