SERVICIOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD			
PROCESO:	GESTIÓN TIC´S		
PROCEDIMIENTO	POLÍTICA GENERAL DE GOBIERNO DIGITAL		
FECHA APROBACIÓN:	**CÓDIGO**	**VERSIÓN**	**PÁGINA**
30/10/2025	GTI02 - CTG01	01	1 de 1

ID	NOMBRE DEL SERVICIO	DESCRIPCIÓN	OBJETIVO (próposito en la entidad)	ALCANCE (sobre que infraestructura)	RESPONSABLE (roles o responsables de la implementación)	ANS (Horario de Prestación)	PROCESO A QUIEN VA DIRIGIDO (Procesos de negocio soportados)	PROVEEDOR Y CONTACTO	CANAL DE ATENCION
1	Administración plataforma de seguridad perimetral	Configurar políticas de seguridad de Firewall	Establecer y mantener una configuración segura de los firewalls que permita controlar, permitir o restringir el acceso a la red interna y externamente. Además de proteger frente a amenazas y ataques internos y externos.	La configuración de las políticas de seguridad de firewalls abarca la aplicación y ajuste de reglas de control de acceso a la infraestructura y plataforma tecnológica sobre la red de la CGN. incluye políticas de prevención de intrusos IPS, filtrado de contenido web y DNS y control de aplicaciones.	Administrador de la infraestructura de gestión y red de datos y comunicaciones.	Solicitud Alta: 16 horas Media: 24 horas Bajo 48 horas Incidente Alto: 8 horas Medio: 12 horas Bajo: 24 horas	Todos los procesos	Proveedor: Opengroup Contacto: servicios@opengroupsa.com	Plataforma de mesa de servicio GLPI
2	Administración Antivirus	Configurar antivirus en equipos terminales	Garantizar la protección proactiva de los equipos terminales mediante la implementación, configuración y mantenimiento de la solución de antivirus que permita la detección, prevención contra amenazas digitales y eliminación de malware minimizando el riesgo de compromiso de seguridad, perdida de información o interrupciones operativas en la CGN	El alcance de la configuración de antivirus en los equipos terminales comprende la instalación, configuración, actualización y monitoreo para la protección contra amenazas digitales en todos los dispositivos finales de la CGN.	Administrador de infraestructura de Software	Solicitud Alto: 1 hora Medio: 4 horas Bajo: 8 horas Incidente Pasa al proveedor de servicios Alto: 1 hora Medio: 4 horas Bajo: 8 horas	Todos los procesos	Proveedor: Kavantic Contacto: soporte@kavantic.co	Plataforma de mesa de servicio GLPI
3	Incidente de seguridad	Servicio que permite gestionar, investigar y resolver incidentes de seguridad que afectan la confidencialidad, integridad o disponibilidad de la información.	Establecer un proceso estructurado y eficaz para la identificación, reporte, evaluación, respuesta y aprendizaje de los incidentes de seguridad de la información, con el fin de minimizar su impacto y afectación de los activos de información de la CGN.	El servicio de gestión de incidentes de seguridad de la información abarca desde el reporte, clasificación, investigación, gestión y resolución de eventos o incidentes que comprometan la confidencialidad, integridad o disponibilidad de la información.	Oficial de Seguridad y Privacidad de la Información Equipo de Seguridad	Evento Alto: 40 horas Medio: 64 horas Bajo: 80 horas Incidente Alto: 2 horas Medio: 4 horas Bajo: 6 horas	Todos los procesos	N/A	Plataforma de mesa de servicio GLPI
4	Autenticación multifactor	Refuerzo del acceso seguro mediante múltiples factores	Fortalecer los mecanismos de control de acceso a sistemas y servicios críticos mediante la implementación de autenticación multifactor (MFA) con el fin de reducir el riesgo de accesos no autorizados, proteger las credenciales y garantizar un nivel adicional de seguridad en la verificación de identidad.	El refuerzo de acceso seguro mediante múltiples factores (MFA) comprende la implementación, configuración y gestión de mecanismos de autenticación adicionales a la contraseña que normalmente se utiliza.	Administrador de infraestructura de Software Administrador de redes Administrador de Aplicaciones Administrador de correo electrónico	Solicitud Alta: 8 horas Media: 12 horas Bajo 24 horas	Todos los procesos	Proveedor: Google Contacto: soporte@maestrosdelcloud.com Proveedor: Opengroup Contacto: servicios@opengroupsa.com Proveedor: Comercializadora Serlecom SAS Contacto: soporte tecnico de microsoft	Plataforma de mesa de servicio GLPI
5	Respaldo y recuperación de información misional	Asegurar backups protegidos y recuperables ante incidentes de la plataforma misional.	Asegurar la disponibilidad e integridad de la información crítica misional de la CGN mediante la implementación y gestión de copias de seguridad, que permitan la recuperación oportuna de datos ante incidentes, fallos técnicos o desastres, garantizando la continuidad operativa.	El alcance comprende el diseño, implementación, gestión y monitoreo de un sistema de copias de seguridad que garantice la protección, disponibilidad e integridad de la información crítica de la CGN, incluye la definición de copias de respaldo, la programación de copias periódicas, el control de acceso, la replicación y la verificación regular de la restauración efectiva. El alcance abarca los sistemas de información y aplicaciones de misión crítica también los entornos locales y alternos, cubre servidores lógicos y físicos y bases de datos.	Administrador de infraestructura de Hardware Administrador de infraestructura de Software	Respaldo de información misional y gestión: ANS: Solicitud Alta: 16 horas Media: 24 horas Bajo 48 horas Incidente Alto: 8 horas Medio: 12 horas Bajo: 24 horas	Gestión TICs	N/A	Plataforma de mesa de servicio GLPI
6	Respaldo y recuperación de información de gestión	Asegurar backups protegidos y recuperables ante incidentes de la plataforma de gestión.	Asegurar la disponibilidad e integridad de la información de gestión de la CGN mediante la implementación y gestión de copias de seguridad, que permitan la recuperación oportuna de datos ante incidentes, fallos técnicos o desastres, garantizando la continuidad operativa.	El alcance comprende el diseño, implementación, gestión y monitoreo de un sistema de copias de seguridad que garantice la protección, disponibilidad e integridad de la información de gestión de la CGN, incluye la definición de copias de respaldo, la programación de copias periódicas, el control de acceso, la replicación y la verificación regular de la restauración efectiva. El alcance abarca los sistemas de información y aplicaciones de gestión en los entornos locales y nube, cubre servidores físicos y lógicos y bases de datos.	Administrador de infraestructura de Hardware Administrador de infraestructura de Software	Respaldo de información misional y gestión: ANS: Solicitud Alta: 16 horas Media: 24 horas Bajo 48 horas Incidente Alto: 8 horas Medio: 12 horas Bajo: 24 horas	Gestión TICs	N/A	Plataforma de mesa de servicio GLPI
7	Análisis de código fuente	Análisis de vulnerabilidades del código del software	Identificar vulnerabilidades, errores de seguridad y malas prácticas de desarrollo mediante el análisis de código fuente, con el fin de prevenir riesgos. antes de la puesta en producción.	El análisis de vulnerabilidades durante el desarrollo de software y aplicaciones en producción abarca la identificación, evaluación y mitigación de debilidades de seguridad en el código de fuente, componentes y configuraciones. Este proceso incluye la aplicación de pruebas y análisis estático, con el fin de detectar vulnerabilidades comunes, errores de autenticación o autorización.	Desarrollador	Solicitud Alta: 16 horas Media: 24 horas Bajo 48 horas Incidente Alto: 8 horas Medio: 12 horas Bajo: 24 horas	Gestión TICs	N/A	Plataforma de mesa de servicio GLPI

8	Conexión segura VPN	Control seguro del acceso a la red desde ubicaciones externas.	Garantizar el acceso remoto seguro a los sistemas y recursos de la CGN, mediante la implementación y control de conexiones VPN, con autenticación robusta y políticas de acceso restringido, minimizando los riesgos de interceptación, accesos no autorizados y exposición de información confidencial fuera de la CGN.	El control seguro de acceso a la red desde ubicaciones externas abarca la aplicación de medidas técnicas que permiten el acceso remoto seguro a través de la VPN a los recursos de la CGN por parte de usuarios autorizados. Este control incluye la autenticación multifactor (MFA), uso de conexión cifrada (token), políticas de acceso basadas en roles y necesidades, monitoreo de sesiones remotas, restricciones por ubicaciones geográficas o el tipo de dispositivo. El alcance también aplica para funcionarios, contratistas o terceros que acceden fuera de las instalaciones de la CGN.	Administrador de la infraestructura de gestión y red de datos y comunicaciones.	Solicitud Alta: 8 horas Media: 12 horas Bajo 24 horas Incidente Alto: 2 horas Medio: 4 horas Bajo: 8 horas	Todos los procesos, proveedores y terceros.	Proveedor: Opengroup Contacto: servicios@opengroupsa.com Proveedor: GSE Contacto: mesa.servicio@gse.com.co	Plataforma de mesa de servicio GLPI
9	Seguridad Digital Certificados SSL	Certificado digital que autentica la identidad de un sitio web	Garantizar la confidencialidad, integridad y autenticidad de la identidad del sitio web de la CGN, asegurando la información transmitida a través de los servicios digitales de la entidad. Mediante la implementación, gestión y renovación oportuna de certificados SSL/TL	La infraestructura de certificados SSL/TLS abarca los servicios de sistemas de información y acceso a servidores que establecen comunicaciones digitales a través de sitios web, garantizando que dichas interacciones se realicen de forma segura, confiable y autenticada.	Administradores de las infraestructuras misionales, de gestión, red de datos y comunicaciones.	Solicitud Alta: 2 horas Media: 8 horas Bajo 24 horas Incidente Alto: 2 horas Medio: 4 horas Bajo: 8 horas	Todos los procesos	Proveedor: GSE Contacto: mesa.servicio@gse.com.co	Plataforma de mesa de servicio del proveedor
10	Custodia copias de seguridad	Custodia, almacenamiento y control de las copias de seguridad	Asegurar la protección, disponibilidad y recuperación confiable de la información crítica de la entidad mediante la custodia, almacenamiento y control de las copias de seguridad, garantizando que estén resguardadas frente a accesos no autorizados, pérdidas, alteraciones o desastres, y que puedan ser restauradas de manera oportuna para dar continuidad a los procesos institucionales	La custodia de copias de seguridad comprende archivos de datos de algunos de los ambientes de los servicios misionales, para garantizar la protección, almacenamiento, disponibilidad y recuperación de la información crítica de la CGN.	Administrador de la infraestructura misional	Solicitud Alta: 2 horas Media: 8 horas Bajo 24 horas	Procesos misionales	Proveedor: Documental siglo XXI Contacto: mrubiano@siglo21.com.co apedraza@siglo21.com.co dperez@siglo21.com.co	Correo del proveedor
11	Monitoreo SOC	Detección, análisis y respuesta oportuna a incidentes	Detectar, analizar y dar respuesta oportuna a incidentes de ciberseguridad dentro de la CGN. Su razón de ser es garantizar la continuidad operativa, protección de la información crítica y reducción de riesgos frente a amenazas internas o externas.	El alcance del Monitoreo SOC cubre toda la superficie de ataque digital de la entidad (redes, sistemas, usuarios y dispositivos), gestiona la detección, análisis y respuesta a incidentes, asegura el cumplimiento normativo y protege tanto infraestructura interna como conexiones con terceros.	Administrador de la infraestructura de gestión y red de datos y comunicaciones.	Solicitud Alta: 2 horas Media: 8 horas Bajo 24 horas Incidente Alto: 2 horas Medio: 4 horas Bajo: 8 horas	GIT de Apoyo Informatico	Proveedor: Opengroup Contacto: servicios@opengroupsa.com	Plataforma de servicios del proveedor
12	Seguridad Digital Certificados de persona	Transacciones seguras a través de plataformas públicas y privadas	Garantizar la identidad digital, la confidencialidad de la información y la integridad de las transacciones electrónicas que realiza un servidor público en el entorno digital donde se realizan estas transacciones.	El alcance en la infraestructura de Seguridad Digital con Certificados de Persona define qué componentes tecnológicos y organizacionales se deben cubrir para garantizar la autenticidad, confidencialidad, integridad y no repudio en el uso de identidades digitales.	Soporte técnico del GIT de apoyo informático	Solicitud Alta: 2 horas Media: 8 horas Bajo 24 horas Incidente Alto: 4 horas Medio: 8 horas Bajo: 24 horas	Todos los procesos	Proveedor: GSE Contacto: mesa.servicio@gse.com.co	Plataforma de mesa de servicio del proveedor Plataforma de mesa de servicio CGN - GLPI
13	Gestión activos de información	Identificar, proteger, controlar y administrar los activos de información durante todo su ciclo de vida	El objetivo de la Gestión de Activos de Información es asegurar que toda la información de la CGN y los medios que la soportan estén identificados, protegidos, controlados y administrados durante todo su ciclo de vida, de manera que se preserve su confidencialidad, integridad y disponibilidad.	El alcance comprende la Gestión de Activos de Información en los componentes de información, software, hardware, servicios y talento humano para su control y protección.		Revisión y/o Actualización anual	Todos los procesos	mesadeservicio@contaduria.gov.co	Plataforma de mesa de servicio GLPI
14	Borrado seguro	Eliminar de manera segura la información contenida en los discos duros que vayan a ser dados de baja o sean entregados en donación	Eliminar de manera definitiva e irrecuperable la información almacenada en dispositivos electrónicos, que vayan a ser dados de baja o sean entregados en donación garantizando que no pueda ser recuperada con técnicas forenses o herramientas de recuperación de datos.	El alcance de la infraestructura del borrado seguro se refiere a qué activos y entornos deben ser considerados para garantizar que los datos eliminados no puedan ser recuperados.	Soporte técnico del GIT de apoyo informático	Borrado seguro - Gestión: ANS Solicitud Alta: 8 horas Media: 16 horas Bajo 24 horas	Gestión Administrativa	mesadeservicio@contaduria.gov.	Plataforma de mesa de servicio GLPI
15	Gestión de vulnerabilidades	identificar, evaluar, priorizar y mitigar las debilidades de seguridad en los sistemas, aplicaciones, redes y procesos de la CGN	Identificar, evaluar, priorizar y mitigar las debilidades de seguridad en los sistemas, aplicaciones, redes y procesos de CGN, con el fin de reducir riesgos de explotación por atacantes y fortalecer la detección de amenazas de ciberseguridad.	El alcance a la infraestructura para la Gestión de Vulnerabilidades define qué componentes, entornos y procesos deben incluirse en este ciclo de identificación, análisis, priorización y remediación de debilidades.	Administrador de la infraestructura de gestión y red de datos y comunicaciones. Administrador de infraestructura de Hardware Administrador de infraestructura de Software Equipo de seguridad de la información	Ejecución anual y seguimiento periódico	Gestión TICs	mesadeservicio@contaduria.gov.co	Plataforma de mesa de servicio GLPI
16	Gestión controlador de dominio y direccionamiento	Administrar los servicios del directorio activo	Asegurar la correcta administración de los servicios de directorio, autenticación, autorización y resolución de nombres/direcciones, garantizando la disponibilidad, integridad, seguridad y eficiencia en la infraestructura tecnológica de la Entidad.	El alcance de la Gestión del Controlador de Dominio y Direccionamiento define qué componentes, servicios y procesos forman parte de su administración y protección dentro de la infraestructura de la CGN.	Administrador de Seguridad Informática	ANS Solicitudes: Alta:6 Horas Media:12 horas Baja: 24 Horas Incidentes: Alta:2 Horas Media:4 horas Baja: 8 Horas	Gestión TICs	mesadeservicio@contaduria.gov.co	Plataforma de mesa de servicio GLPI
17	Gestión de usuarios	Gestión de acceso a usuarios internos y externos, a través de la creación, configuración de permisos, cancelación o eliminación, en las diferentes aplicaciones administradas por el proceso de Gestión TICS bajo el principio del mínimo privilegio, trazabilidad y revisiones periódicas de acceso.	Asegurar que el ciclo de vida de identidades y accesos de los servidores públicos, colaboradores y cuentas de servicio de la CGN se gestiones con el mínimo privilegio multifactor de autenticación MFA y segregación de funciones garantizando la trazabilidad y revocación oportuna.	El alcance a la infraestructura en la Gestión de Usuarios define qué componentes tecnológicos, entornos y recursos están incluidos cuando se administra el ciclo de vida de las identidades y accesos.	Administrador de Seguridad Informática Administrador de la infraestructura de gestión y red de datos y comunicaciones. Administrador de infraestructura de Hardware Administrador de infraestructura de Software	ANS Solicitudes: Alta:6 Horas Media:12 horas Baja: 24 Horas Incidentes: Alta:2 Horas Media:4 horas Baja: 8 Horas	Gestión TICs	mesadeservicio@contaduria.gov.co	Plataforma de mesa de servicio GLPI