
	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del Riesgo, Seguridad y Continuidad del Negocio		Proceso: Gestión Integral de Seguridad	
	Políticas de Seguridad de Personas, Bienes e Información			
	Código: RSC-02-PO-003	Versión: 1.0	Fecha de Publicación en el Aplicativo: 23/08/2022	Página 1 de 32


Tabla de Contenido

1. Contexto.....	3
2. Objetivos	4
3. Campo de Aplicación	4
4. Términos y Definiciones del Sistema de Gestión de Seguridad.....	4
5. Política General de Seguridad	5
5.1 Política de Organización de la Seguridad.	7
5.2 Política de Talento Humano	7
5.3 Política de Seguridad de la Información para el trabajo por fuera de las instalaciones físicas de la CGR8	
5.4 Política de Seguridad de las Personas.....	9
5.5 Política de Responsabilidad por los Activos.....	10
5.6 Política de Clasificación de Información y Manejo de Medios.....	11
5.7 Política de Seguridad de los Bienes.....	12
5.8 Política de Control de Acceso	13
5.9 Política de Controles Criptográficos	14
5.10 Política de Seguridad Física y del Entorno.....	14
5.11 Políticas de Seguridad de Equipos.....	15
5.12 Política de Escritorio Limpio y Pantalla Limpia.....	16
5.13 Política de Procedimientos Operacionales y Responsabilidades.....	17
5.14 Política de Protección contra Códigos Maliciosos.....	18
5.15 Política de Copias de Respaldo	19
5.16 Política de Registro y Seguimiento de Eventos de Seguridad	20
5.17 Política de Control de Software Operacional.....	21
5.18 Política de Gestión de Vulnerabilidades.....	21
5.19 Política de Gestión de Seguridad de las Redes	22
5.20 Política de Uso de Internet	23
5.21 Política de Transferencia y Transmisión de Información.....	24
5.22 Política de Seguridad de Correo Electrónico.....	24
5.23 Política de Adquisición, Desarrollo y Mantenimiento de Sistemas	25
5.24 Política de Desarrollo Seguro.....	26
5.25 Política de Datos de Prueba.....	26
5.26 Política de Gestión de Relaciones con los Proveedores	27
5.27 Política de Gestión de Incidentes	28

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del Riesgo, Seguridad y Continuidad del Negocio		Proceso: Gestión Integral de Seguridad	
	Políticas de Seguridad de Personas, Bienes e Información			
	Código: RSC-02-PO-003	Versión: 1.0	Fecha de Publicación en el Aplicativo: 23/08/2022	Página 2 de 32

5.28	Política de Gestión de Continuidad del Negocio	29
5.29	Política de Cumplimiento de Requisitos Legales y Contractuales.....	30
5.30	Política para Uso y Licenciamiento de Software	30
6.	Normatividad y documentos de referencia.....	31
7.	Vigencia, derogatorias y trnasción	32

UNA VEZ DESCARGADO Y/O IMPRESO ESTE DOCUMENTO, SERÁ COPIA NO CONTROLADA

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del Riesgo, Seguridad y Continuidad del Negocio		Proceso: Gestión Integral de Seguridad	
	Políticas de Seguridad de Personas, Bienes e Información			
	Código: RSC-02-PO-003	Versión: 1.0	Fecha de Publicación en el Aplicativo: 23/08/2022	Página 3 de 32

1. Contexto

La Contraloría General de la República -CGR es el máximo órgano de control fiscal del Estado; como tal, tiene la misión de procurar el buen uso de los recursos y bienes públicos y contribuir a la modernización del Estado.

Además, considera que la utilización de tecnología, en el procesamiento, almacenamiento, recuperación y transmisión de la información, implica importantes riesgos de seguridad en cuanto a disponibilidad, confidencialidad e integridad, por lo que la Contraloría General de la República debe asegurar tales atributos en su información institucional en el cumplimiento de sus funciones constitucionales y legales.

Es así como se crea el Sistema de Gestión de Seguridad -SGG el cual se formalizó mediante la Resolución Organizacional OGZ-0531 del 28 de diciembre de 2016, modificada por la Resolución Organizacional OGZ-0593 del 30 de junio de 2017, que, además, crea al Comité de Seguridad y adopta la Política General de Seguridad, la Política de Seguridad y Privacidad de la información y la Política de Tratamiento de Datos personales. De otra parte, la Resolución Organizacional OGZ-0758-2020, modifica la conformación y funciones del Comité de Seguridad, a la par que crea el Programa de Protección y Seguridad del Contralor General de la República, los excontralores generales de la República y demás servidores de la Contraloría General de la República y adopta los lineamientos técnicos para la operación del programa.

El SGS es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de personas, bienes e información institucionales para el logro de los objetivos. Consta de las políticas, normas, procedimientos, guías, recursos asociados y actividades que constituyen la gestión integral de seguridad en la CGR.


Dado lo anterior, el SGS define los lineamientos que garantizan la seguridad de las personas, los bienes y la información, a través de una correcta gestión de riesgos de seguridad, lo que involucra la participación de todos los servidores públicos, contratistas de prestación de servicios, proveedores, visitantes y terceras partes, como elementos integrantes del Sistema, por cuanto la seguridad es responsabilidad de todos

En este contexto, el conjunto de políticas de seguridad es uno de los componentes del SGS, el que denota el compromiso de la Alta dirección con la seguridad en la Contraloría General de la República, que orientan el desarrollo de las buenas prácticas y lineamientos para preservar la seguridad en la Entidad.

Los propósitos de las políticas de seguridad son los siguientes:

- Proteger la integridad y bienestar de todas las personas (servidores públicos, contratistas de prestación de servicios, proveedores, visitantes y terceras partes) que hacen parte del SGS.
- Salvaguardar el capital humano, así como los recursos físicos y de información de la Entidad.
- Cuidar y defender la seguridad de personas, bienes e información de las amenazas.

De igual forma, es función de la Unidad y Seguridad y Aseguramiento Tecnológico e Informático - USATI prestar apoyo profesional y técnico para la formulación y ejecución de las políticas y programas de los servidores públicos, de los bienes y de la información de la Entidad, así como promover la celebración de convenios con Entidades u organismos nacionales e internacionales para garantizar la protección de las personas al servicio de la Contraloría General de la República, tal como lo establece el artículo 128 de la Ley 1474 de 2011.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del Riesgo, Seguridad y Continuidad del Negocio		Proceso: Gestión Integral de Seguridad	
	Políticas de Seguridad de Personas, Bienes e Información			
	Código: RSC-02-PO-003	Versión: 1.0	Fecha de Publicación en el Aplicativo: 23/08/2022	Página 4 de 32

De otra parte, para el componente de información del SGS, se adoptan las buenas prácticas de la Norma Técnica NTC-ISO 27001 del 2013, la cual define los requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un Sistema de Gestión de Seguridad de la Información -SGSI-; con la finalidad de preservar la confidencialidad, la integridad y disponibilidad de los activos de información.

2. Objetivos

- Establecer controles para mitigar el impacto de los riesgos que afecten la seguridad de las personas, los bienes e información y prevenir la materialización de dichos riesgos.
- Definir los controles que se deben implementar para preservar la confidencialidad, integridad y disponibilidad de la información y los activos de información que la gestionan.
- Fortalecer el conocimiento de los servidores públicos, contratistas y demás terceros de la CGR frente a las políticas de seguridad de personas, bienes e información.
- Establecer un marco de referencia para la protección frente a la seguridad de las personas, los bienes e información.

3. Campo de Aplicación

Las políticas establecidas en este documento son de obligatoria aplicación en la CGR por parte de los empleados públicos de carrera administrativa, provisionales, libre nombramiento y remoción, contratistas de prestación de servicios, proveedores de bienes y servicios y terceros relacionados.


4. Términos y Definiciones del Sistema de Gestión de Seguridad

Activo de información: Son los elementos de información que la entidad recibe o produce en el ejercicio de sus funciones, por lo tanto, se debe proteger. Incluye la información que se encuentre presente en forma impresa, escrita, en papel, transmitida por cualquier medio electrónico o almacenado en equipos de cómputo, incluyendo software, hardware, talento humano, datos contenidos en registros, archivos, bases de datos, videos e imágenes entre otros que tengan valor para la entidad de información clasificado e información reservada.

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000-2013).

Confidencialidad: Acceso a la información por parte únicamente de quienes estén autorizados, Según [ISO/IEC 13335-1: 2004]: "característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados"

Control: Son todas aquellas políticas, procedimientos, prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido, (Nota: Control es también utilizado como sinónimo de salvaguarda).

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del Riesgo, Seguridad y Continuidad del Negocio		Proceso: Gestión Integral de Seguridad	
	Políticas de Seguridad de Personas, Bienes e Información			
	Código: RSC-02-PO-003	Versión: 1.0	Fecha de Publicación en el Aplicativo: 23/08/2022	Página 5 de 32

Disponibilidad: Esta propiedad está destinada a garantizar el uso de los activos de información en el momento requerido, según [ISO/IEC 13335-1: 2004]: característica/ propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.

Gestión de incidentes de seguridad: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de las personas, bienes e información.

Información: La información constituye un importante activo, esencial para las actividades de una organización y, en consecuencia, necesita una protección adecuada. La información puede existir de muchas maneras, es decir, puede estar impresa o escrita en papel, puede estar almacenada electrónicamente (digital), ser transmitida por correo o por medios electrónicos, se la puede mostrar en videos, o exponer oralmente en conversaciones.

Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos.

Información pública clasificada. Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados.

Información pública reservada. Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados.

Mesa Técnica de Seguridad de la Información: Conformada por la DIARI, OSEI y la USATI mediante el memorando SIGEDOC 2020IE0032735 para dar cumplimiento a las metas institucionales en temas de seguridad informática y de la información, la cual se encuentra enmarcada en el Gobierno de TI, y que propende por la utilización de las mejores prácticas en la CGR.


Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000-2013). / Efecto de la incertidumbre sobre los objetivos. (ISO 31000-2018).

Riesgo Público: Suceso que puede afectar a una persona o a una comunidad determinada, sin necesidad que alguna de estas tenga alguna característica en particular. En ese sentido, el hecho de estar vivos nos hace estar en riesgo público.

Para mayor información sobre los términos y definiciones se podrán consultar en <https://clic-online.contraloria.gov.co/USATI/Documents/GLOSARIO%20SGS.pdf>

5. Política General de Seguridad


Declaración de Política: En la CGR, es importante la adecuada gestión de la seguridad de las personas, los bienes e información, por lo que la Entidad establece su compromiso para diseñar, desarrollar, implementar, mantener y mejorar constantemente las estrategias que aseguren la protección de las personas y los activos, mediante la ejecución de políticas, programas, controles, lineamientos, gestión de riesgos y mejores prácticas nacionales e internacionales a nivel de seguridad, en el marco de cumplimiento normativo y alineados con el plan estratégico de la Entidad.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del Riesgo, Seguridad y Continuidad del Negocio		Proceso: Gestión Integral de Seguridad	
	Políticas de Seguridad de Personas, Bienes e Información			
	Código: RSC-02-PO-003	Versión: 1.0	Fecha de Publicación en el Aplicativo: 23/08/2022	Página 6 de 32

Enunciado: En la CGR, la seguridad incluye acciones orientadas a establecer, evaluar y gestionar bajo el enfoque de resiliencia organizacional¹ los riesgos de seguridad que enfrentan las personas, los bienes y la información de la Entidad. Para la adecuada aplicación de las políticas establecidas en este documento la Entidad debe:

- Declarar el compromiso por parte de la Alta Dirección, los Líderes de macroproceso, Líderes de los procesos, y los directivos para el cumplimiento de los requisitos aplicables en materia de diseño, desarrollo, mantenimiento y mejoramiento de estrategias para la protección de las personas, los bienes y la información.
- Establecer y ejecutar estrategias de seguridad que permitan tomar acciones ante las amenazas, vulnerabilidades y riesgos que puedan afectar a las personas, bienes e información.
- Suministrar los recursos que fortalezcan la seguridad de las personas, bienes e información de la Entidad con el fin de fomentar prácticas efectivas en armonía con los sistemas de gestión existentes en la CGR.
- Establecer, implementar, mantener y fortalecer de forma permanente el programa de protección que permita gestionar la seguridad de las personas de la Entidad cuando se encuentren en situación de vulnerabilidad y riesgo derivado del ejercicio del cargo y/o del desempeño de funciones públicas.
- Asegurar que se cuente con el talento humano con conocimientos, competencias y formación idónea para poner en práctica las estrategias y acciones de seguridad definidos.
- Establecer controles para gestionar la seguridad de los bienes de la Entidad, con el fin de preservar la integridad, disponibilidad y seguridad de los mismos.
- Establecer los indicadores para medir el desempeño y el nivel de madurez y efectividad del SGS.
- Fortalecer permanentemente el mejoramiento continuo del SGS.
- Definir los objetivos de seguridad y gestionar las vulnerabilidades y los riesgos asociados a la misma.
- Establecer los acuerdos pertinentes en materia de seguridad entre la CGR y los grupos de valor y demás partes interesadas.
- Desarrollar y fortalecer alianzas estratégicas y convenios de cooperación con Entidades públicas y privadas, en los ámbitos nacional e internacional, que permitan el intercambio y apropiación de experiencias para la seguridad de las personas, los bienes y la información.
- Establecer controles para preservar la confidencialidad, la integridad y la disponibilidad de la información.

¹ Capacidad para superar y recuperarse ante situaciones adversas en la CGR.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del Riesgo, Seguridad y Continuidad del Negocio		Proceso: Gestión Integral de Seguridad	
	Políticas de Seguridad de Personas, Bienes e Información			
	Código: RSC-02-PO-003	Versión: 1.0	Fecha de Publicación en el Aplicativo: 23/08/2022	Página 7 de 32

- Desarrollar acciones de sensibilización y concientización a servidores públicos, contratistas de prestación de servicios, proveedores de servicios, terceros relacionados y demás personal sobre estas Políticas, para fortalecer la cultura de seguridad de las personas, los bienes y la información, al interior de la CGR.

5.1 Política de Organización de la Seguridad

Declaración de Política: La CGR, en aras de preservar la seguridad de las personas, los bienes y la información de la Entidad, establece su compromiso de definir e implementar una estructura para el gobierno de la seguridad mediante la expedición de la reglamentación respectiva y/o adopción de los procedimientos y demás instrumentos a que haya lugar.

Enunciado: La CGR contará con una organización administrativa y estratégica con el fin de diseñar, gestionar e implementar la seguridad de personas, bienes e información. Lo anterior se logra con la creación del Sistema de Gestión de Seguridad -SGS-, el Comité de Seguridad y el Programa de Protección y Seguridad del Contralor General de la República, los excontralores generales de la República y demás servidores de la Contraloría General de la República².

De conformidad con lo anterior, mediante el memorando radicado 2020IE0032735 se adoptó la mesa técnica de seguridad de la información.


5.2 Política de Talento Humano en Relación con la Seguridad de la Información

Declaración de Política: La CGR establece su compromiso de definir e implementar los controles necesarios en la vinculación, inducción, desarrollo, permanencia, retiro y cambio de funciones de los servidores públicos y contratistas de prestación de servicios para que conozcan el sentido y alcance de sus responsabilidades en relación con la confidencialidad, integridad y disponibilidad de la información a fin de reducir el nivel de riesgo por la exposición, pérdida, fraude o compromiso de la misma.

Enunciado: De conformidad con los lineamientos establecidos al interior de la Entidad en el marco del Talento Humano y la seguridad de los activos de información, y teniendo en cuenta que estos son un componente esencial para la operación y prestación de servicios; se hace necesario establecer controles que mitiguen el riesgo de fuga de información. Para tal fin la CGR debe:

- Permitir la verificación de la Entidad del sujeto, cualidades académicas y laborales, antecedentes disciplinarios, penales y fiscales, además de la verificación de referencias personales, familiares y laborales, en los procesos de selección de los funcionarios públicos vinculados a la CGR.
- Informar sobre las responsabilidades y compromisos con la seguridad de la información a la que tenga acceso en el desempeño de sus funciones una vez se vinculen servidores públicos o contratistas de prestación de servicios.

² Resoluciones Organizacionales OGZ-0531-2016, OGZ-0593-2017 y OGZ-0758-2020.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del Riesgo, Seguridad y Continuidad del Negocio		Proceso: Gestión Integral de Seguridad	
	Políticas de Seguridad de Personas, Bienes e Información			
	Código: RSC-02-PO-003	Versión: 1.0	Fecha de Publicación en el Aplicativo: 23/08/2022	Página 8 de 32

- Incluir en el acto administrativo, contrato de prestación de servicios o convenio dispuesto una vez se vincule el servidor público o contratista de prestación de servicios, los siguientes puntos:
 - Que establezca la responsabilidad y los compromisos con la seguridad de la información de carácter clasificado o reservado y que sea de su conocimiento durante el desarrollo de su actividad misional.
 - Que se contemplen acuerdos de confidencialidad y no divulgación de la información reservada y clasificada de la Entidad y que ésta se prolongue más allá de la terminación del vínculo laboral, contrato o convenio.
 - Derechos morales y patrimoniales de autor.
- Establecer en los programas de inducción, reinducción, entrenamiento y capacitación, los capítulos correspondientes a las responsabilidades sobre la formación que incluyan mecanismos y permitan determinar el grado de conciencia adquirido por el funcionario público vinculado a la CGR.


5.3 Política de Seguridad de la Información para el Trabajo por fuera de las Instalaciones Físicas de la CGR

Declaración de Política: La CGR, en aras de preservar la seguridad de la información, incluye la definición e implementación de controles para mantener la confidencialidad, disponibilidad e integridad de la información cuando ésta es tratada, usada, alimentada, explotada y, en general, gestionada fuera de las instalaciones físicas de la Entidad por parte de los funcionarios y contratistas de prestación de servicios de la CGR, y en armonía con la Ley 2088 de 2021, expedida por el Gobierno Nacional.

Enunciado: La CGR se compromete con la prestación del servicio y la ejecución de las funciones misionales de vigilancia y control, por lo que se presenta la alternativa de llevar a cabo el cumplimiento de las funciones del personal de la Entidad en la prestación del servicio, en instalaciones físicas por fuera de la CGR con base en el uso de las tecnologías de información y comunicación, y en concordancia con los marcos regulatorios aplicables a nivel nacional y territorial

Por lo tanto, para lograr la confidencialidad, integridad y disponibilidad de la información dentro de esta modalidad de trabajo, la CGR estable:

- Desarrollar el trabajo fuera de las instalaciones de la Entidad, con sujeción a la normativa general y reglamentación interna aplicables sobre el particular, siempre y cuando el mismo bajo tal circunstancia no implique retroceso, demoras y/o falta de calidad en el cumplimiento de las funciones y en la prestación de los servicios. Lo mismo aplica para el cumplimiento de las obligaciones contractuales de los contratistas de prestación de servicios de la CGR.
- Permitir la ejecución de las funciones asignadas a los funcionarios y contratistas de prestación de servicios de forma transitoria fuera del sitio designado legal o contractualmente, sin que ello modifique las condiciones pactadas inicialmente, siempre y cuando las funciones sean compatibles o permitan su correcto desarrollo o cumplimiento por fuera de las instalaciones de la entidad.
- Diseñar e implementar mecanismos de seguimiento y control que se consideren pertinentes, para asegurar la confidencialidad, integridad y disponibilidad de la información con respecto a las funciones institucionales asignadas a cada servidor público, y que se lleven a cabo por fuera de las instalaciones de la Entidad.


	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del Riesgo, Seguridad y Continuidad del Negocio		Proceso: Gestión Integral de Seguridad	
	Políticas de Seguridad de Personas, Bienes e Información			
	Código: RSC-02-PO-003	Versión: 1.0	Fecha de Publicación en el Aplicativo: 23/08/2022	Página 9 de 32

- Aplicar los principios de igualdad, eficacia, imparcialidad, publicidad y todos aquellos que se deriven del ejercicio de la función pública para el desarrollo de las labores misionales del trabajo por fuera de las instalaciones físicas de la Entidad.
- Mantener el cumplimiento de las prerrogativas laborales y sociales de los trabajadores incluyendo, pero no limitando, el respeto a los horarios laborales, el derecho a la desconexión, y el disfrute de jornadas de descanso como lo son las vacaciones, los festivos, las licencias y las demás reconocidas en la normatividad vigente.
- Permitir a los funcionarios de la CGR que trabajan por fuera de las instalaciones físicas de la entidad, el acceso efectivo y seguro a los sistemas de información institucionales, en los equipos de cómputo provistos por la Entidad, mediante la instalación del software de conectividad necesario para el correcto desempeño de sus funciones y cumpliendo los requisitos de seguridad de la información y licenciamiento de los aplicativos de software específico para el desarrollo de sus funciones.
- Permitir el traslado de los equipos de cómputo de propiedad de la entidad al lugar externo de trabajo del funcionario de la CGR, asegurando la instalación, configuración y funcionamiento adecuado de las herramientas de seguridad de la información en cada uno de los equipos institucionales.
- Promover el uso de equipos de cómputo de propiedad de la Entidad para el trabajo por fuera de las instalaciones, evitando en lo posible el uso de equipos personales por parte de los funcionarios de la CGR, en razón a que por condiciones de licenciamiento de software, estos equipos no pueden tener todos los controles de seguridad de la información que se requieren para desarrollar sus actividades preservando la confidencialidad, integridad y disponibilidad de la información de propiedad de la CGR.
- Realizar capacitaciones, sensibilizaciones y transferencias de conocimiento a los servidores públicos a los cuales les sea autorizados el trabajo por fuera de las instalaciones de la Entidad, en lo relacionado al correcto uso de las tecnologías de información y comunicación, la seguridad de personas, bienes e información.
- Verificar el cumplimiento de las directrices asociadas a la seguridad de equipos y de información propios de la CGR.

5.4 Política de Seguridad de las Personas

Declaración de Política: La CGR es el máximo órgano de control fiscal del Estado, por ende, es la responsable de la protección integral de las personas que se encuentran en riesgo extraordinario o extremo, o en razón del ejercicio de su cargo en la CGR, por lo cual establece su compromiso de coordinar con las autoridades competentes la protección de los derechos a la vida, la libertad, la integridad y seguridad del señor Contralor General de la República, los ex Contralores Generales de la República y todos los servidores de la Entidad.


Enunciado: En la CGR, el talento humano constituye un activo primordial para el ejercicio y desarrollo de su misión constitucional y legal, como máximo órgano de control fiscal del Estado. Por lo tanto, la Entidad debe definir, elaborar, implementar, mantener y mejorar constantemente los procedimientos internos de seguridad de personas, que permitan una coordinación eficiente y segura con las autoridades y órganos competentes en la protección de los derechos a la vida, así como fomentar y fortalecer dichos procedimientos mediante la cooperación interinstitucional en desarrollo del principio de colaboración armónica constitucional. Para tal fin, la CGR debe:

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del Riesgo, Seguridad y Continuidad del Negocio		Proceso: Gestión Integral de Seguridad	
	Políticas de Seguridad de Personas, Bienes e Información			
	Código: RSC-02-PO-003	Versión: 1.0	Fecha de Publicación en el Aplicativo: 23/08/2022	Página 10 de 32

- Realizar y actualizar cuando amerite el estudio de nivel de riesgo, a las personas objeto del programa de protección y seguridad de la Entidad y gestionar lo correspondiente para que los organismos de seguridad del Estado realicen la asignación directa y oportuna de los recursos humanos y físicos.
- Adoptar y gestionar las medidas de protección para la seguridad de las personas.
- Administrar los riesgos de seguridad de las personas, verificar y evaluar la efectividad de sus controles asociados.
- Diseñar los programas de protección y seguridad del Contralor General de la República, excontralores generales y demás servidores de la Entidad, de acuerdo con el nivel de riesgo al que estén sometidos.
- Definir los lineamientos técnicos para las medidas de protección y seguridad de las personas.
- Además de los principios constitucionales y legales que orientan a la Contraloría General de la República en el ejercicio del control fiscal y la función administrativa, los procedimientos de seguridad de personas y las acciones a desarrollar en ejecución de la presente política, para todos sus intervinientes, se registrarán por los siguientes principios:
 - **Consentimiento:** Manifestación expresa, libre, informada y voluntaria por parte del peticionario respecto de la aceptación o no de su vinculación laboral.
 - **Causalidad:** Conexidad directa entre los riesgos en el marco de la Resolución 0758 del 2020 y el ejercicio de las actividades o funciones que desempeña los servidores públicos en razón de su profesión o de carácter misional dentro de la Contraloría General de la República. Los interesados en ser acogidos por el programa de protección y seguridad de las personas, deben demostrar, siquiera sumariamente, dicha conexidad, para ser confirmada o descartada, lográndose de esta manera una clasificación objetiva.
 - **Enfoque Diferencial:** Para la Evaluación de Riesgo, así como para la recomendación y adopción de las medidas de protección y seguridad, deberán ser observadas las especificidades y vulnerabilidades por edad, etnia, género, discapacidad, orientación sexual y procedencia urbana o rural de las personas objeto de protección.
 - **Protección:** Deber del Estado colombiano de adoptar medidas especiales para personas, grupos o comunidades en situación de riesgo extraordinario o extremo, que sean objeto de este Programa, con el fin de salvaguardar sus derechos.
 - **Reserva Legal:** La información relativa a los solicitantes de activación de los procedimientos de protección a personas será de carácter reservado y confidencial.
- Coordinar con la Gerencia de Talento Humano la formulación de los lineamientos y recomendaciones para minimizar la posible materialización del riesgo público en el desarrollo de sus funciones, actividades y labores en el nivel central y gerencias departamentales, a fin de que sea aplicado para la generación de una cultura de autocuidado, autoprotección, buenos hábitos y prácticas en seguridad.

5.5 Política de Responsabilidad por los Activos

Declaración de Política: La CGR, como propietaria de la información, establece su compromiso de asignar como corresponda, sin perjuicio de definir los controles pertinentes a los activos de información, la responsabilidad sobre los activos de información a los servidores públicos, contratistas de prestación de servicios, proveedores y terceros que

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del Riesgo, Seguridad y Continuidad del Negocio		Proceso: Gestión Integral de Seguridad	
	Políticas de Seguridad de Personas, Bienes e Información			
	Código: RSC-02-PO-003	Versión: 1.0	Fecha de Publicación en el Aplicativo: 23/08/2022	Página 11 de 32

necesiten realizar las funciones y actividades correspondientes a su misión y objetivos; dicha responsabilidad se enmarca en todo el ciclo de vida de la información, que incluye su creación, procesamiento, almacenamiento, transferencia, transmisión, así como su disposición final.

Enunciado: En la CGR, los activos de información constituyen una parte esencial para la operación, prestación de servicios y generación de productos enmarcados dentro de los procesos institucionales que soportan la toma de decisiones, los cuales deben realizarse en un entorno seguro, conforme a los requisitos legales, contractuales y normativos correspondientes; para tal fin la CGR debe:


- Definir e implementar controles para el buen uso de los activos de información, aplicando la normatividad y las buenas prácticas existentes enmarcados en la capacidad tecnológica de la Entidad.
- Establecer procedimientos, instructivos, guías y demás documentos para la gestión segura de los activos de información.
- Elaborar, documentar y mantener actualizado el inventario de la información y de los activos de información asociados, en especial los relacionados con el ciclo de vida de la información.
- Asignar responsables para cada uno de los activos de información para su protección y gestión en todo el ciclo de vida del activo.
- Aplicar controles enmarcados en la capacidad tecnológica de la Entidad para que, una vez terminada la relación contractual o finalizado el vínculo con la CGR, sean restituidos los activos de información que se hayan entregado para el cumplimiento de sus labores.
- Elaborar una metodología para la gestión de los riesgos de seguridad digital y activos de información y además implementar un sistema de reporte de incidentes que permita que todos los servidores públicos y contratistas de prestación de servicios informen de posibles incidentes de seguridad.

Todos los funcionarios de la CGR son responsables de custodiar y salvaguardar la información que tienen a su cargo como se encuentra establecido en la Ley 1952 de 2019, por la cual se expide el Código Disciplinario Único. *“Artículo 38. Deberes. Numeral 6: Custodiar y cuidar la documentación e información que por razón de su empleo, cargo o función conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebidas”.*

5.6 Política de Clasificación de Información y Manejo de Medios

Declaración de Política: La información y los activos de información deben ser clasificados y protegidos en función de los requisitos legales, valor y criticidad para la Entidad. Tomando en consideración que en el desarrollo de las actividades relacionadas con la protección de la seguridad de la información es posible encontrar información en estados no definitivos o que corresponda a información de carácter personal se tendrán en cuenta estos dos tipos adicionales de clasificación información de uso interno e información de carácter personal.

El esquema de clasificación debe incluir las convenciones y criterios para su clasificación en el tiempo que deben considerar primordialmente la confidencialidad, integridad y disponibilidad de los activos de información en todo su ciclo de vida.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del Riesgo, Seguridad y Continuidad del Negocio		Proceso: Gestión Integral de Seguridad	
	Políticas de Seguridad de Personas, Bienes e Información			
	Código: RSC-02-PO-003	Versión: 1.0	Fecha de Publicación en el Aplicativo: 23/08/2022	Página 12 de 32

Enunciado: En la CGR, la información constituye un activo esencial para la operación, prestación de servicios y generación de productos enmarcados dentro de los procesos institucionales que soportan la toma de decisiones, por lo que debe ser protegida de acuerdo con su importancia para la Entidad teniendo en cuenta criterios para su clasificación y etiquetado, así como el manejo de los activos y medios requeridos en todo el ciclo de vida de la información. Por tal razón, la CGR debe:


- Definir categorías de clasificación de la información y reglas para el manejo, copiado, reproducción, almacenamiento, autorización de acceso, uso, disposición y derecho a conocer la información. Estas categorías deben considerar los requisitos legales, valor, criticidad y procesos en los que se utiliza la misma.
- Establecer los criterios para la clasificación y desclasificación de la información institucional y los activos de información. Así mismo, socializarlos a quienes deberán aplicarlos y propender por su cumplimiento.
- Asignar los responsables de la información y los activos de información, quienes responderán por la debida clasificación de la misma, utilizando los criterios de clasificación y desclasificación de la información institucional.
- Implementar un procedimiento para el etiquetado ya sea de forma física o electrónica que facilite el reconocimiento de la información.
- Establecer controles para el uso, respaldo, modificación, borrado seguro o destrucción de información alojada en los medios de almacenamiento utilizados en la Entidad.
- Disponer de los medios de almacenamiento de forma segura cuando estos no se requieran o se encuentren deteriorados.
- Proteger los medios de almacenamiento contra accesos o usos no autorizados.

5.7 Política de Seguridad de los Bienes

Declaración de Política: La CGR como máximo órgano de control fiscal del Estado, establece su compromiso de preservar la seguridad de sus bienes, para el correcto ejercicio de su misión constitucional y legal.

Enunciado: En la Contraloría General de la República los bienes constituyen uno de los activos esenciales para el ejercicio y desarrollo de su misión constitucional y legal. Para la aplicación de esta política la CGR debe:

- Realizar periódicamente una evaluación del riesgo, la vulnerabilidad y la criticidad de las instalaciones de la Entidad realizando un análisis del entorno, con el fin de determinar el nivel y tipos de amenazas a las que se está expuesto.
- Disponer con servicio de vigilancia con las competencias necesarias para hacer frente a la inseguridad que puedan poner en riesgo la integridad de las instalaciones y sus ocupantes.
- Establecer contactos con autoridades pertinentes tales como Policía, Fuerzas Militares, entre otros que puedan prestar servicios de apoyo en caso de presentarse un incidente.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del Riesgo, Seguridad y Continuidad del Negocio		Proceso: Gestión Integral de Seguridad	
	Políticas de Seguridad de Personas, Bienes e Información			
	Código: RSC-02-PO-003	Versión: 1.0	Fecha de Publicación en el Aplicativo: 23/08/2022	Página 13 de 32


- Mantener actualizado el inventario de equipos de seguridad adquiridos o administrados por la Entidad y garantizar su adecuado uso y sus mantenimientos preventivos y correctivos bajo ANS (acuerdos de niveles de servicios), con el fin de garantizar su disponibilidad.
- Definir y aplicar medidas de protección contra las amenazas de origen ambiental (desastres naturales, inundaciones, conflagraciones).
- Definir y vigilar el perímetro de seguridad física de las instalaciones de la CGR, con el fin de detectar personas, vehículos y elementos extraños que puedan generar riesgo.
- Aplicar controles de seguridad electrónicos en cada uno de los ingresos peatonales y vehiculares a la CGR tales como detección de paquetes y objetos, detección de metales, Circuito Cerrado de Televisión -CCTV-, entre otros.
- Disponer de personal capacitado para la operación de sistemas de seguridad electrónica de la Entidad.
- Constituir pólizas de seguro contra riesgos que puedan afectar los bienes muebles e inmuebles de la Entidad.
- Gestionar las acciones necesarias para diseñar, implementar y monitorear los sistemas de seguridad físicos y electrónicos para cada una de las áreas de la CGR.
- Monitorear el funcionamiento, administrar y aplicar los controles necesarios desde el nivel central para el funcionamiento seguro en cada una de las sedes de la CGR, en los casos que aplique.

5.8 Política de Control de Acceso

Declaración de Política: La CGR, en aras de preservar la seguridad de las personas, los bienes y la información de la Entidad, establece su compromiso de definir e implementar los controles necesarios para el acceso a sus instalaciones evitando la pérdida de confidencialidad, integridad y disponibilidad de la información, así como para mantener la integridad física de las personas y la protección de los bienes de la CGR.

Enunciado: En la CGR, se hace necesario definir y aplicar controles de acceso a la infraestructura física, infraestructura computacional, servicios tecnológicos, sistemas de información, entre otros, con el fin de conservar la integridad de las personas, la protección de los bienes y la confiabilidad e integridad de la información de este órgano de control. Para tal fin, la CGR debe:

- Aplicar el principio de caducidad a los accesos concedidos, teniendo en cuenta los criterios definidos para cada uno de estos.
- Definir y aplicar los controles necesarios para prevenir el acceso no autorizado a instalaciones, infraestructura, servicios tecnológicos y sistemas de información; incluyendo las áreas de procesamiento de información.
- Aplicar los principios del mínimo privilegio para conceder los accesos, teniendo en cuenta los perfiles de los usuarios a los sistemas de información, ajustados a las funciones, necesidades y autorizaciones por parte de los responsables.
- Establecer los diferentes controles de accesos múltiples y complementarios cuando sea necesario.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del Riesgo, Seguridad y Continuidad del Negocio		Proceso: Gestión Integral de Seguridad	
	Políticas de Seguridad de Personas, Bienes e Información			
	Código: RSC-02-PO-003	Versión: 1.0	Fecha de Publicación en el Aplicativo: 23/08/2022	Página 14 de 32

- Aplicar el principio de trazabilidad para que en cada control se registren los accesos y se realicen las gestiones sobre dichos registros, a fin de mantener las bases de datos actualizadas.

5.9 Política de Controles Criptográficos


Declaración de Política: La CGR; genera, procesa, almacena, despliega y transmite información por lo cual la Entidad establece su compromiso de gestionar lo necesario para la protección de esta principalmente aquella que ha sido categorizada como clasificada o reservada, considerando la confidencialidad, integridad, autenticidad y no repudio de la información, durante todo el ciclo de vida de la misma.

Enunciado: En la CGR, la información constituye un activo esencial para la operación, prestación de servicios y generación de productos enmarcados dentro de los procesos institucionales que provee la Entidad por lo que debe ser protegida de acuerdo con su importancia para la Entidad. Para tal fin, la CGR debe:

- Realizar una evaluación de riesgos de seguridad con el fin de establecer el nivel de protección necesario, mediante la aplicación de controles criptográficos.
- Establecer controles para la gestión de las claves criptográficas.
- Implementar la herramienta de cifrado en todos los equipos de cómputo de la Entidad, la cual será la única autorizada para el cifrado de información institucional.
- Considerar las medidas de protección para el intercambio de información cifrada o cuando se requiera del transporte o distribución tanto manual como electrónica de las claves criptográficas.
- Mantener copia de las claves de cifrado en un lugar seguro de forma que la recuperación de la información cifrada sea posible en caso de ausencia temporal o definitiva del custodio o responsable de las claves y de la información cifrada.
- Determinar que los propietarios son los responsables del cifrado de la información que tengan a su cargo.
- Permitir la auditabilidad de todo proceso de cifrado de la información por parte de los responsables del mismo incluyendo el registro (logging) de las actividades correspondientes.
- Mantener actualizada la documentación sobre la utilización de la criptografía en la Entidad incluyendo las actividades sobre la gestión de las claves para el cifrado de información.
- En los casos que se requiera el almacenamiento de información de tipo confidencial, personal o sensible en servicios cloud o de nube, ésta se debe mantener en la medida de lo posible cifrada para evitar su divulgación o accesos no autorizados.

5.10 Política de Seguridad Física y del Entorno

Declaración de Política: La CGR, en aras de preservar la seguridad de las personas, los bienes y la información, establece su compromiso de definir e implementar los controles que eviten el acceso físico no autorizado a las instalaciones de procesamiento de la información y a sus áreas circundantes.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del Riesgo, Seguridad y Continuidad del Negocio		Proceso: Gestión Integral de Seguridad	
	Políticas de Seguridad de Personas, Bienes e Información			
	Código: RSC-02-PO-003	Versión: 1.0	Fecha de Publicación en el Aplicativo: 23/08/2022	Página 15 de 32

Enunciado: En la CGR, el procesamiento de la información requerida para la toma de decisiones en la Entidad se realiza en un entorno seguro. Para tal fin, la CGR debe:


- Realizar una evaluación de riesgos de seguridad a fin de establecer el nivel de protección física y del entorno.
- Definir perímetros de seguridad física para proteger las áreas de procesamiento de información.
- Diseñar y aplicar controles de seguridad física para la entrada a las oficinas, despachos, salas e instalaciones en especial aquellas donde se procese información crítica.
- Realizar el monitoreo continuo a las instalaciones de procesamiento de información y sus áreas circundantes.
- Definir y aplicar medidas de protección contra las amenazas externas (vandalismo, asonadas, terrorismo entre otros) y de origen ambiental (desastres naturales, inundaciones, conflagraciones entre otros).
- Diseñar y aplicar los controles especiales para acceder y desarrollar trabajos en áreas consideradas seguras.
- Aplicar controles para la ubicación y protección de los equipos de procesamiento y acceso a la información.
- Aplicar medidas de seguridad y protección del cableado (eléctrico, telecomunicaciones) de la Entidad, contra interceptación, interferencia o daños.
- Implementar controles para el retiro de los activos de la CGR en especial aquellos que contengan información.

5.11 Políticas de Seguridad de Equipos

Declaración de Política: La CGR, como propietaria de su infraestructura tecnológica que se encuentra tanto dentro de sus instalaciones como fuera de ella y, además, como responsable de los activos de información que no son de su propiedad, establece su compromiso de definir e implementar los controles pertinentes para el uso y administración, que realizan los responsables y encargados en cada una de las dependencias de la Entidad, para el desarrollo de su misión, objetivos y funciones. En consecuencia, los responsables y encargados de los activos de infraestructura tecnológica deben gestionar oportunamente su seguridad con el fin de prevenir afectaciones a la operación de la CGR.

Enunciado: En la CGR, la información constituye un activo esencial para la operación, prestación de servicios y generación de productos enmarcados dentro de los procesos institucionales que soportan la toma de decisiones, por lo que la infraestructura tecnológica que se encuentre en las instalaciones o fuera de ella, se debe proteger para prevenir la afectación de la operación de la Entidad. Por lo anterior, la CGR debe:


- Los usuarios de los sistemas de información deben aplicar los controles definidos relacionados con la seguridad de los equipos y activos de la infraestructura tecnológica de la Entidad durante su ciclo de vida: adquisición, utilización u operación, mantenimiento y retiro o renovación.
- Los equipos y activos de infraestructura tecnológica de la Entidad deben estar ubicados en áreas protegidas dentro de la CGR, para asegurar que sólo sean utilizados por el personal autorizado.
- Asegurar los equipos que pertenezcan a la Entidad como: computadores, servidores, red de comunicaciones y activos de infraestructura tecnológica que se encuentren fuera de las instalaciones de la CGR.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del Riesgo, Seguridad y Continuidad del Negocio		Proceso: Gestión Integral de Seguridad	
	Políticas de Seguridad de Personas, Bienes e Información			
	Código: RSC-02-PO-003	Versión: 1.0	Fecha de Publicación en el Aplicativo: 23/08/2022	Página 16 de 32

- Los equipos y activos de infraestructura tecnológica que se encuentren ubicados cerca de zonas de atención o tránsito de público deben estar asegurados o vigilados físicamente (CCTV, sistema de control de acceso) para que no sean retirados sin autorización del puesto de trabajo donde se ubican.
- Los equipos pertenecientes a la infraestructura tecnológica de la Entidad deben estar protegidos contra afectaciones por fallas en la infraestructura de servicios de la CGR. Los activos de información críticos en especial servidores, red de comunicaciones y sistemas de aire acondicionado, entre otros, deben contar, en lo posible, con sistemas de redundancia.
- Los equipos y activos de infraestructura tecnológica deben contar con medidas de protección y verificación complementarios, tales como: sistemas de control de acceso, sistemas de detección y extinción de incendios y CCTV a fin de mantener seguro su entorno de factores como humo, incendios, deficiencias en la ventilación o aire acondicionado, energía y acceso no autorizado, entre otros.
- Planear y realizar periódicamente los mantenimientos preventivos y correctivos a los equipos pertenecientes a la infraestructura tecnológica de la Entidad, para preservar su disponibilidad.
- Contratar pólizas de seguros para los equipos pertenecientes a la infraestructura tecnológica de la Entidad, usando criterios de mérito.
- Las áreas responsables de los equipos pertenecientes a la infraestructura tecnológica son las únicas autorizadas para efectuar traslados o movimientos de los recursos a su cargo. Ninguna persona puede disponer de los equipos de la Entidad sin cumplir con los requisitos de seguridad aplicables. En caso de requerirse el transporte de los mismos se deben cumplir estrictamente las medidas de seguridad que preserven la integridad física de las personas y los equipos.
- Para la disposición o reutilización de los equipos pertenecientes a la infraestructura tecnológica de la Entidad, se debe preservar la confidencialidad, integridad y disponibilidad de la información alojada en éstos, para lo cual se deben aplicar controles como copias de seguridad y borrado seguro.
- Establecer controles para reducir los riesgos generados por las amenazas ambientales.
- En el evento que sea necesario acceder a los equipos o a su información por temas técnicos, de seguridad, administrativos, judiciales o disciplinarios, los servidores públicos deben recordar que la información personal podrá ser accesible por parte de la Entidad.
- Se permitirá el acceso de los equipos de cómputo personales a la infraestructura tecnológica de la CGR, siempre y cuando el responsable del equipo de cómputo acepte los lineamientos establecidos por la Entidad para tal fin.
- Establecer controles para el respaldo, borrado seguro o destrucción de información alojada en los equipos cuando estos son datos de baja.

5.12 Política de Escritorio Limpio y Pantalla Limpia

Declaración de Política: La CGR establece su compromiso de definir e implementar los controles relacionados con la limpieza y presentación de escritorio físico, pantalla limpia, puesto de trabajo, y de equipos de cómputo a cargo de cada servidor público y contratista de prestación de servicios a partir de la definición de los lineamientos respectivos.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del Riesgo, Seguridad y Continuidad del Negocio		Proceso: Gestión Integral de Seguridad	
	Políticas de Seguridad de Personas, Bienes e Información			
	Código: RSC-02-PO-003	Versión: 1.0	Fecha de Publicación en el Aplicativo: 23/08/2022	Página 17 de 32

Enunciado: La CGR promueve una cultura de seguridad de escritorio limpio y pantalla limpia, con el objetivo de reducir los riesgos de acceso no autorizado, pérdida, alteración o fuga de información, además de fortalecer la percepción que sobre seguridad tienen los servidores públicos y contratistas de prestación de servicios, así como los terceros ajenos a la CGR que estén cerca a los equipos de la Entidad. Para tal fin el personal de la CGR debe tener en cuenta:


- Mantener apagados los equipos cuando no estén en uso, adicionalmente deben bloquear la sesión con clave de acceso cuando los dejen desatendidos. Dentro de este mismo contexto, para los equipos servidores, se debe cerrar la sesión del usuario.
- Conservar la pantalla de escritorio de los equipos de cómputo limpia, libre de archivos, carpetas y accesos directos, salvo aquellos que permitan el ingreso a las aplicaciones institucionales.
- Retirar de manera inmediata toda la información pública reservada o clasificada e información personal semiprivada, privada y sensible de las impresoras, copadoras, escáneres y fax, así como los dispositivos de almacenamiento extraíbles, teniendo en cuenta que este tipo de información no se debe dejar en el escritorio sin la debida custodia. Los documentos físicos que van a ser desechados deben ser debidamente destruidos antes de su disposición final.
- Mantener los puestos de trabajo físicos debidamente organizados, limpios y sin información pública reservada o clasificada e información personal semiprivada, privada y sensible a la vista. Esta deberá ser guardada bajo llave, elemento que también debe permanecer bajo custodia.

5.13 Política de Procedimientos Operacionales y Responsabilidades

Declaración de Política: La CGR establece su compromiso de definir e implementar los controles necesarios para la administración y la operación de las instalaciones de procesamiento de información que soportan los procesos, gestionan la eficiencia y mejora continua de los controles implantados y los procesos operativos asociados, a fin de proteger la confidencialidad, la integridad y la disponibilidad de la información de la Entidad.

Enunciado: La CGR promueve y fortalece la administración y la operación de las instalaciones de procesamiento de información que permite una mejora continua de los controles desarrollados en los procesos operativos. Por lo cual la CGR debe:

- Documentar y mantener actualizados todos sus procedimientos operativos para mantener la disponibilidad, integridad y confidencialidad de la información; y por ende realizar una operación segura definiendo los roles, responsabilidades y procedimientos de gestión.
- Establecer controles para la gestión de cambios normales y de emergencia a nivel de infraestructura, aplicativos y servicios tecnológicos.
- Establecer el comité gestión de cambios, quien se encargará de evaluar, aprobar o negar la implementación de los cambios.
- Evaluar las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas de capacidad.
- Monitorear el rendimiento de la infraestructura tecnológica para determinar el uso de la capacidad existente.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del Riesgo, Seguridad y Continuidad del Negocio		Proceso: Gestión Integral de Seguridad	
	Políticas de Seguridad de Personas, Bienes e Información			
	Código: RSC-02-PO-003	Versión: 1.0	Fecha de Publicación en el Aplicativo: 23/08/2022	Página 18 de 32

- Asignar los recursos adecuados de hardware y software, para todos los servicios y aplicaciones de tecnología.
- Separar de manera física y lógica los ambientes de desarrollo, pruebas y producción para las aplicaciones de software.
- Considerar los controles necesarios para asegurar que las migraciones entre los ambientes de desarrollo, pruebas y producción han sido aprobadas, de acuerdo con el procedimiento de control de cambios de la CGR.
- Utilizar en los ambientes de prueba de software datos que no sean sensibles para la Entidad.
- Verificar que los ambientes de prueba, desarrollo y producción sean similares, para prevenir situaciones en las cuales el software desarrollado presente comportamientos distintos y errores.
- Utilizar nombres de dominios diferentes para los ambientes de prueba, desarrollo y producción para evitar confusión y diferenciar de manera clara cada ambiente. Además, realizar las pruebas funcionales y no funcionales necesarias y pertinentes para que el software desarrollado cumpla con las especificaciones acordadas.
- Verificar que los desarrolladores realicen su trabajo exclusivamente en el ambiente de desarrollo y nunca en los ambientes de pruebas o producción.
- Dar cumplimiento a los lineamientos establecidos en la Política de Gobierno Digital.^{3y 4}


5.14 Política de Protección contra Códigos Maliciosos

Declaración de Política: La CGR establece su compromiso de definir y aplicar procedimientos operacionales y socializar los riesgos asociados con el código malicioso, además de gestionar lo pertinente para contar con una plataforma de hardware y software dotada de herramientas especializadas que coadyuven en la detección, prevención y recuperación de las amenazas generadas por virus, troyanos, gusanos y todo tipo de código malicioso a nivel de red, estaciones de trabajo, servidores y aplicaciones.

Enunciado: En la CGR, la información constituye un activo esencial para la operación, prestación de servicios y generación de productos, procesamiento, almacenamiento, entrega y exposición de información, que se realiza en un entorno seguro y controlado, libre de amenazas de códigos maliciosos. Por lo cual, la CGR debe:

³ <http://es.presidencia.gov.co/normativa/normativa/DECRETO%201008%20DEL%2014%20DE%20JUNIO%20DE%202018.pdf>

⁴ <https://mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/162626:MinTIC-expide-la-resolucion-que-establece-los-lineamientos-y-estandares-para-la-estrategia-de-seguridad-digital>

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del Riesgo, Seguridad y Continuidad del Negocio		Proceso: Gestión Integral de Seguridad	
	Políticas de Seguridad de Personas, Bienes e Información			
	Código: RSC-02-PO-003	Versión: 1.0	Fecha de Publicación en el Aplicativo: 23/08/2022	Página 19 de 32


- Aplicar controles para detectar, prevenir y eliminar el software no autorizado presente en la infraestructura tecnológica de la CGR.
- Establecer controles de seguridad para evitar incidentes de seguridad de la información generados por la presencia de código malicioso en los equipos de cómputo, redes de comunicaciones, dispositivos de almacenamiento fijos o removibles de los computadores o dispositivos informáticos.
- Usar un software de protección contra código malicioso (antivirus) y mantenerlo activo en todos los computadores, dispositivos móviles, teléfonos inteligentes y cualquier tipo de equipo de cómputo empleado para acceder a los servicios y sistemas de información de la CGR. Este software deberá estar actualizado con la versión más reciente.
- Sensibilizar a los servidores públicos sobre el cuidado para detener, desinstalar o alterar el funcionamiento del software de antivirus.
- Implementar un servicio especializado, preferiblemente centralizado para la detección y contención de código malicioso en todos los servidores e infraestructura tecnológica de la Entidad con el apoyo de herramientas de hardware y software estándar debidamente autorizadas.
- Establecer y articular los procedimientos de recuperación contra ataques por código malicioso con: La estrategia de continuidad del negocio definida en la Entidad, con la gestión de vulnerabilidades que permita identificar, priorizar y dar tratamiento permanente a las vulnerabilidades de carácter tecnológico, con la gestión de incidentes de seguridad y la gestión de cambios de la Entidad.

5.15 Política de Copias de Respaldo

Declaración de Política: La CGR establece su compromiso de definir e implementar los controles necesarios para asegurar el respaldo de la información, como parte de la estrategia de continuidad de negocio siguiendo los procedimientos que implemente para desarrollar dicha estrategia.

Enunciado: La información constituye un activo esencial para la operación, prestación de servicios y generación de productos enmarcados dentro de los procesos institucionales en la CGR, por lo cual se debe asegurar el almacenamiento de la misma mediante la ejecución de procedimientos y controles que permitan el resguardo y conservación de la información en los medios dispuestos por la Entidad. Por lo cual, la CGR debe:

- Respaldar la información de los procesos de acuerdo con requisitos legales, nivel de clasificación de la información, períodos de retención documental y requerimientos de uso establecidos por la CGR.
- Documentar el esquema de preservación de las copias de respaldo, identificación de la información a respaldar, periodicidad de ejecución de la copia de respaldo, nivel de clasificación de la información respaldada, período de retención y rotación de las copias de respaldo, el medio de almacenamiento y la tecnología utilizada.
- Preservar las copias de respaldo por el tiempo definido y aprobado por los responsables a los que pertenece la información.
- Almacenar las copias de respaldo en sitios seguros con controles físicos y tecnológicos que permitan el cumplimiento de los estándares mínimos necesarios.


	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del Riesgo, Seguridad y Continuidad del Negocio		Proceso: Gestión Integral de Seguridad	
	Políticas de Seguridad de Personas, Bienes e Información			
	Código: RSC-02-PO-003	Versión: 1.0	Fecha de Publicación en el Aplicativo: 23/08/2022	Página 20 de 32

- Cifrar las copias de respaldo que contengan información reservada, en concordancia con la Política de Controles Criptográficos.
- Realizar pruebas de restauración a las copias de respaldo con el fin de asegurar la disponibilidad de las mismas, dejando la evidencia de la ejecución, para efectos de las revisiones y auditorías que sean requeridas.
- Proceder con la destrucción o disposición final de los medios, cumpliendo los requisitos de retención que así lo establezcan.
- Establecer los requisitos mínimos de la tecnología que debe utilizarse (redes de almacenamiento, cintas magnéticas, almacenamiento en la nube con esquemas de redundancia, entre otros) para la generación de las copias de respaldo, así como las características de los medios de almacenamiento respectivos.
- Alojarse copias de respaldo fuera de las instalaciones de la CGR en un sitio que asegure su custodia, conservación, seguridad y consulta, como puede ser el almacenamiento en la nube u otros medios de almacenamiento de información externos.

5.16 Política de Registro y Seguimiento de Eventos de Seguridad

Declaración de Política: La CGR, en aras de preservar la confidencialidad, integridad y disponibilidad de la información, establece su compromiso de definir e implementar los controles necesarios para llevar la trazabilidad de los eventos de seguridad que se generan en las plataformas tecnológicas de la Entidad.

- **Enunciado:** En la CGR, la información y los activos de información son esenciales para la operación, prestación de servicios y generación de productos enmarcados dentro de los procesos institucionales de la Entidad, por lo que es necesario registrar y revisar regularmente los eventos de seguridad de la información. Por lo cual, la CGR debe
- Desarrollar actividades para la detección y reporte de amenazas, vulnerabilidades técnicas y eventos de seguridad que puedan transformarse en incidentes de seguridad y que causen afectación a la confidencialidad, disponibilidad e integridad de la información.
- Integrar la gestión de eventos con la gestión de incidentes de seguridad de la Entidad y la toma de decisiones correspondiente a la identificación del riesgo.
- Habilitar la auditoría de eventos de seguridad en todos los sistemas de información que se encuentren operativos en la Entidad.
- Proteger los registros de eventos contra el acceso no autorizado, exposición, pérdida, alteración, fraude o manipulación por parte de usuarios con privilegios especiales como los administradores del sistema, de las bases de datos o de las aplicaciones de la CGR.
- Gestionar la capacidad de almacenamiento de los registros de eventos y proyectar futuras demandas de capacidad para evitar la pérdida de información de los registros por razones de sobreescritura.
- Sincronizar los relojes de los servidores, sistemas y servicios dentro de la CGR con un tiempo convenido y proveniente de una única fuente.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del Riesgo, Seguridad y Continuidad del Negocio		Proceso: Gestión Integral de Seguridad	
	Políticas de Seguridad de Personas, Bienes e Información			
	Código: RSC-02-PO-003	Versión: 1.0	Fecha de Publicación en el Aplicativo: 23/08/2022	Página 21 de 32

5.17 Política de Control de Software Operacional

Declaración de Política: La CGR, en aras de preservar la confidencialidad, integridad y disponibilidad de la información, establece su compromiso de definir e implementar los controles necesarios para la instalación y actualización del software operativo en la plataforma tecnológica de la Entidad.

Enunciado: En la CGR, los activos de información y la información constituyen un activo esencial para la operación, prestación de servicios y generación de productos enmarcados dentro de los procesos institucionales, por lo que es necesario controlar la instalación/actualización/modificación de software operativo en la plataforma tecnológica de la Entidad. Por lo cual, la CGR debe


- Definir las responsabilidades que permitan realizar y controlar de manera segura la instalación/actualización/modificación de aplicaciones, utilitarios y servicios de las Tecnologías de la Información y Comunicaciones -TIC en general relacionados con el software operativo en la plataforma tecnológica de la Entidad.
- Habilitar un sistema de versionamiento de código que permita mantener el registro de la versión/modificación/reléase del programa, utilitario o software instalado en la plataforma tecnológica.
- Autorizar el acceso lógico y físico a los proveedores para realizar las actividades relacionadas con instalación/actualización/modificación de las aplicaciones, utilitarios y servicios de TIC relacionados con el software de base u operativo.
- Asegurar las configuraciones requeridas para reducir las vulnerabilidades inherentes al software de básico y software operativo teniendo en cuenta los diferentes mecanismos de seguridad tales como: Plantillas de aseguramiento, contraseñas robustas, actualización del firmware a la última versión, programas de seguridad requeridos, entre otros.
- Activar el servicio de auditoría en los sistemas de información para tener un registro de las actividades relacionadas con la instalación/configuración/actualización/mantenimiento del software y de los eventos que se producen en el sistema.

5.18 Política de Gestión de Vulnerabilidades

Declaración de Política: En la CGR, la adecuada gestión de la seguridad de la información es de enorme importancia. Por lo tanto, la Entidad gestiona las vulnerabilidades técnicas a las que puedan estar expuestos los activos de la CGR, de modo que las cuales puedan ser abordadas en todo su ciclo de vida, implementando las opciones de tratamiento necesarias, de modo que se prevenga la materialización de los riesgos asociados a las mismas.

Enunciado: En la CGR, la información constituye uno de los activos esenciales para la operación, prestación de servicios y generación de productos enmarcados dentro de los procesos estratégicos, misionales y de apoyo; por ello, establece su compromiso de realizar una debida gestión de vulnerabilidades que incluya la detección y solución de las fallas o debilidades a las que están expuestos los activos institucionales, incluyendo los de información. Para tal fin, la CGR debe:

- Establecer estrategias de seguridad que permitan tomar acciones ante las vulnerabilidades que puedan afectar la información.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del Riesgo, Seguridad y Continuidad del Negocio		Proceso: Gestión Integral de Seguridad	
	Políticas de Seguridad de Personas, Bienes e Información			
	Código: RSC-02-PO-003	Versión: 1.0	Fecha de Publicación en el Aplicativo: 23/08/2022	Página 22 de 32


- Detectar, reportar, valorar y gestionar las vulnerabilidades técnicas de los activos de información, a fin de evitar el compromiso de la confidencialidad, disponibilidad e integridad de la información en la Entidad.
- Definir e implementar planes de remediación para la solución de las vulnerabilidades de acuerdo con las estrategias que se definan.
- Hacer seguimiento a los planes de remediación y medidas de control correspondientes de las vulnerabilidades reportada enfocados en la mitigación de los riesgos asociados a las mismas.
- Disponer de los recursos humanos, tecnológicos y de información necesarios para apoyar la gestión de vulnerabilidades en cada una de sus fases.
- Incluir, en la gestión de las vulnerabilidades, la revisión regular de los registros relacionados con las actividades ejecutadas por los servidores públicos a cargo de su manejo.
- Gestionar lo necesario para que los proveedores de infraestructura tecnológica certifiquen que los equipos y servicios de TI suministrados y prestados a la CGR se encuentran libres de códigos maliciosos y vulnerabilidades técnicas, realizando los monitoreos y análisis periódicos necesarios para ello.
- Realizar anualmente, como mínimo, una (1) prueba de hacking ético a la infraestructura y sistemas de información de la CGR, por parte de personal competente y calificado. Los resultados de estas pruebas deben ser consideradas dentro de la planeación de remediación, en coherencia con la criticidad y nivel de exposición de las vulnerabilidades encontradas.

5.19 Política de Gestión de Seguridad de las Redes

Declaración de Política: La CGR, en aras de preservar la confidencialidad, integridad y disponibilidad de la información, establece su compromiso de definir e implementar los controles necesarios tanto lógicos como físicos para asegurar las redes y los servicios asociados con la transferencia y transmisión de información.

Enunciado: En la CGR, la información y los activos de información constituyen un activo esencial para la operación, prestación de servicios y generación de productos enmarcados dentro de los procesos institucionales, por lo que es necesario definir y aplicar controles para asegurar las redes y la información que se transmite a través de las mismas. Para tal fin, la CGR debe.

- Definir y aplicar los controles de seguridad necesarios para salvaguardar la confidencialidad e integridad de los datos que se transfieren y se transmiten a través de la red de datos de la Entidad y los sistemas asociados.
- Definir y aplicar los procedimientos de seguridad necesarios en la administración de los equipos de redes y comunicaciones, sea en forma local o remota.
- Registrar todas las actividades de operación, mantenimiento y actualización de las redes de la Entidad y sus equipos para efectos de seguimiento y auditoría a los controles de seguridad que se establezcan.
- Monitorear y registrar la actividad que se realiza a través de las redes para filtrar y controlar el contenido mediante los diferentes mecanismos de seguridad, particularmente a lo referido con el control de acceso, protección contra códigos maliciosos, controles criptográficos entre otros.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del Riesgo, Seguridad y Continuidad del Negocio		Proceso: Gestión Integral de Seguridad	
	Políticas de Seguridad de Personas, Bienes e Información			
	Código: RSC-02-PO-003	Versión: 1.0	Fecha de Publicación en el Aplicativo: 23/08/2022	Página 23 de 32


- Controlar la conexión de equipos a la red corporativa que no sean de propiedad de la Entidad.
- Evitar realizar conexiones remotas o utilizar paquetes, programas o protocolos inseguros para la transferencia de información, utilizando la infraestructura de red de la Entidad a menos que sea expresamente autorizado.
- Establecer los requisitos de seguridad de los recursos y servicios de red mediante el uso de listas de control de acceso y la segmentación de la red.
- Establecer los niveles de servicio y requisitos para los servicios de red que se presten interna o externamente y gestionar lo necesario para su cumplimiento.
- Definir y aplicar las directrices de seguridad distribuidas desde el directorio activo y desde las herramientas de gestión y monitoreo de infraestructura y sistemas de información de la Entidad.

5.20 Política de Uso de Internet

Declaración de Política: La CGR, en aras de preservar la confidencialidad, integridad y disponibilidad de la información, establece su compromiso de definir e implementar los controles necesarios para el acceso y uso del servicio de internet utilizado en el cumplimiento de las actividades misionales y de soporte requeridos en la Entidad.

Enunciado: En la CGR, la información y los activos de información constituyen activos esenciales para la operación, prestación de servicios y generación de productos enmarcados dentro de los procesos institucionales, por lo que es necesario definir y aplicar controles que mitiguen los riesgos en el acceso y el uso del servicio de internet. Con la utilización del servicio de internet la CGR busca incentivar la innovación y generación de conocimiento. Para tal fin, la CGR debe:

- Regular el acceso a páginas web y demás servicios que están disponibles en los sitios de internet, a través de la definición de perfiles de navegación.
- Asegurar la disponibilidad y continuidad del servicio bloqueando cualquier tráfico que comprometa el rendimiento de la red de la Entidad.
- Informar a los servidores públicos que el manejo de la información enviada o descargada de internet por medio de la red institucional, solo será para el cumplimiento de las labores propias de la Entidad.
- Realizar monitoreo al tráfico de información que se recibe desde internet para evitar la descarga e instalación de software no licenciado y malware en la infraestructura tecnológica de la CGR.
- Supervisar la navegación y uso del servicio de internet mediante el acceso a los informes y estadísticas de navegación, para controlar aquellos contenidos que no estén relacionados directamente con el quehacer institucional.
- Utilizar el servicio de auditoría del sistema para tener un registro de las actividades relacionadas con la navegación y uso de internet.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del Riesgo, Seguridad y Continuidad del Negocio		Proceso: Gestión Integral de Seguridad	
	Políticas de Seguridad de Personas, Bienes e Información			
	Código: RSC-02-PO-003	Versión: 1.0	Fecha de Publicación en el Aplicativo: 23/08/2022	Página 24 de 32

5.21 Política de Transferencia y Transmisión de Información

Declaración de Política: La CGR, en aras de preservar la seguridad de la información en la Entidad, establece su compromiso de definir e implementar los controles relacionados con la seguridad para la transferencia y transmisión de información tanto al interior de la CGR como la realizada con los grupos de interés o partes interesadas.

Enunciado: En la CGR, se hace necesario el uso de recursos que permitan que la transferencia y transmisión de la información se efectúe de manera controlada y segura. Para tal fin, la CGR debe:


- Establecer acuerdos para la transferencia o transmisión de la información, que registren claramente las responsabilidades y obligaciones adquiridas por las partes respecto de su posesión, acceso y uso, en razón del cumplimiento de los objetivos estratégicos, misionales y de apoyo.
- Establecer controles en la transferencia y transmisión de información, para la detección y protección contra software malicioso.
- Establecer los controles para proteger la disponibilidad, integridad y confidencialidad de la información transferida o transmitida.
- Proteger la propiedad intelectual y patrimonial de la información transferida o transmitida, conforme a la legislación colombiana.
- Establecer controles para proteger la información, de acuerdo con los niveles de clasificación definidos por la CGR.
- Definir acuerdos de confidencialidad con las partes interesadas, cuando sea pertinente.
- Establecer controles para proteger los canales de comunicación y la información transferida o transmitida contra la afectación de su confidencialidad, disponibilidad e integridad.
- Para la transmisión o transferencia de información que involucre datos personales, seguir además las reglas establecidas por la legislación vigente y la jurisprudencia, así como lo estipulado en la política de tratamiento de datos personales de la Entidad.

5.22 Política de Seguridad de Correo Electrónico

Declaración: La CGR, en aras de preservar la seguridad en el uso del correo electrónico institucional asignado a los servidores públicos y contratistas de prestación de servicios, proveedores y terceros que considere pertinentes, establece su uso exclusivo para el desarrollo de las funciones propias de la Entidad.

Enunciado: En la CGR, se hace necesario el uso seguro del servicio de correo electrónico institucional y establecer un medio de comunicación oficial para gestionar el intercambio de información con los grupos de interés o partes interesadas. Para tal fin, la CGR debe:

- Promover el compromiso hacia un comportamiento ético y ser consecuente con todas las políticas y procedimientos institucionales que apliquen para comunicaciones oficiales.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del Riesgo, Seguridad y Continuidad del Negocio		Proceso: Gestión Integral de Seguridad	
	Políticas de Seguridad de Personas, Bienes e Información			
	Código: RSC-02-PO-003	Versión: 1.0	Fecha de Publicación en el Aplicativo: 23/08/2022	Página 25 de 32


- Aplicar las buenas prácticas de seguridad para el servicio de correos electrónicos y los mecanismos de autenticación autorizados por la CGR.
- Establecer seguimientos y controles para el servicio y uso del correo electrónico institucional.
- Incluir en todo mensaje de correo saliente una nota de legalidad que identifique claramente la propiedad de la información y otros aspectos de tipo legal.
- Establecer controles para que las comunicaciones oficiales y almacenamiento de correo electrónico de la CGR, únicamente se realicen a través de los canales oficiales permitidos por la Entidad.

5.23 Política de Adquisición, Desarrollo y Mantenimiento de Sistemas

Declaración de Política: La CGR, en aras de preservar la confidencialidad, integridad y disponibilidad de la información, establece su compromiso de definir e implementar los controles para asegurar que los servicios, software, aplicaciones y sistemas de información adquiridos externamente o desarrollados internamente cumplan con los requisitos de seguridad mínimos durante todo el ciclo de vida del software, aplicaciones y sistemas de información.

Enunciado: En la CGR, la información y los activos de información constituyen activos esenciales para la operación, prestación de servicios y generación de productos enmarcados dentro de los procesos institucionales, por lo que es necesario considerar la seguridad de la información como una parte integral de la adquisición, desarrollo y mantenimiento de sistemas de información, servicios o aplicaciones requerido por la Entidad. Por tanto, en cada fase del ciclo de vida se deben definir, diseñar, construir e implementar los requisitos de seguridad. Para tal fin, la CGR debe:

- Establecer una fase de requisitos (levantamiento, especificación, validación y modelamiento) que se realizará a partir de las necesidades de las dependencias y deberá incluir los requisitos correspondientes de la seguridad de la información.
- Definir un responsable para la adquisición, desarrollo y mantenimiento de cada uno de los sistemas de información que soportan las actividades misionales de la Entidad.
- Emplear metodologías para el desarrollo de software considerando los requisitos de seguridad y buenas prácticas de desarrollo seguro, con el fin de proporcionar a los desarrolladores un marco de referencia que permita asegurar los sistemas de información durante todo el ciclo de desarrollo.
- Incluir de forma detallada todos los roles (grupos, privilegios, autorizaciones) y los derechos de acceso usados en la aplicación, servicios o sistema de información que se desarrolle.
- Tramitar, mediante la gestión de cambios implementado en la CGR, una revisión pos implementación para asegurar que el cambio no tenga un impacto adverso en la operación o seguridad de la Entidad.
- Implementar un registro de versionamiento para que los responsables de los sistemas de información administren los cambios realizados en los mismos.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del Riesgo, Seguridad y Continuidad del Negocio		Proceso: Gestión Integral de Seguridad	
	Políticas de Seguridad de Personas, Bienes e Información			
	Código: RSC-02-PO-003	Versión: 1.0	Fecha de Publicación en el Aplicativo: 23/08/2022	Página 26 de 32

- Identificar, establecer, valorar y documentar los posibles riesgos de seguridad de la información que se puedan derivar de la adquisición o desarrollo considerando los requerimientos de seguridad necesarios para la entrada a producción del desarrollo.

5.24 Política de Desarrollo Seguro


Declaración de Política: La CGR, en aras de preservar la confidencialidad, integridad y disponibilidad de la información, establece su compromiso de definir e implementar los controles para la definición y aplicación de estándares y buenas prácticas existentes para el desarrollo seguro de software, aplicaciones y sistemas de información adquiridos externamente o desarrollados internamente.

Enunciado: En la CGR, la información y los activos de información constituyen activos esenciales para la operación, prestación de servicios y generación de productos enmarcados dentro de los procesos institucionales, por lo que es necesario que la seguridad de la información sea considerada dentro de todo el ciclo de vida de desarrollo de los sistemas de información, por lo tanto, el desarrollo seguro es un requisito para crear cualquier servicio, sistema de información, aplicación o base de datos. Para tal fin, la CGR debe:

- Identificar, valorar y documentar los posibles riesgos que contenga el desarrollo de un sistema de información, servicio o aplicación.
- Exigir la suscripción de acuerdos de confidencialidad y certificar la ejecución de análisis de seguridad del personal que se encuentre vinculado a proyectos de desarrollo de software en la Entidad.
- Emplear tecnologías y mecanismos seguros para el desarrollo de los sistemas de información.
- Establecer condiciones para la transferencia de los derechos de propiedad intelectual de código fuente, de acuerdo con la normatividad vigente.
- Separar los ambientes de desarrollo, pruebas, producción de tal forma que el desempeño y la seguridad de un ambiente no influya en los demás.
- Verificar el buen funcionamiento del software y el respectivo ciclo de vida mediante un control de versiones debidamente documentado.
- Delimitar el acceso solo a las actividades exclusivas del ambiente de trabajo, mediante la aplicación de perfiles definidos para cada ambiente (desarrollo, pruebas y producción)
- Incorporar dentro del plan institucional de capacitación temas sobre desarrollo de software seguro dirigido a los desarrolladores de sistemas de información de la Entidad.

5.25 Política de Datos de Prueba

Declaración de Política: La CGR, en aras de preservar la confidencialidad, integridad y disponibilidad de la información, establece su compromiso de definir e implementar los controles para asegurar la protección de los datos usados en las pruebas que se deben practicar a todo servicio tecnológico, sistema de información, aplicación o base de datos.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del Riesgo, Seguridad y Continuidad del Negocio		Proceso: Gestión Integral de Seguridad	
	Políticas de Seguridad de Personas, Bienes e Información			
	Código: RSC-02-PO-003	Versión: 1.0	Fecha de Publicación en el Aplicativo: 23/08/2022	Página 27 de 32

Enunciado: En la CGR, la información y los activos de información constituyen activos esenciales para la operación, prestación de servicios y generación de productos enmarcados dentro de los procesos institucionales, por lo que es necesario definir qué tipo de datos o información es requerida para las pruebas operativas. Para tal fin, la CGR debe:


- Realizar el plan de pruebas de acuerdo con los requerimientos funcionales de los servicios, sistemas de información, aplicaciones o bases de datos; para verificar su funcionalidad.
- Analizar los requisitos funcionales a nivel seguridad antes del paso a producción, teniendo en cuenta la actividad de marcha atrás (*rollback*) en caso de presentar algún fallo, las técnicas de ofuscamiento de información, enmascaramiento, limpieza de datos entre otros.
- Seleccionar, proteger y controlar los datos de pruebas de los sistemas de información, servicios, aplicaciones o software, evitando la exposición de datos sensibles o reservados.
- Realizar control y seguimiento para la adecuada gestión de los datos de prueba.

5.26 Política de Gestión de Relaciones con los Proveedores

Declaración de Política: La CGR, en aras de preservar la confidencialidad, integridad y disponibilidad de la información, establece su compromiso de definir e implementar los controles que regulan la relación con los proveedores de la Entidad incluyendo los requisitos de seguridad de la información durante el ciclo de vida de la provisión de servicios por parte de los proveedores.

Enunciado: La información constituye un activo esencial de la CGR, razón por la cual la Entidad ha incluido dentro de su estrategia de adquisición de productos y contratación de servicios los requisitos de seguridad de la información para llevar a cabo la gestión de los servicios, disminuyendo el impacto que pueda tener la materialización de los riesgos en los activos de información. Para tal fin, la CGR debe:

- Dar a conocer y exigir el cumplimiento de las políticas de seguridad de la información a los proveedores.
- Identificar los requisitos de seguridad de la información los cuales deben mantenerse actualizados y disponibles a efectos de ser considerados en los procesos de contratación de productos y servicios de TIC con los proveedores de la Entidad.
- Integrar las condiciones de seguridad entre ellas los Acuerdos de Confidencialidad y Acuerdos de Nivel de Servicio – ANS en los contratos, acuerdos o convenios con los proveedores, atendiendo las políticas de seguridad de la información establecidas por la Contraloría General de la República.
- Realizar seguimiento con fines de auditoría a las actividades, controles y prácticas que el proveedor aplica, en cumplimiento de los términos contractuales y de los requisitos de seguridad de la información establecidos.
- Identificar los riesgos de gestión de proveedores para disminuir el impacto de la materialización de los riesgos que puedan afectar los activos de información.
- Requerir a los proveedores tecnológicos a cargo de labores de soporte técnico de equipos y sistemas informáticos para que mantengan estos equipos libres de código malicioso y vulnerabilidades técnicas, y realicen revisiones

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del Riesgo, Seguridad y Continuidad del Negocio		Proceso: Gestión Integral de Seguridad	
	Políticas de Seguridad de Personas, Bienes e Información			
	Código: RSC-02-PO-003	Versión: 1.0	Fecha de Publicación en el Aplicativo: 23/08/2022	Página 28 de 32

frecuentes de vulnerabilidades junto a la gestión y respuesta oportuna de remediación según la criticidad de los hallazgos. Las acciones realizadas deben ser registradas y estar a disposición de la CGR.


- Verificar que, dentro de las obligaciones contractuales de los proveedores de servicios de computación en la nube, se incluya el cumplimiento de las políticas y requisitos de seguridad de la información de la CGR los acuerdos de niveles de servicio, responsabilidades legales y derechos de propiedad intelectual sobre la información, así como las leyes y regulaciones sobre la protección de datos personales.
- Verificar que los proveedores de servicios en la nube almacenen la información personal o sensible en países que estén identificados como viables por la Superintendencia de Industria y Comercio en materia de protección de datos personales. Así mismo, asegurar que se cumpla con los mínimos requeridos por la legislación nacional vigente aplicable y la Política de Tratamiento de Datos Personales de la CGR.
- Validar que los proveedores de servicios en la nube apliquen políticas y prácticas robustas de seguridad, tanto al interior de sus procesos como en la infraestructura y plataforma tecnológica sobre la cuál prestan sus servicios.

5.27 Política de Gestión de Incidentes

Declaración de Política: La CGR, en aras de preservar la seguridad de las personas, los bienes y la información establece su compromiso de gestionar los incidentes de seguridad, incluida la comunicación sobre ellos, a partir de la definición de los lineamientos para responder eficazmente ante esta situación, teniendo en cuenta las etapas de detección, la recolección de evidencia, la evaluación, la respuesta, el reporte, el cierre y aprendizaje de los incidentes de seguridad de las personas, los bienes y la información.

Enunciado: En la CGR, la gestión de incidentes de seguridad tiene en cuenta a las personas, los bienes y la información, aspectos que son pilares esenciales para la prestación de los servicios y el desarrollo de sus actividades estratégicas, misionales y de apoyo, además de todas las situaciones que afecten la confidencialidad, integridad y disponibilidad de la información, bienes y servicios creando una cultura de prevención en cuanto a la ocurrencia de incidentes de seguridad, teniendo como referencia la gestión del conocimiento. Por lo cual, la CGR debe:

- Establecer procedimientos para la gestión de incidentes de seguridad de las personas, los bienes y la información los cuales deben considerar la planificación y preparación; la detección y reporte; la evaluación y decisión; la respuesta y las actividades pos incidentes para mitigar su impacto.
- Establecer los canales y procedimientos para que los grupos de interés o partes interesadas informen cualquier situación relacionada con la seguridad de las personas, los bienes y la información para que sea gestionada por la USATI, quien tiene como objetivo mantener contacto con las autoridades pertinentes, y atender sus recomendaciones al interior de la CGR o las recibidas de autoridades competentes.
- Definir la línea base de recursos para la gestión de incidentes de seguridad a cargo de la mesa técnica de seguridad, los responsables de los procesos deben tener en cuenta estas políticas de seguridad, para poder prevenir e identificar los posibles incidentes de seguridad de las personas, bienes e información.
- Promover y realizar acuerdos o convenios con terceras partes nacionales e internacionales con el objetivo de fortalecer la gestión de incidentes de seguridad de las personas, los bienes e información.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del Riesgo, Seguridad y Continuidad del Negocio		Proceso: Gestión Integral de Seguridad	
	Políticas de Seguridad de Personas, Bienes e Información			
	Código: RSC-02-PO-003	Versión: 1.0	Fecha de Publicación en el Aplicativo: 23/08/2022	Página 29 de 32


- Ejecutar las directrices impartidas por el Comité de Seguridad frente a los eventos e incidentes de seguridad, en los casos que por su importancia ameriten el pronunciamiento de esa instancia.

5.28 Política de Gestión de Continuidad del Negocio

Declaración de Política: La CGR, en aras de ser una Entidad resiliente ante situaciones que afecten la continuidad del negocio, entendiendo por tales aquellas que comprometan la seguridad de las personas, bienes e información; originadas por crisis, interrupciones, desastres o la ocurrencia de cualquier suceso que interrumpa la prestación de los servicios o que ponga en riesgo el cumplimiento de las funciones de la CGR establece su compromiso de definir e incluir los requisitos y controles de seguridad en la estrategia y gestión de la continuidad del negocio en la Entidad, así como su planeación e implementación.

Enunciado: En la CGR, la continuidad del negocio está basada en personas, bienes e información, los cuales son pilares esenciales para la prestación de los servicios y el desarrollo de sus actividades estratégicas, misionales y de apoyo. Por lo tanto, para la gestión de la continuidad de negocio, la CGR debe:

- Declarar el compromiso por parte de la alta Dirección, Líderes de los macroprocesos, Líderes de los procesos y demás directivos del nivel central y desconcentrado con el cumplimiento de los requisitos aplicables en materia de continuidad del negocio, tales como la identificación de recursos mínimos para mantener su operación, la aplicación y actualización del análisis de impacto al negocio y riesgos de continuidad, para ser considerados en las estrategias e implementación de planes de respuesta.
- Estipular un marco de gobierno y objetivos de la gestión de la continuidad del negocio, considerando la planeación, implementación, operación, seguimiento y mejora continua.
- Ejecutar las actividades establecidas para la planeación, implementación y respuesta de continuidad de negocio por la CGR.
- Articular los planes de respuesta a incidentes, plan de recuperación de desastres, planes de continuidad y plan de gestión de crisis por parte de la alta Dirección de la CGR.
- Definir los lineamientos, por parte de la USATI, para que los Líderes de los macroprocesos, Líderes de los procesos y demás directivos del nivel central y desconcentrado implementen y operen las estrategias y planes de continuidad correspondientes.
- Actualizar, de manera periódica (o cuando la condición lo amerite), los planes de: continuidad del negocio, de recuperación de desastres, de emergencia y de gestión de crisis a cargo de los líderes de macroproceso, procesos y directivos.
- Planear y ejecutar de manera periódica las pruebas de los planes de continuidad de negocio, recuperación de desastres, emergencias y crisis que tengan a cargo los Líderes de los macroprocesos, procesos y directivos.
- Participar activamente en las pruebas que la CGR programe para aquellos servidores públicos y contratistas de prestación de servicios, proveedores y terceros que integren los equipos de respuesta definidos en los diferentes planes.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del Riesgo, Seguridad y Continuidad del Negocio		Proceso: Gestión Integral de Seguridad	
	Políticas de Seguridad de Personas, Bienes e Información			
	Código: RSC-02-PO-003	Versión: 1.0	Fecha de Publicación en el Aplicativo: 23/08/2022	Página 30 de 32

- Generar conciencia y cultura en los servidores públicos y contratistas de prestación de servicios, proveedores y terceros sobre la importancia de la Continuidad del Negocio.

5.29 Política de Cumplimiento de Requisitos Legales y Contractuales


Declaración de Política: La CGR, en aras de preservar la confidencialidad, integridad y disponibilidad de la información, establece su compromiso de definir e implementar los controles para el cumplimiento de las obligaciones legales, reglamentarias y contractuales pertinentes a cualquier requisito de seguridad de personas, bienes e información.

Enunciado: En la CGR, la información y los activos de información constituyen un activo esencial para la operación, prestación de servicios y generación de productos enmarcados dentro de los procesos institucionales, por lo que es necesario identificar, documentar, aplicar y mantener actualizadas todas las obligaciones legales, reglamentarias y contractuales relacionadas con los controles para la seguridad de personas, bienes e información. Para tal fin, la CGR debe:

- Identificar, revisar, documentar y mantener actualizadas todas las obligaciones reglamentarias, legales y contractuales relacionadas con los requisitos de seguridad de personas, bienes e información.
- Verificar el cumplimiento de las legislaciones relacionadas con la protección de los derechos de propiedad intelectual, uso y licenciamiento de software, transferencia de información y control del software operacional, tratamiento de datos personales entre otras.
- Validar que todo el software (operacional, de base, bases de datos) y código fuente de sistemas de información provistos por terceros que se encuentre instalado y/o se ejecute en la plataforma tecnológica de la CGR esté protegido por derechos de autor y disponga de las respectivas licencias de uso o en su defecto sea software de libre distribución y uso.
- Proteger los registros y documentos que constituyan evidencia y/o reflejan las actividades de la operación de la CGR de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de la Entidad.
- Verificar el cumplimiento de la legislación vigente para el tratamiento de datos personales, asegurando la protección y privacidad de la información y de los datos personales que hayan sido administrados, almacenados, procesados o distribuidos por la Entidad.
- Revisar de manera periódica el cumplimiento de las políticas de seguridad, procedimientos y demás reglamentos adoptados por la Entidad.
- Prevenir sanciones disciplinarias, civiles y/o penales por el uso de software ilegal, productos no licenciados o no autorizados.

5.30 Política para Uso y Licenciamiento de Software

Declaración de Política: La CGR, en aras de preservar la confidencialidad, integridad y disponibilidad de la información, establece su compromiso de definir e implementar los controles para la adquisición, uso y mantenimiento de software legalmente obtenido para el desarrollo de los objetivos misionales y de apoyo de la Entidad.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del Riesgo, Seguridad y Continuidad del Negocio		Proceso: Gestión Integral de Seguridad	
	Políticas de Seguridad de Personas, Bienes e Información			
	Código: RSC-02-PO-003	Versión: 1.0	Fecha de Publicación en el Aplicativo: 23/08/2022	Página 31 de 32

Enunciado: En la CGR, los activos de información y la información constituyen un activo esencial para la operación, prestación de servicios y generación de productos enmarcados dentro de los procesos institucionales, por lo que es necesario controlar el uso de software autorizado y licenciado por la Entidad. Por lo cual, la CGR debe:

- Utilizar el software debidamente autorizado y licenciado en los equipos de la Entidad, cualquier software que no cuente con su debida licencia o no cumpla con las especificaciones o condiciones legales para ser utilizado deberá ser desinstalado o desactivado.
- Controlar el uso de copias de software licenciado por la CGR en computadores o dispositivos que no pertenezcan a la Entidad.
- Cumplir con los Acuerdos internacionales y la legislación nacional vigente sobre los derechos de autor a la cual está sujeto todo software instalado y utilizado en los equipos de propiedad de la Entidad.
- Utilizar listas blancas para controlar el software autorizado e instalado en los equipos de la Entidad.
- Utilizar las herramientas tecnológicas de información y comunicación adoptadas al interior de la Entidad como son: mensajería instantánea, ofimática, trabajo colaborativo, almacenamiento en nube, entre otras.


6. Normatividad y documentos de referencia

La normatividad y los documentos bajo los cuales se soporta la aplicación de las presentes Políticas de Seguridad se indican a continuación:

- Decreto No. 1078 de 2015 *“Por medio del cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones”*.

Adicionalmente, se tienen como referencia las guías, lineamientos y documentos emitidos para la implementación de la estrategia de Gobierno Digital, además del conjunto de normas técnicas que rigen la implementación de Sistemas de Gestión de Seguridad.

- ISO/IEC 27001-2013. Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos.
- ISO/IEC 27002-2015. Tecnologías de la Información. Técnicas de Seguridad. Código de práctica para controles de seguridad de la información.
- ISO/IEC 13335-2004. Tecnologías de la Información. Técnicas de Seguridad. Gestión de Información y seguridad de las tecnologías de las comunicaciones.
- Decreto 1008 del 14 junio de 2018. Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
- Artículo 10 de la Ley 1753 de 2015. Derecho de Propiedad Intelectual.
- Resolución Organizacional OGZ-0531-2016. *“Por la cual se crea el Sistema de Gestión de Seguridad, se crea el comité de seguridad de la Contraloría General de la República, política general de seguridad, la política de*

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del Riesgo, Seguridad y Continuidad del Negocio		Proceso: Gestión Integral de Seguridad	
	Políticas de Seguridad de Personas, Bienes e Información			
	Código: RSC-02-PO-003	Versión: 1.0	Fecha de Publicación en el Aplicativo: 23/08/2022	Página 32 de 32

seguridad y privacidad de la información, la política de tratamiento de datos personales y se dictan otras disposiciones”

- Resolución Organizacional OGZ–0593-2017. “Por la cual se modifica la Resolución Organizacional OGZ-0531-2016”.
- Resolución Organizacional OGZ–0758-2020. “Por la cual se crea el Programa de Protección y Seguridad del Contralor General de la República, los excontralores generales de la República y demás servidores de la Contraloría General de la República; se adoptan lineamientos técnicos para el programa y se modifica la conformación y funciones del Comité de Seguridad”.
- Ley 1450 de 2011, Racionalización de Trámites.
- Decreto 2573 de 2014, Privacidad y Seguridad de la Información.

Para mayor información sobre los procedimientos y documentos asociados a los macro procesos de la CGR correspondientes al SGS, los términos se podrán consultar en el link de la intranet en el SIGECI <https://prorrogasireci.contraloria.gov.co/CDISC/Entorno/MaestroGeneral> Vigencia, derogatorias y transición

7. Vigencia

Este documento tiene vigencia a partir de la fecha de la comunicación a todos los servidores públicos y contratistas de prestación de servicios de la CGR sobre su publicación en el Aplicativo SIGECI, por parte de la Oficina de Planeación.

Elaborado por el (los) servidor(es)	Presentado por el Directivo:	Aprobador por:	Validado en el contexto del SIGECI por (Servidor(es) del GTSIGECI)	Validación en el contexto del SIGECI revisada por (Líder del GTSIGECI)	Validación en el contexto del SIGECI aprobada por (Administrador del SIGECI)
Jairo Hernán Barragán Gómez, Unidad de Seguridad y Aseguramiento Tecnológico Informático – USATI. Diana Patricia Murillo Calderón, Unidad de Seguridad y Aseguramiento Tecnológico Informático – USATI.	José Antonio Poveda Montes, Jefe de Unidad de Seguridad y Aseguramiento Tecnológico e Informático – USATI.	Líder de Proceso Gestión Integral de Seguridad: Margarita María Márquez Figueroa, Directora de la Unidad de Seguridad y Aseguramiento Tecnológico e Informático – USATI. Líder del Macroproceso de Gestión de Riesgo, Seguridad y Continuidad del Negocio: José Antonio Poveda Montes, Jefe de Unidad de Seguridad y Aseguramiento Tecnológico e Informático – USATI y Vanessa Varón Garrido, Directora Oficina de Planeación.	Paola Tatiana Tovar, Contratista de la Oficina de Planeación. Yahaira Karina González, Profesional de la Oficina de Planeación.	José Nehemán Gómez Lozada, Asesor de Gestión de la Oficina de Planeación.	Vanessa Varón Garrido, Directora Oficina de Planeación.