
	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 1 de 71

TABLA DE CONTENIDO

1.	Introducción	4
2.	Objetivos	5
3.	Campo de aplicación	5
4.	Principios de seguridad de la información en los Procesos de Gestión de información y Análisis de información en la DIARI.....	5
5.	Glosario y siglas.....	6
6.	Marco Normativo.....	11
7.	Lineamientos generales y políticas operativas de seguridad de la información en la operación de los procesos Gestión de información y Análisis de información en la DIARI.	11
7.1	Política Operativa General de Seguridad en la operación de los procesos Gestión de información y Análisis de información en la DIARI.....	12
7.2	Política Operativa de la organización de la seguridad de la información.....	13
7.3	Políticas Operativas de Seguridad del Recurso Humano	15
7.4	Política Operativa de seguridad de Control de Acceso.....	16
7.4.1	Mecanismos de seguridad para controlar el acceso en recursos y servicios tecnológicos.....	18
7.4.1.1	Gestión de los Accesos de los Usuarios.....	19
7.4.1.1.1	Usuarios Privilegiados y/o Administradores.....	20
7.4.1.1.2	Perfiles de Auditoría	21
7.4.2	Gestión de contraseñas	21
7.4.3	Uso de información de autenticación secreta	25
7.5	Política Operativa de Gestión de Información y de Activos de Información.....	25
7.5.1	Inventario y Propiedad de Activos.....	25
7.5.2	Uso aceptable de Activos de Información.....	26
7.5.3	Clasificación de información	28
7.5.4	Tratamiento de la información.....	29
7.5.5	Destrucción de información.....	30
7.5.6	Uso de Internet	30
7.5.7	Carpetas compartidas.....	32
7.5.8	Uso de medios removibles.....	32

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 2 de 71

7.6 Política Operativa de Dispositivos Móviles de propiedad de funcionarios y contratistas de prestación de servicios
34

7.7 Política Operativa de Controles Criptográficos 35

7.7.1 Uso de Controles Criptográficos 36

7.7.2 Generación de HASH para datos estructurados y no estructurados 37

7.8 Política Operativa de Seguridad Física y del Entorno 38

7.8.1 Seguridad Física de Áreas de Acceso Restringido 38

7.8.2 Protección Contra Amenazas Externas y Ambientales 39

7.8.3 Seguridad de los Equipos 40

7.9 Política Operativa de Seguridad de las Operaciones 42

7.9.1 Procedimientos Operacionales y Responsabilidades 42

7.9.2 Control de Software Operacional y Contra Código Malicioso 45

7.9.3 Copias de Respaldo y Almacenamiento 46

7.9.4 Registro y Seguimiento 47

7.9.5 Gestión de las Vulnerabilidades Técnicas 49

7.10 Política Operativa de Seguridad de las Comunicaciones 50

7.10.1 Gestión de la Seguridad de las Redes 50

7.10.2 Transferencia de Información 52

7.10.3 Mensajería Electrónica 54

7.11 Política Operativa de Servicios de Computación en la Nube 56

7.12 Política Operativa de Adquisición, Desarrollo y Mantenimiento de Sistemas de Información 57

7.12.1 Responsabilidad y Propiedad de los Sistemas de Información y Desarrollos de Software 57

7.12.2 Análisis y Especificación de Requisitos de Seguridad de la Información 58

7.12.3 Separación de Ambientes 59

7.12.4 Datos de Prueba 59

7.12.5 Seguridad de las Aplicaciones en Redes Públicas 60


7.12.6 Desarrollo Seguro 60

7.13 Política Operativa de Gestión de Incidentes de Seguridad de la Información 62

7.14 Política Operativa de Relaciones con los Proveedores 63


7.15 Política Operativa de Aspectos de Seguridad de la Información de la Gestión de Continuidad de Negocio 64

7.16 Política Operativa de Cumplimiento 65

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 3 de 71

7.17 Política Operativa de Propiedad Intelectual	66
7.18 Política Operativa de Protección para BYOD	67
7.19 Política Operativa de Trabajo en Casa	69
8. Anexos, plantillas y formatos	71
9. Vigencia, derogatorias y transición	71

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 - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 4 de 71


1. Introducción

La Contraloría General de la República ejerce el control y vigilancia fiscal a los recursos públicos de forma oportuna, independiente y efectiva, garantizando la participación activa de la ciudadanía y la articulación regional, con base en el conocimiento y la tecnología, lo cual contribuye al desarrollo sostenible y al cumplimiento de los fines esenciales del Estado. El artículo 267 de la Constitución Política de Colombia, modificado por el artículo 1° del Acto Legislativo No. 04 de 2019, establece que “la vigilancia de la gestión fiscal del Estado incluye el seguimiento permanente al recurso público, sin oponibilidad de reserva legal para el acceso a la información por parte de los órganos de control fiscal”. En razón de ello, la Contraloría General de la República gestiona grandes volúmenes de información que deben ser soportados y gestionados a través del uso de las tecnologías de la información y la comunicación, siendo necesario promover la modernización y actualización de herramientas tecnológicas, para hacer más eficiente su labor de vigilancia sistemática y permanente sobre las diversas entidades del Estado y aquellos particulares que manejan recursos públicos que son sujetos de control de la CGR.

Para la gestión efectiva de la información y en el cumplimiento de su misión, la Contraloría General de la República es sometida a una transformación llevada a cabo mediante el Acto Legislativo No. 04 de 2019, que modificó los artículos 267, 268, 271, 272 y 274 de la Constitución Política. Además, se expidió el Decreto N°2037 de 2019 “por el cual se desarrolla la estructura de la Contraloría General de la República, se crea la Dirección de Información, Análisis y Reacción Inmediata”.

En su operación, la Dirección de Información, Análisis y Reacción Inmediata – DIARI realiza el uso eficiente de la tecnología en el ejercicio de vigilancia y control fiscal, siendo una de las principales instancias de apoyo al Sistema Nacional de Control Fiscal; para lo cual a través de la Unidad de Información realiza la conexión a miles de fuentes de datos e información de las diferentes entidades del país que manejan recursos públicos, lo que permite realizar una gestión que involucra la adquisición, acceso, almacenamiento, aseguramiento, calidad y posterior disposición de datos e información para la Unidad de Análisis de Información. Ésta, a través de las capacidades tecnológicas disponibles, tales como inteligencia artificial, analítica y minería de datos, análisis predictivo y prospectivo, entre otras; realiza el procesamiento y análisis de grandes volúmenes de datos e información de manera eficiente, segura y escalable para la determinación anticipada de eventos o malas prácticas, con probabilidad significativa de ocurrencia, persistencia o mutación, y que impliquen riesgos de pérdida del patrimonio público.

Por lo anterior, el macroproceso de Gestión de Información y Análisis de información -GIA está integrado por los procesos de Gestión de Información y Análisis de Información, cuya adecuada operación requiere un Gobierno de Seguridad de la Información basado en un estándar internacional (NTC-ISO-IEC-27001) que permita establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de los datos y la información que se gestiona, de tal manera que se pueda preservar su confidencialidad, integridad y disponibilidad, durante todo su ciclo de vida.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 5 de 71

2. Objetivos

Objetivo General:

Establecer las políticas operativas para la gestión de la seguridad de la información en los procesos Gestión de información y Análisis de información en la Dirección de Información, Análisis y Reacción Inmediata -DIARI-, que permitan preservar la confidencialidad integridad y disponibilidad de la información y de los activos que la gestionan, en ambientes On Premise y en la Nube.

Objetivos Específicos:

- Gestionar los riesgos de seguridad de la información con el fin de preservar la confidencialidad, integridad y disponibilidad de la información y los datos gestionados en la operación de los procesos Gestión de información y Análisis de información en la DIARI.
- Gestionar de manera oportuna los incidentes y eventos relevantes de seguridad de la información con el fin de mitigar los impactos derivados de una materialización del riesgo, en la operación del Proceso Gestión de información y Proceso de Gestión de Análisis de información en la DIARI.
- Desarrollar y fortalecer de forma continua una cultura de seguridad de la información con el fin de mitigar la materialización de incidentes de seguridad de la información derivados del comportamiento humano en la operación de los procesos Gestión de información y Análisis de información en la DIARI.


3. Campo de aplicación

Las políticas establecidas en este documento son de obligatoria aplicación por parte de los empleados públicos de planta (carrera administrativa, provisionales, funcionarios de libre nombramiento y remoción), trabajadores oficiales, contratistas de prestación de servicios, y demás personal, proveedores de servicios y terceros relacionados, que en la operación de los procesos Gestión de información y Análisis de información en la DIARI interactúen de cualquier manera con los datos, información y los activos de información en dicha dependencia.

4. Principios de seguridad de la información en los Procesos de Gestión de información y Análisis de información en la DIARI.

Los principios que fundamentan las políticas, procedimientos o instructivos asociados a la seguridad y privacidad de la información en los procesos Gestión de información y Análisis de información en la DIARI son:

- **Confidencialidad:** Propiedad que determina que la información solo sea accedida, conocida y/o divulgada por los usuarios autorizados.
- **Integridad:** Propiedad de salvaguardar la exactitud y completitud de la información, para que no surjan modificaciones de manera no autorizada durante su almacenamiento, transporte, custodia y procesamiento.
- **Disponibilidad:** Propiedad de que la información estará disponible para los usuarios autorizados cuando se requiera.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 6 de 71

5. Glosario y siglas

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

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.

Amenazas*: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

Amenaza informática: La aparición de una situación potencial donde un agente tiene la capacidad de generar un ataque cibernético contra la Entidad, población, el territorio y la organización política del estado.

Análisis de riesgo¹: Proceso para comprender la naturaleza del riesgo y para determinar el nivel de riesgo.

Anonimización del dato: Eliminar o sustituir algunos nombres de personas (naturales o jurídicas), direcciones y demás información de contacto, números identificativos, apodos o cargo.

Aplicación: Programa desarrollado mediante un lenguaje de programación orientado a facilitar la administración de información dentro de un proceso productivo o administrativo de una organización.

Autenticación*: Es el mecanismo de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.

Autenticidad: Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.


Backup: Copia de respaldo de los datos y archivos almacenados en un equipo de cómputo a un medio o ubicación secundaria.

Base de datos*: Es un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso.

BYOD: Término en inglés: Bring Your Own Device, Traducción: (Trae tu propio dispositivo). Acrónimo definido como la práctica en la que se alienta a los trabajadores al uso de los dispositivos que tienen en casa para acceder a los sistemas y datos empresariales.

Ciberseguridad*: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

¹ Término tomado de ISO/IEC 27000:2018

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 7 de 71

Ciberespacio: Se refiere a un entorno no físico creado por equipos de cómputo unidos mediante una red para interoperar entre sí.

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".

Clave (Llave) Criptográfica: Una clave, palabra clave o clave criptográfica es una pieza de información que controla la operación de un algoritmo de criptografía. Habitualmente, esta información es una secuencia de números o letras mediante la cual, en criptografía, se especifica la transformación del texto plano en texto cifrado, o viceversa.

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control también es utilizado como sinónimo de salvaguarda o contramedida, es una medida que modifica el riesgo.

Custodio: Ente natural o jurídico que supervisa, monitorea y vigila un objeto o actividad.

Datos Abiertos*: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6)


Datos biométricos: Son datos sensibles que permiten identificar a una persona natural a través del reconocimiento de una característica física e intransferible, que al ser única de cada individuo, permite distinguir a un ser humano de otro.

Datos Personales*: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

Datos personales sensibles*: Se entiende por datos sensibles aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)

Dato privado: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.

Dato público: Es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con presente ley. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 8 de 71

Dato semiprivado*: Es el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero, y crediticio de actividad comercial o de servicios a que se refiere el título IV de la ley 1266.

Directorio Activo (AD): Active Directory es un servicio de directorio desarrollado por Microsoft para redes de dominio de Windows. Usado para la administración centralizada de dominios locales.

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.

Dispositivo Móvil: Son equipos de fácil portabilidad con características de almacenamiento, procesamiento, conectividad a internet y que permiten el procesamiento de datos.

Evento de seguridad de la información: Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

Gestión de claves: Son controles que realizan mediante la gestión de claves criptográficas.

Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

Gestión de riesgos: Actividades coordinadas para dirigir controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.


Habeas data: Derecho a acceder a la información personal que se encuentre en archivos o bases de datos; implica la posibilidad de ser informado acerca de los datos registrados sobre sí mismo y la facultad de corregirlos.

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.

Información Pública*: Es toda información que ha sido declarada de acceso público, de acuerdo con las normas existentes por la persona o grupo de personas de la Entidad responsables del activo de información y que por lo tanto no tienen requerimientos de seguridad frente a la confidencialidad.

Impacto: El costo o consecuencia de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros - p.ej., pérdida de reputación, implicaciones legales, etc.

Incidente de seguridad*: Es cualquier evento que tenga o pueda tener como resultado la interrupción de los servicios suministrados por un sistema informático y/o posibles pérdidas físicas, de activos o financieras. Se considera que un incidente es la materialización de la amenaza.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 9 de 71

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

Inventario de activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

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.

No repudio²: Servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido).

Página web: Es un documento digital que permite albergar información de tipo texto, sonido, vídeo, gráfico, que se dispone en internet y es accesible mediante el protocolo http y https para su uso.

Parte interesada (Stakeholder): Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

Perfil de acceso: Mecanismo de seguridad mediante el cual se definen los permisos de acceso de usuario o grupo de usuarios a un recurso o sistema de información

Plataforma tecnológica: Conjunto de elementos tecnológicos de hardware, software y comunicaciones que se utilizan como base y están destinados al procesamiento de información con características específicas.


Proceso: Conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas.

Propietario del activo de información: Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con el proceso institucional se clasifican adecuadamente. Así mismo, debe controlar la gestión de la información, incluyendo la seguridad de la misma; igualmente debe definir y revisar periódicamente las restricciones y clasificaciones del acceso, así como gestionar los riesgos asociados a los activos de información, de acuerdo a su nivel de severidad.

Responsable de la información (activo de información): funcionario o unidad organizacional que tiene responsabilidad aprobada por el propietario de la información, para el control de la producción, el desarrollo, el mantenimiento, el uso y la seguridad de los activos de información.

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). / Efecto de la incertidumbre sobre los objetivos. (ISO 31000)

² Término tomado de norma ISO-7498-2.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 10 de 71

Responsable del tratamiento*: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la información y su tratamiento. (Ley 1581 de 2012, art 3).

Seguridad de la Información*: Es la propiedad que asegura que los recursos de un sistema de información sean utilizados de la manera correcta y que su acceso sólo sea posible a las personas que se encuentren autorizadas, preservando la Integridad, Confidencialidad y Disponibilidad de los activos de información

Sistema de gestión de seguridad SGS³: El Sistema de Gestión de Seguridad se puede definir como un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la Organización con el fin de lograr los objetivos de negocio. El SGS está conformado por políticas, normas, guías e instructivos que proporcionarán al usuario recursos y herramientas que propendan por la seguridad de nuestra Entidad. Se enfoca en tres aspectos: la seguridad de las personas (SGSP), la seguridad de la información (SGSI) y la seguridad de los bienes (SGSB).

Sitio web: Es un espacio virtual en la red que está conformado por varias páginas web relacionadas y con una temática definida, las cuales están guardadas en un hosting y se identifica con un nombre de dominio.

Terceros: Se entiende por tercero a toda persona, jurídica o natural, como proveedores, contratistas de prestación de servicios o consultores, que provean servicios o productos.

Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información, un recurso, un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.

Token: Es un dispositivo que brindan algunas entidades bancarias a sus usuarios para que por medio de éste puedan hacer uso de los Servicios electrónicos de manera segura y confiable.

Usuario: Será aquella persona que para ejercer una funcionalidad definida necesita acceder mediante un equipo de cómputo con un perfil y privilegios definidos a un sistema, un recurso o una plataforma para el normal desempeño de sus actividades y que le permita interactuar con los datos e información.


Vulnerabilidad⁴: Debilidad de un activo o control que pueda ser explotado por una o más amenazas

Nota: * Tomado del Glosario de términos comunes utilizados en la Unidad de Seguridad y Aseguramiento Tecnológico e Informático –USATI– Contraloría General de la República Colombia.

<https://clic-online.contraloria.gov.co/USATI/Documents/GLOSARIO%20SGS.pdf>

³ Resolución Organizacional OGZ-0531-2016 y Resolución Organizacional OGZ-0593-2017.

⁴ Término de la norma ISO 27000 de 2012.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 11 de 71

6. Marco Normativo

El marco normativo aplicable para el Sistema de Gestión de Seguridad SGS que incluye entre otros los procesos Gestión de información y Análisis de información en la DIARI, se incorpora y actualiza permanentemente a través de la matriz requisitos legales aplicables en el Sistema de Gestión de Seguridad SGS, cuya última versión se encuentra disponible y publicada en el Micrositio de la USATI en la Intranet. (ClickOnLine). La actualización de la misma será realizada por parte de la Unidad de Seguridad y Aseguramiento Tecnológico e Informático - USATI.

7. Lineamientos generales y políticas operativas de seguridad de la información en la operación de los procesos Gestión de información y Análisis de información en la DIARI.


Las políticas operativas de seguridad en la operación de los procesos Gestión de información y Análisis de información en la DIARI, se enmarcan en la política de seguridad de la CGR.

La Dirección de Información, Análisis y Reacción Inmediata DIARI es responsable de supervisar las medidas adoptadas, para garantizar la seguridad de la información al interior de la misma, así como de revisar, proponer y mantener, el texto de las Políticas operativas de seguridad de la información en la operación de los procesos Gestión de información y Análisis de información en la DIARI, las funciones generales, los manuales, los procedimientos, las guías y/o instructivos, las capacitaciones, las recomendaciones, las normas y los planes de seguimiento, etc., así mismo deberá proponer mejoras continuas al Sistema de Gestión de Seguridad en materia de Información.

Todo el personal de la DIARI es responsable de aplicar las directrices definidas por el Comité de Seguridad de la Información y la Mesa Técnica de Seguridad de la CGR, así como de participar activamente en procura de preservar la seguridad de la información al interior de la DIARI.

El incumplimiento de las políticas operativas de seguridad en la operación de los procesos Gestión de información y Análisis de información en la DIARI, tendrá como resultado la aplicación de sanciones, conforme a la magnitud y característica de la violación a la seguridad de la información y de acuerdo al Código General Disciplinario - CGD (Ley 1952 del 2019), a la legislación colombiana vigente y a todo acuerdo internacional que se relacione con la falta incurrida.

El líder de seguridad de la información de la DIARI debe revisar y actualizar anualmente el presente documento o si ocurren cambios significativos en la Dirección de Información Análisis y Reacción Inmediata DIARI o en la Entidad, que puedan influenciar en la dinámica del Sistema de Gestión de Seguridad sobre los procesos Gestión de información y Análisis de información.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 12 de 71

7.1 Política Operativa General de Seguridad en la operación de los procesos Gestión de información y Análisis de información en la DIARI

“La Dirección de Información, Análisis y Reacción Inmediata DIARI establece como compromiso preservar la confidencialidad, integridad y disponibilidad de los datos e información gestionados dentro de su operación, mediante un enfoque basado en riesgos, la adopción de estándares y mejores prácticas de la industria, la adopción de la estrategia de defensa en profundidad, el establecimiento de una cultura de seguridad de la información y el mantenimiento del proceso de mejora continua del Sistema de Gestión de Seguridad en materia de información.”

La DIARI ha establecido las siguientes Políticas Operativas de Seguridad de la Información, las cuales corresponden a las directrices generales de seguridad de la información en las que se abordan los siguientes temas:

- **Organización de la Seguridad de la Información:** ⁵ Orientada a suministrar las directrices para administrar la seguridad de la información, dentro de la DIARI y establecer un marco gerencial para controlar su implementación.
- **Seguridad del Recurso Humano:** Orientada a asegurar que los integrantes de la planta de personal y contratistas de prestación de servicios entiendan sus responsabilidades y obtengan las competencias para desempeñar su labor reduciendo los riesgos de seguridad asociados a los mismos.⁵
- **Control de Acceso:** Dirigida a establecer las directrices para el acceso autorizado a la data, información, sistemas, recursos y servicios.^{6 7 8 9 10 11}
- **Gestión de información y activos de información:** Destinado a mantener una adecuada protección de los activos de información de la DIARI.^{6 7 8 9 10}
- **Dispositivos Móviles:** Orientada a preservar la seguridad de la información tratada en los dispositivos móviles cuando se consulte, transfiera o almacene.
- **Uso de controles criptográficos:** Enfocado al establecimiento de directrices de cifrado dentro de las operaciones de acceso a sistemas, gestión de claves, transferencia de información en la DIARI con el fin de asegurar la confidencialidad e integridad de la información.¹⁰
- **Seguridad física y del entorno:** Orientada a evitar el acceso físico no autorizado, daño e interferencia de las instalaciones donde se almacena o reposa la data y la información.¹¹
- **Escritorio y pantalla limpia:** Orientado a minimizar los riesgos de acceso no autorizado, pérdida o daño de información almacenada en los puestos de trabajo, equipos de cómputo, medios extraíbles, dispositivos de impresión y digitalización de documentos.
- **Seguridad de las operaciones:** Dirigida a preservar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y medios de comunicación.^{7 8 9 10 11}

⁵ Defensa en profundidad capa de Gobierno

⁶ Defensa en profundidad capa de Perímetro.


⁷ Defensa en profundidad capa de Red Interna.

⁸ Defensa en profundidad capa de Host.

⁹ Defensa en profundidad capa de Aplicación.

¹⁰ Defensa en profundidad capa de Datos.

¹¹ Defensa en profundidad capa Física.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 13 de 71


- **Seguridad de las comunicaciones:** Asegurar la protección de las redes y los recursos empleados en el tratamiento de la data e información. ⁹
- **Adquisición, desarrollo y mantenimiento de los sistemas de información:** Orientado a incorporar directrices de seguridad dentro del ciclo de vida de los sistemas de información. ^{10 11}
- **Gestión de incidentes de seguridad de la Información:** Dirigido a establecer la guía para gestionar los incidentes de seguridad y los canales de comunicación. ⁶
- **Relación con proveedores:** Destinado a establecer las directrices para la protección de los activos de información accesibles por proveedores y aliados comerciales. ^{10 11 9 8 10 11}
- **Gestión de la Continuidad** Orientado a mitigar las interrupciones de las actividades críticas de los procesos esenciales. ⁶
- **Cumplimiento:** Destinado al cumplimiento de la normatividad aplicable en materia de seguridad de la información
- **Propiedad Intelectual:** Es un tipo de propiedad que implica el derecho de goce y disposición sobre las creaciones del talento o ingenio humano producidas por su creador.
- **Protección para (BYOD):** Medidas de seguridad necesarias para evitar que la información de la CGR se vea comprometida en su integridad y confidencialidad al ser almacenada en dispositivos ajenos a la entidad (BYOD - Trae tu propio dispositivo).
- **Trabajo en Casa:** Es la habilitación al servidor público o trabajador del sector privado para desempeñar transitoriamente sus funciones o actividades laborales por fuera del sitio donde habitualmente las realiza, sin modificar la naturaleza del contrato o relación laboral, o legal y reglamentaria respectiva, ni tampoco desmejorar las condiciones del contrato laboral, cuando se presenten circunstancias ocasionales, excepcionales o especiales que impidan que el trabajador pueda realizar sus funciones en su lugar de trabajo, privilegiando el uso de las tecnologías de la información y las comunicaciones.

7.2 Política Operativa de la organización de la seguridad de la información¹²

La DIARI establece, implementa, opera, revisa, mantiene y mejora el Sistema de Gestión de Seguridad en materia de información en los procesos de Gestión de información y Análisis de información, a través de la adopción de un marco de referencia basado en el estándar internacional ISO 27001:2013 que especifica los requisitos para la gestión dentro del contexto de la Dirección, así mismo se apoyará en la arquitectura de negocio definido para el gobierno de datos e información.

Se apoyará en la definición de políticas operativas para la seguridad de la información las cuales serán aprobadas por la dirección de la DIARI, publicadas y comunicadas a los funcionarios y a las partes externas pertinentes, con un periodo de revisión anual o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continúa.

¹² Referencia Estándar Internacional ISO/IEC 27001:2013 Anexo A numeral A.5 y A.6

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 14 de 71

La DIARI forma parte de la Mesa Técnica de Seguridad de la información la cual responde a las necesidades de la CGR en materia de seguridad informática y de la información, coordinando esfuerzos con la Oficina de Sistemas e Informática –OSEI- y la Unidad de Seguridad y Aseguramiento Tecnológico e Informático –USATI-¹³

La DIARI como parte de la Mesa Técnica de Seguridad de la información debe conocer los datos de contacto de las entidades que representen autoridad en temas de seguridad de la información y ciberseguridad, así como grupos de interés reconocidos.


Como evidencia del compromiso con la seguridad de la información y de la estructura de la organización de la seguridad de la información, la Dirección de la DIARI liderará en la operación del Proceso Gestión de información y de Análisis de información:

- La aprobación, aceptación y establecimiento de un esquema de políticas, procedimientos, guías formatos y demás documentos relacionados a la gestión de la Seguridad de la información.
- La conformación del equipo de Seguridad de la Información de la DIARI, el cual tendrá definido sus roles y responsabilidades siendo un componente necesario en todo el ciclo de vida del Sistema de gestión de seguridad en materia de información.
- La autorización para la comunicación de los compromisos a los jefes de unidad de los Procesos Gestión de información y Análisis de información en la coordinación e implementación, de las actividades de seguridad de la información al interior de su área, definidas al interior de la DIARI y por la CGR.
- El Suministro y aseguramiento de la disponibilidad de los recursos necesarios para la operación del Sistema de Gestión de Seguridad en materia de Información.
- El aval para la ejecución de las actividades propias en el establecimiento, implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad en materia de Información y las estrategias que de este se derive.
- La socialización de las propuestas de estrategias, programas y proyectos relacionados a la gestión de la Seguridad de la Información.

La DIARI debe designar a la persona que será la responsable del gobierno de la seguridad de la información al interior de la dirección, el cual diseñará e implementará el plan de seguridad de la información previa aprobación del Director (a) de la DIARI; este plan podrá estar alineado con el plan de seguridad definido para la CGR y debe tener en cuenta la estructura del Gobierno de Datos establecido al interior de la Dirección.

Es responsabilidad del líder de seguridad de la información de la DIARI, mantener, mejorar y gestionar la aplicación de las políticas o lineamientos de protección física, lógica o procedimental del Sistema de gestión de seguridad en materia de Información para la protección de los activos de información.

¹³ Las funciones de la Mesa Técnica de Seguridad están definidas en el memorando 2020IEC0032735.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 15 de 71

7.3 Políticas Operativas de Seguridad del Recurso Humano¹⁴

La DIARI debe informar a los funcionarios, pasantes, contratistas de prestación de servicios, proveedores y terceros relacionados, las responsabilidades con la seguridad de la información, adquiridas dentro del ejercicio de sus funciones y obligaciones contractuales. Estas responsabilidades aplicarán para todo el ciclo de la relación laboral o contractual e incluirán, entre otros, la definición de las funciones y responsabilidades sobre la data, la información, los recursos y los activos que la gestionan, las cláusulas de compromiso con la seguridad de la información, la firma de acuerdos de confidencialidad y las actividades tendientes a generar cultura y conciencia sobre la seguridad de la información. Esta obligación permanecerá vigente aún después de la terminación por cualquier causa de la vinculación que ligue a las partes tendientes a generar cultura y conciencia sobre la seguridad de la información. Esta obligación permanecerá vigente aún después de la terminación por cualquier causa de la vinculación que ligue a las partes.

La DIARI se sujeta a los procedimientos establecidos en la Contraloría General de la República -CGR- dentro de su proceso de selección de personal, por ello a través de los jefes de las unidades que la conforman determinará los perfiles requeridos para los cargos de la misma, para lo cual se debe considerar las cualidades académicas y laborales, la experiencia y los antecedentes disciplinarios, penales y fiscales del aspirante.


Todo funcionario, pasante, contratista de prestación de servicios y proveedor que acceda, genere, procese o transfiera información institucional debe firmar el compromiso de confidencialidad¹⁵ previo al inicio del ejercicio de sus funciones u obligaciones contractuales dentro de la DIARI; este acuerdo estará vigente durante el tiempo definido en el mismo, salvo que las partes en común acuerdo de manera escrita y bajo aprobación por parte de la oficina jurídica de la Contraloría General de la República, establezcan condiciones para su modificación o terminación.

Ante la identificación y validación de un incidente de seguridad de la información generado por la acción u omisión de las actuaciones de un funcionario, se evaluará la apertura de un proceso disciplinario al funcionario y/o el traslado a las autoridades competentes.

Todo cambio de la planta de personal y contratistas de prestación de servicios debe ser informado por el enlace de Talento Humano de la DIARI a los responsables de la gestión de los derechos de acceso a los recursos tecnológicos, con el fin de proceder a realizar las modificaciones sobre los privilegios de acceso de acuerdo a la novedad o en su defecto la denegación o retiro de los mismos.

¹⁴ Referencia Estándar Internacional ISO/IEC 27001:2013 Anexo A numeral A.7

¹⁵ Compromiso definido en coordinación con la USATI, la Gerencia de Talento Humano y la Dirección de Contratación, en lo de competencia de cada una, con la asesoría de la Oficina Jurídica.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 16 de 71

7.4 Política Operativa de seguridad de Control de Acceso¹⁶

La DIARI debe implementar un esquema de Gestión de Identidades y Acceso para administrar la identidad digital y el acceso a los recursos.

El acceso a las instalaciones físicas y recursos tecnológicos, deben otorgarse a través de los perfiles de usuario definidos de manera conjunta entre los jefes de las unidades y Seguridad de la Información de la DIARI, con una definición clara de roles y responsabilidades, que permita garantizar la segregación de privilegios y acceso a los recursos tecnológicos, sistemas y a la información.

Los controles que permiten el acceso a las instalaciones físicas y recursos tecnológicos deben proveer mecanismos de identificación, autenticación, no repudio y autorización; en lo posible aquellos recursos que lo permitan deben contar con factores de múltiple autenticación.

Se restringe el acceso a las áreas que contengan, almacenen o procesen información de la DIARI o dispongan de equipos de cómputo y comunicaciones especializados (computadores, servidores, routers, firewall, switches, consolas de administración, racks de comunicaciones, entre otros) mediante un perímetro de seguridad (tarjetas de identificación, señales de acceso restringido o mecanismos biométricos, chapas de seguridad o cualquier otro mecanismo de seguridad física o lógica implementado).¹⁷

El perfil asignado al funcionario, contratista de prestación de servicios, tercero, otorgará los derechos de acceso con el principio de mínimo privilegio y exclusivamente para las instalaciones y los recursos tecnológicos que la función del cargo requiera, durante el tiempo determinado por los Jefes de Unidad y/o el director(a) de la DIARI.¹⁷


La DIARI en coordinación con la USATI y OSEI procurará que el acceso a áreas seguras y/o restringidas de la DIARI solo esté permitido para:

- Desarrollar actividades de carácter tecnológico como: instalación de equipos, desarrollo de sistemas, pruebas e implementación de software y aplicaciones propias o de terceros.
- Efectuar visitas o inspecciones legales y de auditoría por parte de las áreas de control de la CGR u otros organismos de control del Estado.
- Realizar actividades de limpieza previamente planeadas y autorizadas.
- Efectuar los mantenimientos preventivos y correctivos para la infraestructura física y tecnológica que han sido programados y autorizados con anterioridad.

Cualquier otra actividad debe ser expresamente autorizada por el responsable (propietario o custodio) de los activos de información y estará sujeta al seguimiento correspondiente por parte de las áreas mencionadas

¹⁶ Referencia Estándar Internacional ISO/IEC 27001:2013 Anexo A numeral A.9.

¹⁷ Referencia Política de Control de acceso de la CGR.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 17 de 71

Las credenciales de acceso a los recursos tecnológicos estarán integradas con el Directorio Activo (AD) de la CGR, de tal manera que se mantengan las mismas políticas establecidas por la Contraloría General de la República en relación a su estándar de creación de usuarios y complejidad de contraseñas.

Las matrices de roles y perfiles registran la información referente a los recursos tecnológicos a los cuales se otorgará el acceso, el tipo de accesos autorizados al recurso por dependencia y cargo, perfil sobre el recurso, responsable de asignación y la fecha de actualización. Igualmente, los cargos de las matrices deben corresponder al grado, escala y denominación.

Los accesos tanto físicos como lógicos, asignados a los funcionarios, contratistas de prestación de servicios y terceros deben ser desactivados o modificados una vez terminados los vínculos contractuales con la DIARI y se deben devolver todas las credenciales que lo identifiquen como funcionario o contratista de prestación de servicios.

Los accesos a los tableros de los modelos de análisis de datos¹⁸ deben ser autorizados exclusivamente por el director(s) de la Dirección de información, análisis y reacción inmediata DIARI.

Observaciones:

Se deben registrar los accesos a la información, recursos tecnológicos, sistemas de información e instalaciones, de manera tal que permitan garantizar la trazabilidad de las acciones realizadas, identificando, entre otros datos relevantes, quién realiza el acceso, las operaciones ejecutadas, fecha, hora, lugar, cantidad de intentos de acceso, accesos denegados.

A los equipos de cómputo que no sean propiedad de la DIARI se les dará acceso únicamente a los recursos tecnológicos una vez se evalué la disponibilidad de estos, y los riesgos asociados al dispositivo y a su conexión.

Los derechos de acceso para cada usuario o grupo de usuarios deben tener las características de ser suficientes y con el principio de mínimo privilegio, de tal manera que le permita desarrollar sus labores sin exceder sus privilegios.¹⁹


Se deben crear perfiles de acceso asociados a roles que tienen responsabilidades y cumplen con actividades comunes; estos perfiles deben permitir el acceso mínimo y suficiente para el adecuado desempeño de las actividades de los usuarios. La asignación de los privilegios de acceso a los usuarios se hará con base en los perfiles de usuario aprobados y no basados en requerimientos individuales.

El uso de perfiles debe permitir la definición, control y alineación de roles, funciones, cargos, actividades y procesos con los derechos de acceso a los sistemas de información.

El acceso a los recursos tecnológicos se otorgará a través de cuentas de usuario personalizadas con el fin de evitar el uso de cuentas de usuarios genéricos que dificultan el seguimiento de las actividades de un usuario específico.

¹⁸ Los tableros de los modelos de análisis de datos son consultas visuales desarrolladas en herramientas de analítica y modelado de datos, utilizadas en el Proceso Gestión de información y Proceso de Gestión de Análisis de información para apoyar la toma de decisiones.

¹⁹ Los requerimientos de acceso de una aplicación a otra pueden variar por el esquema de control y aspectos técnicos. Las aplicaciones deben permitir la configuración de los accesos apropiadamente, pero a su vez a la hora de definir los accesos, cada aplicación debe ser considerada individualmente.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 18 de 71

Los jefes de las Unidades de Información y Análisis de Información de la DIARI deben realizar una revisión periódica de los privilegios de acceso otorgados a los usuarios de los servicios o activos de información a su cargo, que garantice que tengan los permisos de acuerdo a su perfil y sólo a la información de su competencia. La revisión debe incluir los usuarios (ID) con privilegios superiores utilizados para la administración de infraestructura, aplicaciones y sistemas de información de la entidad.

Observaciones:

La no adopción de perfiles de acceso aumenta la probabilidad de otorgar privilegios superiores a los requeridos, lo cual conlleva a que la revisión de los mismos requiera mayor esfuerzo para su detección y actualización.

Los funcionarios, contratistas de prestación de servicios y terceros deben informar al Líder de seguridad de la información de la DIARI sobre los eventos de seguridad de la información que detecten o sospechen sobre los activos de información.


Requerimientos para su aplicación:

- Los perfiles de usuario deben estar definidos, documentados y aprobados incluyendo todos los roles de acceso a los diferentes sistemas de información y demás recursos informáticos con su correspondencia de cargos y/o funciones.
- Se deben otorgar permisos de acceso a la información, sistemas de información y recursos informáticos en función de grupos; estos grupos deben ser conformados por individuos cuyo rol, responsabilidad y actividades sean equivalentes. Cada grupo debe ser asociado a un perfil de acceso autorizado por el propietario de la Información y los usuarios a quienes sea asignado un mismo perfil contarán con los mismos privilegios.
- Los mecanismos de control de acceso para cada aplicativo deben estar identificados y documentados.
- Los sistemas de información deben permitir la agrupación de derechos de acceso en perfiles.
- Los controles de acceso a la información y/o recursos tecnológicos deben estar definidos, documentados e implementados.
- La DIARI debe mantener un registro de la creación, modificación, desactivación y eliminación de las cuentas de usuarios de los funcionarios y contratistas de prestación de servicios autorizados para acceder a las instalaciones, recursos y sistemas de procesamiento de información.

7.4.1 Mecanismos de seguridad para controlar el acceso en recursos y servicios tecnológicos

Los administradores de infraestructura deben asegurar la eliminación o bloqueo de las cuentas de usuarios sobre los recursos tecnológicos, servicios de red y sistemas de información de manera oportuna, cuando les sean reportadas novedades de desvinculación, incapacidades, vacaciones, licencias u otras.

Los administradores de la infraestructura tecnológica asignarán los accesos a plataformas, usuarios y segmentos de red de acuerdo a procesos formales de autorización que serán gestionados a partir del formato solicitud de niveles de acceso servicios de red y sistemas de información; los niveles de acceso deberán ser revisados y autorizados por el

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 19 de 71

grupo de seguridad de la información, con el fin de verificar su autenticidad y evitar que puedan poner en riesgo la integridad y confidencialidad de los activos de información.

Se debe procurar que para el acceso a recursos tecnológicos de la DIARI se implementen mecanismos de autenticación multifactorial para mitigar los accesos no autorizados.

Los usuarios de los diferentes recursos tecnológicos realizarán un uso adecuado de los recursos y sistemas de información, quienes serán los responsables de las acciones realizadas en los mismos, así como de la cuenta de usuario asignado y la gestión de su contraseña para el acceso a estos.

Los usuarios deben acatar y respetar los privilegios provistos a través de la asignación de los perfiles para acceder a los aplicativos y no intentar sobrepasarlos mediante el uso de herramientas o utilitarios no autorizados. Cualquier modificación a los datos de un sistema debe realizarse por medio de la aplicación y usuario autorizados para tal fin.

Todo usuario al retirarse del equipo de cómputo debe dejar bloqueada su sesión para mitigar el acceso no autorizado por parte de otros funcionarios o terceros al mismo, que permitan suplantarlo y darle acceso a la información, recursos tecnológicos y sistemas de información.

Cualquier usuario interno o externo que requiera tener acceso remoto a la red y/o a la infraestructura de procesamiento de información, deberá adoptar las medidas de seguridad para establecer la conexión mediante el uso de VPN definidas por la Oficina de Sistemas e Informática (OSEI).


Por ningún motivo los usuarios podrán compartir las credenciales de acceso a la red interna o sistemas de información de la CGR entre sí o con personas externas para acceder en nombre de otro usuario, esto incurrirá en el delito de suplantación regido por el Código Penal en el artículo 296 llamado falsedad personal.²⁰

7.4.1.1 Gestión de los Accesos de los Usuarios

Se debe realizar una gestión centralizada del acceso de los usuarios a los diferentes sistemas de información que incluya el registro, modificación y cancelación de usuarios y que los accesos asignados correspondan a los derechos previamente definidos y autorizados. La gestión debe basarse en la matriz de roles y perfiles.

Todo acceso otorgado por el administrador del sistema de información debe contar con la debida autorización del propietario o custodio de la información permitiendo el acceso. Se debe realizar una revisión periódica entre los requerimientos de acceso de los usuarios a los aplicativos y el nivel de acceso autorizado y otorgado.

²⁰ <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=6388>

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 20 de 71

Observación:


Para garantizar la eficacia de la gestión de accesos, es necesario deshabilitar, actualizar o reasignar los privilegios de acceso a los recursos informáticos inmediatamente se presente la novedad correspondiente como retiro, traslado de dependencia, cambios de cargo de funcionarios, o cuando se genere un cambio de privilegios en un rol o perfil. Esta misma política se debe aplicar para los externos que tengan acceso a los recursos tecnológicos o información de la DIARI.

Requerimientos para su aplicación:

- Debe existir una identificación única de usuario (ID) para garantizar que los usuarios queden vinculados y sean responsables de sus acciones.
- No se permite la asignación de usuarios genéricos y/o la conservación de usuarios por defecto de la aplicación o del sistema sin asignación de responsables.
- Debe verificarse que el usuario tenga autorización de los propietarios de la Información para el uso del sistema o servicio.
- Debe verificarse que el nivel de acceso, o perfil, solicitado corresponda a los propósitos de su función, tarea o responsabilidad.
- Debe realizarse un mantenimiento formal y periódico de los usuarios registrados para usar el sistema.
- Informar a los usuarios los derechos asignados y los deberes que dicho acceso implica en el momento en que se entregan las credenciales.
- Debe existir un reporte oportuno de cualquier asignación, modificación, reasignación, desactivación, eliminación o cualquier otro evento relativo a la gestión de accesos y dejar registro de la actividad.
- Los recursos informáticos que manejan contraseñas deben conservar éstas cifradas y protegidas por algún otro mecanismo, para evitar comprometer su confidencialidad e integridad.
- Se debe exigir a los usuarios que cumplan las buenas prácticas de la organización para el uso y creación de contraseñas.
- En la medida de lo posible los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.
- Todas las contraseñas creadas en la DIARI deben cumplir con los requisitos establecidos en la política de gestión de contraseñas expuesta en este mismo documento.

7.4.1.1 Usuarios Privilegiados y/o Administradores

El uso de privilegios especiales en los recursos informáticos debe ser restringido y controlado. En general los usuarios con privilegios especiales deben usar métodos de acceso y comunicación seguros que autenticuen de manera fuerte al usuario y que garanticen la confidencialidad del acceso. Los usuarios privilegiados de los recursos informáticos deberán ser exclusivamente los autorizados por el propietario del recurso informático y deben disponer de dos códigos de usuario, uno para la ejecución de actividades privilegiadas y otro para la ejecución de las actividades habituales de usuario, con el fin de reducir el riesgo de incurrir en errores o en utilizar privilegios sin autorización ni justificación.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 21 de 71

Se debe implementar autenticación multifactorial para los usuarios privilegiados y administradores de la plataforma tecnológica de la DIARI.

Requerimientos para su aplicación

- Debe existir un inventario de usuarios privilegiados, administradores, usuarios del sistema y de comandos sensibles por plataforma.
- Los privilegios deben ser asignados basados en una necesidad de la DIARI y deben ser los mínimos para suplir los requerimientos funcionales del rol.
- Todos los usuarios privilegiados habilitados, deben estar asignados a un funcionario específico.
- En la medida de lo posible se debe desarrollar, automatizar y promover el uso de rutinas en los sistemas de información que lo requieran para evitar la necesidad de elevación de privilegios continuamente a los usuarios que requieran de ello para la ejecución de sus labores.²¹

7.4.1.1.2 Perfiles de Auditoría

Se debe contar con perfiles especiales definidos para ser usados por la auditoría interna. Los auditores deben tener privilegios y contar con los accesos necesarios para ver la información de la DIARI acorde con su clasificación, con la restricción que no puedan realizar ningún tipo de modificación. Toda actividad de los auditores debe quedar registrada en las plataformas tecnológicas.

Observación:

La función de auditoría requiere de acceso en forma de consulta a una gran cantidad de información de la DIARI e incluso de seguridad, derecho que por sus labores resulta incompatible con cualquier privilegio que permita modificación de la misma.


Requerimientos para su aplicación:

En todos los sistemas de información a los que por su función requieren acceso la auditoría interna, se debe contar con perfiles con permisos exclusivamente de consulta.

7.4.2 Gestión de contraseñas

Aplica a todos los servidores públicos de la DIARI: Empleados públicos de planta (Carrera administrativa y provisionales), funcionarios de libre nombramiento y remoción, trabajadores oficiales, contratistas de prestación de servicios y demás personal que tenga asignado un usuario y una contraseña para el acceso a alguno de los sistemas de información, bases de datos, equipos de cómputo o aplicativos que soliciten autenticación, de igual manera para los administradores de las diferentes plataformas tecnológicas con la que cuenta la CGR. Estos deberán preservar la

²¹ Referencia Estándar Internacional ISO/IEC 27001:2013 - A.9.2.3 - Gestión de derechos de acceso privilegiado.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 22 de 71

confidencialidad de la información de la CGR, los cuales están sujetos a los mismos requerimientos de seguridad, y tienen las mismas responsabilidades de salvaguardar la información; así como están obligados a continuar protegiendo y cumpliendo los acuerdos de confidencialidad durante y una vez terminada su relación laboral y/o contractual con la CGR.


El uso de credenciales para acceder a los recursos de red, aplicaciones, sistemas de información y los servicios dispuestos por la -CGR- para el cumplimiento de las labores de los funcionarios, contratistas de prestación de servicios y terceros son de carácter personal e intransferibles, por tal razón, están obligados a protegerlas cumpliendo con los acuerdos de confidencialidad y los lineamientos de esta política.

El usuario es responsable de establecer una contraseña segura, que cumpla con las siguientes características:

- La longitud de la contraseña debe ser mínimo de 8 caracteres, entre más caracteres tenga la contraseña es más difícil de descifrar por algún tercero.
- Las aplicaciones en las cuales la tecnología utilizada no contemple una longitud mínima de ocho caracteres, la longitud mínima deberá ser la máxima contemplado por el sistema.
- La contraseña debe estar compuesta por una combinación de letras mayúsculas, minúsculas, caracteres numéricos y símbolos especiales como los siguientes: ` ~! @ # \$ % ^ & * () _ + - = { } | [] \ : " ; ' < > ? , . /.
- Evitar utilizar secuencias básicas de teclado (por ejemplo: "qwerty", "asdf" o las típicas en numeración: "1234" ó "98765")
- No repetir caracteres en la contraseña. (ej.: "111222").
- No deben usarse palabras que aparezcan en los diccionarios de cualquier idioma.
- No debe haber una relación obvia con el usuario, sus familiares, nombre de la entidad, abreviaciones relacionadas a la entidad, ciudad, país, año, fecha de nacimiento, el grupo de trabajo u otras asociaciones parecidas, ya que pueden ser identificadas de manera fácil a través de un ataque de ingeniería social.
- No enviar nunca la contraseña por correo electrónico o en mensaje de texto.
- No se debe facilitar ni mencionar la contraseña en una conversación o comunicación de cualquier tipo.
- La contraseña debe ser cambiada con una periodicidad mínima de 60 días.
- No deben usarse contraseñas que sean idénticas o substancialmente similares a contraseñas previamente empleadas. Siempre que sea posible, debe impedirse que los usuarios vuelvan a usar contraseñas anteriores, esto se debe gestionar desde el sistema.
- No se debe escribir la contraseña en papeles y dejarla en sitios donde pueda ser encontrada por terceros.
- No se debe almacenar la contraseña en la computadora. Algunos cuadros de diálogo o ventanas emergentes de los navegadores presentan una opción para guardar o recordar la contraseña; no debe seleccionarse esa opción.

El usuario es responsable de hacer uso adecuado de las contraseñas cumpliendo con las siguientes recomendaciones:

- No debe escribir la contraseña en papeles o agendas y dejarla en sitios donde pueda ser encontrada por terceros.
- No debe enviar nunca la contraseña por correo electrónico o en mensaje de texto.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 23 de 71

- No se debe facilitar ni mencionar la contraseña en una conversación o comunicación de cualquier tipo, aun si se trata de sus superiores o compañeros.
- No debe almacenar la contraseña en archivos de texto o en cuadros de dialogo de los navegadores para recordar contraseña.
- Debe cambiar la contraseña con una periodicidad de 60 días
- No debe utilizar la misma contraseña para diferentes sistemas de información

Los administradores de plataformas, equipos de infraestructura tecnológica, sistemas operativos, bases de datos, sistemas de información, deben cambiar las contraseñas por defecto para los usuarios de nivel de sistema.

El administrador del Directorio Activo es responsable de asegurar que el mismo sistema solicite el cambio de la contraseña, cada vez que esta sea reestablecida por medio de una contraseña genérica a un usuario.

Se debe implementar mecanismos para solicitar cambio de contraseña cuando el usuario ingresa por primera vez a un sistema de información.

Se debe implementar mecanismos de no visualización de contraseñas en la pantalla cuando se está ingresando a los sistemas de información.

Las credenciales de acceso de administración a los sistemas de información y equipos que hace parte de la infraestructura tecnológica deberán ser almacenadas en un sobre sellado entregado al coordinador o jefe de la OSEI y ser almacenadas en una caja fuerte.

Si se tienen indicios para creer que una contraseña ha sido comprometida, esta debe cambiarse inmediatamente.

Las credenciales de acceso para los diferentes sistemas de información son de uso personal e intransferible.


Se deben implementar mecanismos para el cambio de las credenciales de acceso a sistemas de información cuando el usuario ingresa por primera vez.

Se deben implementar mecanismos de no visualización de contraseñas en la pantalla cuando se está ingresando a los sistemas de información.

Los usuarios por defecto en los sistemas de información o elementos de la plataforma tecnológica deben ser deshabilitados o renombrados siempre y cuando la plataforma lo permita.

Las credenciales de acceso de administración a los sistemas de información y equipos que hace parte de la infraestructura tecnológica deberán ser almacenadas en un sobre sellado entregado al coordinador o jefe de la OSEI y ser almacenadas en una caja fuerte.

En caso de que algún administrador de algún elemento de la plataforma tecnológica o sistema de información no se encuentre en la entidad y se requiera realizar alguna configuración urgente, se tendrá acceso al sobre cómo se

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 24 de 71

mencionó en el anterior párrafo y se realizara la configuración requerida por otra persona, que haya sido definida para el efecto.

Una vez se abra el sobre y realice la configuración requerida el administrador principal debe realizar el cambio de la contraseña y ser entregado de nuevo, así mismo cada vez que se realicen los cambios de las credenciales de acceso de las bases de datos, sistemas de información o aplicativos, elementos de infraestructura tecnológica, deben ser entregadas como se mencionó anteriormente.

El área de Talento Humano en conjunto con el grupo de gestión contractual y la OSEI deben definir un procedimiento que permita controlar de manera oportuna el ingreso, suspensión, retiro y/o movimiento dentro de las dependencias de la DIARI, de cualquier funcionario de la CGR. Novedades que deben ser reportadas inmediatamente sucedan al área correspondiente.

Para el personal que hace parte del operador tecnológico, si ésta figura se aplica en la entidad y son administradores de la plataforma de TI y/o sistemas de información de la entidad, una vez terminen su vinculación laboral con la CGR, se debe garantizar que esas credenciales de acceso sean deshabilitadas.

Las aplicaciones que utilicen mecanismos de autenticación deben almacenar las contraseñas utilizando algún método de cifrado.

Las credenciales asociadas a un usuario que se encuentre en periodo de vacaciones deberán ser deshabilitadas durante el periodo que duren las mismas.

La OSEI debe definir, desarrollar e implementar los procedimientos y acciones necesarias para cumplir con los lineamientos enunciados en esta política.


El administrador de cada sistema de información es responsable de asegurar que sean solicitadas las credenciales de acceso (usuario y contraseña) para el acceso a los mismos.

El administrador del Directorio Activo es responsable de asegurar que el mismo sistema solicite el cambio de la contraseña, cada vez que esta sea reestablecida por medio de una contraseña genérica a un usuario.

El usuario es responsable de bloquear su equipo en el momento en que se retire de su puesto de trabajo a una zona donde pierda visibilidad de este.

Los administradores de la plataforma tecnológica y sistemas de información deben utilizar cuentas de usuario diferentes a la cuenta del usuario administrador, admin o administrator con los mismos privilegios.

Es responsabilidad del administrador de cada sistema establecer los mecanismos para que la contraseña asignada al usuario le sea transmitida de la manera más confidencial posible.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 25 de 71

7.4.3 Uso de información de autenticación secreta

Todos los funcionarios, contratistas de prestación de servicios y terceros de la DIARI deben mantener la confidencialidad de la información de autenticación secreta (credenciales de acceso), asegurando la no divulgación.

Todos los funcionarios, contratistas de prestación de servicios y terceros de la DIARI deben evitar llevar un registro de autenticación secreta a menos que se almacene de forma segura y en un lugar virtual o físico aprobado por la Mesa Técnica de Seguridad.

Está prohibido compartir información de autenticación secreta del usuario individual así mismo está prohibido usar la misma información de autenticación secreta para propósitos que no sean inherentes a la gestión propia de la -CGR-.

La OSEI debe asegurar la protección apropiada de contraseñas cuando se usan como información de autenticación secreta en procedimientos de ingreso automatizados y estén almacenadas.

La DIARI de manera conjunta con la USATI realizará campañas de sensibilización periódicas a los funcionarios, contratistas de prestación de servicios y terceros de la DIARI encaminadas a fortalecer la creación, protección y uso responsable de las contraseñas.

7.5 Política Operativa de Gestión de Información y de Activos de Información²²


7.5.1 Inventario y Propiedad de Activos

La DIARI debe tener el conocimiento de los activos de información que posee como parte importante de la administración de seguridad de la información, estos deberán quedar registrados en un inventario de activos de la DIARI, con su respectiva clasificación de acuerdo a sus características de operación y/o naturaleza, así mismo deberá incorporar su valoración dada por las dimensiones de Confidencialidad, Integridad y Disponibilidad.

Los activos de información de la DIARI se entregan a la planta de personal y contratistas de prestación de servicios con un fin específico y regido por una necesidad de uso, de acuerdo al proceso o actividad laboral desarrollada. Toda utilización de estos activos de información con propósitos no autorizados o ajenos a la labor para la cual fue asignada es considerada indebida y se encuentra prohibida. En el evento que se presenten casos excepcionales deberán ser aprobados por el Director (a) de la Dirección de Información, Análisis y Reacción Inmediata y/o los jefes de unidad.

Las credenciales de acceso (usuario y contraseña) que permitan al funcionario público o contratista de prestación de servicios el ingreso lógico a sistemas de información y acceso a la información, es considerada como un activo de información de carácter reservado con un único responsable.

²² Dominio de control A8 Gestión de Activos, Anexo A Norma ISO 27001

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 26 de 71

Cada uno de los funcionarios de la DIARI, es responsable de los activos de información que le sean asignados o de los cuales haga uso para el desarrollo de las funciones propias de su cargo, por lo tanto, cualquier pérdida de integridad, disponibilidad o confidencialidad sobre los activos, derivado de sus actuaciones será evaluado como un incidente de seguridad.

El uso de los activos de información de la DIARI fuera de las instalaciones de la CGR debe ser autorizado por el Director (a) de la Dirección de Información, Análisis y Reacción Inmediata y/o los jefes de unidad y registrado por minuta digital o física en repositorio interno con tiempo límite de retorno.

Sin excepción al término de la relación laboral, contractual o finalización del vínculo con la CGR se deben devolver los activos de información a cargo de los responsables asignados, retirar los derechos de acceso, las copias no controladas y asegurar la entrega de la información a la DIARI.


Todos los funcionarios de la DIARI- son responsables de custodiar y salvaguardar la información que tienen a su cargo como se encuentra establecido en la ley 734 de 2002, por la cual se expide el Código Disciplinario Único. *“Artículo 34. Deberes. Numeral 5: 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 indebidos”.*

Las siguientes actividades sobre los activos de información de la DIARI, se consideran usos no autorizados y pueden constituir un incidente de seguridad de la información que se gestionan de acuerdo con su respectivo procedimiento.

- Acceder, modificar o divulgar la información sin autorización.
- Modificación o eliminación de los controles de seguridad que protejan la información.
- Conservar la información en condiciones seguras y tomar todas las medidas que sean necesarias para evitar que sea hurtada, copiada, reproducida, distribuida, divulgada o difundida en forma no autorizada.
- Abstenerse de utilizar la información en beneficio directo o indirecto, propio o de terceros.
- Se prohíbe la copia y envío de cualquier información o software que está protegido por copyright y por otras leyes de propiedad intelectual.
- Cualquier acción sobre la información considerada como ilegal o no autorizada por las leyes, regulaciones, normas o procedimientos a los que está sometida la DIARI.
- Utilizar el servicio de correo para suscribirse a servicios de ofertas, listas de correo de servicios no relacionados con las funciones o envío de cadenas.

7.5.2 Uso aceptable de Activos de Información

La DIARI proveerá a los empleados públicos de planta (carrera administrativa, provisionales, funcionarios de libre nombramiento y remoción), trabajadores oficiales, contratistas de prestación de servicios y demás personal, el acceso a la información requerida para el desempeño de las actividades que le han sido asignadas. Para el cumplimiento de esta política, se deben tener en cuenta los siguientes Lineamientos:


	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 27 de 71

- Todo acceso a la información debe ser autorizado formalmente por el área o proceso responsable de la información. Para la autorización de acceso a la información se debe contemplar un análisis previo de la justificación de la necesidad de uso de esta y las actividades a realizar con la información.
- Previo a todo acceso a la información debe considerar el nivel de clasificación según la Guía de Clasificación de Activos de Información y Etiquetado de información de la CGR
- Todas las actividades de administración, operación y uso de la información y de sus activos asociados deben estar orientadas a preservar la prestación de los servicios necesarios para el cumplimiento de la misión de la DIARI, los usos diferentes deben ser formalmente autorizados, tal y como lo establece la ley 734 de 2002, por la cual se expide el Código Disciplinario Único. *“Artículo 34, Deberes. Numeral 4: Utilizar los bienes y recursos asignados para el desempeño de su empleo, cargo o función, las facultades que le sean atribuidas, o la información reservada a que tenga acceso por razón de su función, en forma exclusiva para los fines a que están afectos.”*
- Los jefes de las unidades de Información y Análisis de Información son los responsables, respectivamente, de la gestión de riesgos de seguridad de la información de los procesos Gestión de Información y Análisis de Información.
- Todos los funcionarios y contratistas de prestación de servicios de la DIARI deben reportar sin demoras injustificadas a los responsables de sus áreas, a los líderes de los procesos o al Líder de Seguridad de la Información de la DIARI cualquier evento que pueda afectar la integridad, disponibilidad o confidencialidad de cualquier activo de información de la CGR.
- Dar uso de manera apropiada y coherente a los controles físicos de acceso (biométricos, lector de tarjeta, etc.) que permitan al funcionario público o contratista de prestación de servicios el ingreso a centros de datos, áreas restringidas. La pérdida o deterioro de estos activos debe ser reportada de forma inmediata a su superior.

Las siguientes actividades sobre los activos de información de la DIARI se consideran usos NO autorizados y pueden constituir un incidente de seguridad de la información:

- Modificación de la información sin contar con la autorización del propietario de la información.
- Divulgación no autorizada de información.
- Impedir el acceso a la información a los funcionarios, contratistas de prestación de servicios y terceros autorizados sin justificación.
- Modificación o eliminación de los controles de seguridad que protejan la información.
- Cualquier acción que, sobre la información, se considere como ilegal o no permitida por las leyes, regulaciones, normas o procedimientos que regulen la CGR.
- Utilizar la información de la DIARI para fines personales o diferentes a los requeridos para el cumplimiento de las funciones asignadas o el cumplimiento de las funciones de la CGR.
- Dar a conocer o compartir claves de acceso a la información a un tercero sea este otro funcionario, contratista de prestación de servicios o persona externa.

Es responsabilidad de todo funcionario, contratista de prestación de servicios y tercero, reportar los cambios, deterioros o daños que sucedan sobre los activos de información a su cargo ante los líderes de los procesos.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 28 de 71

Es responsabilidad de todo funcionario y contratista de prestación de servicios, aplicar los procedimientos definidos en el Sistema de gestión de seguridad en materia de información en los procesos de Gestión de información y Análisis de información de la DIARI, para el acceso de terceros a los activos de información a su cargo en situaciones como mantenimiento o garantía.

Es responsabilidad de los jefes de las unidades de Información y Análisis de Información de la DIARI, respectivamente, coordinar la aplicación de los procedimientos definidos en el Sistema de gestión de seguridad en materia de información para la asignación de cuentas de usuario y contraseñas de acceso a servicios y activos de información.

Es responsabilidad de la USATI en compañía de la OSEI proteger la información de configuración o parametrización de seguridad de los diversos componentes o servicios de información y tecnología de la DIARI que estén a su cargo.

7.5.3 Clasificación de información


Para la información se establecerá un criterio de clasificación según lo dispuesto por la CGR, de acuerdo a su nivel de criticidad. Para poder llevar a cabo esta labor, la DIARI ha adoptado el siguiente modelo de definición para la clasificación de la información²³:

- a) **Información pública.** Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal, que ha sido declarada legalmente o por su propietario, de conocimiento público y accesible a cualquier persona. Ej. Rendición de cuentas presentada por la entidad, plan de acción de la entidad, datos abiertos, entre otros.
- b) **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 consagrados en el artículo 18 de la ley 1712 de 2014 “Ley de Transparencia y derecho de acceso a la información pública nacional”..
- c) **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 en el artículo 19 de la Ley 1712 de 2004.

La DIARI adopta la clasificación de la información personal basado en la clasificación de los datos personales dispuesta en la Ley 1581 de 2012 “Ley protección de datos personales” por lo tanto se considera Información personal cualquier información relacionada con datos de personas naturales que permitan identificarlas o que permitan que sean identificables. La información personal se categoriza de acuerdo al dato que contenga, en este sentido, se toma como referencia el artículo 5 y 6 título III Categorías especiales de datos y artículo 2.2.2.25.1.3. Disposiciones generales,

²³ Ley 1712 de 2014 Artículo 6 Definiciones.

GIT-G-01 Guía Para la Calificación de la Información, Archivo General de la Nación.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 29 de 71

sección 1, “reglamenta parcialmente la Ley 1581 de 2012”, capítulo 25, Decreto 1074 de 2015 Sector Comercio, Industria y Turismo, clasificando la información personal como:

- a) **Información Personal Pública:** Información que contenga datos públicos que pueden o son conocidos por todas las personas, tales como datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su misma naturaleza los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.
- b) **Información Personal Semiprivada:** Información que contiene datos personales que no poseen naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, tal como datos financieros y crediticios, de actividad comercial o de servicios.
- c) **Información Personal Privada:** Información que por su naturaleza íntima o reservada sólo es relevante para el titular.
- d) **Información Personal Sensible:** Información que contiene datos sensibles siendo estos aquellos que afectan la intimidad de la persona y que su uso indebido puede generar discriminación. Se consideran datos sensibles aquellos que tengan que ver con el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos


7.5.4 Tratamiento de la información

Los empleados públicos de planta (carrera administrativa, provisionales, funcionarios de libre nombramiento y remoción), trabajadores oficiales, contratistas de prestación de servicios y demás personal, proveedores de servicios y terceros relacionados, de la DIARI, deben abstenerse de almacenar información que no esté relacionada con el desarrollo de sus funciones, en los recursos de Microsoft Office 365, Microsoft Azure o cualquier repositorio de información On- Premise o en la nube suministrado por la CGR, se exceptúa la información propia de capacitaciones realizadas o convocadas por la CGR.

Toda información o producto derivado de la misma que sea generada con recursos de la DIARI, es de propiedad de la CGR y como tal se debe proteger y usar para los fines propios de la labor misional de la DIARI.

Se prohíbe la apropiación y/o manipulación indebida de la información personal de los funcionarios que se transmite por los canales internos de la compañía o que está contenida en repositorios de información de la CGR.

En la medida de lo posible se debe planificar, diseñar, documentar e implementar las medidas para contar con controles relacionados con:

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 30 de 71

- Etiquetado de información en diferentes medios: impresa, en sistemas de información, correo electrónico, medios de almacenamientos, entre otros.
- Entrega de información a terceros.
- Destrucción de información y medios.
- Reutilización de medios.
- Destrucción de información contenida en recursos informáticos que se entregan a terceros.

Para garantizar la disponibilidad de la información de los usuarios, es responsabilidad de cada uno mantener y almacenar la información de la DIARI en los sitios institucionales de SharePoint, One Drive o en el servidor de archivos definido para cada área y/o usuario.

7.5.5 Destrucción de información

Cuando la información de la entidad de tipo pública, confidencial reservada o personal de tipo pública, semiprivada, privada o sensible, deba ser desechada, se deberá destruir de manera segura, independiente del medio en que se encuentre.

La información contenida en repositorios físicos deberá ser eliminada por la Dirección de Gestión Documental, según el Manual de Procedimientos de Gestión Documental, Archivo y Correspondencia publicado en el aplicativo SIGECI.


Para la información que reposa en medios digitales previo a su eliminación se deberá cifrar y posteriormente asegurar el borrado con técnicas que no permitan su reconstrucción, tal como la reescritura con ceros binarios, de tal forma que no sea recuperable.

La eliminación de información debe ser registrada y documentada de acuerdo el Manual de Procedimientos de Gestión Documental, Archivo y Correspondencia publicado en el aplicativo SIGECI.

7.5.6 Uso de Internet

El servicio de internet es suministrado para el cumplimiento misional de la DIARI, por lo tanto, se debe emplear en la ejecución de las actividades propias de la labor de los empleados públicos de planta (carrera administrativa, provisionales, funcionarios de libre nombramiento y remoción), trabajadores oficiales y contratistas de prestación de servicios, a quien le fue concedido el acceso.

Los permisos de accesos a determinadas URL o servicios accedidos por internet para solicitar la creación, modificación o cancelación de las cuentas de acceso al servicio, están definidos por perfiles de navegación, por lo cual, cualquier modificación de permisos debe ser solicitada por el funcionario al Líder de Seguridad de la Información de la DIARI con autorización previa del Director (a) de la Dirección de la Información, Análisis y Reacción Inmediata y/o los jefes de unidad. El aval de los permisos está sujeto a la necesidad de acuerdo a las funciones del solicitante y es otorgado a nivel técnico por la Unidad de Seguridad y Aseguramiento Tecnológico USATI.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 31 de 71

La DIARI de manera conjunta con la USATI y la OSEI regula el acceso a páginas Web dentro de las categorías definidas en los perfiles de navegación.

La OSEI debe establecer los controles para el acceso a internet de acuerdo a las funciones propias de los funcionarios, contratistas de prestación de servicios y terceros, adicionalmente controlar y monitorear el uso de los servicios de internet.

Es responsabilidad de la OSEI implementar y mantener una herramienta de antivirus y Antispam para el control del servicio de internet, Email y servicios relacionados.


Todo usuario es responsable tanto del contenido de las comunicaciones como de cualquier otra información que envíe desde la red de la CGR o descargue desde Internet.

La CGR o en su defecto la DIARI puede supervisar el acceso del servicio de Internet, con el fin de certificar que se está usando para el cumplimiento de las funciones institucionales, en los procesos y verificación del uso apropiado del servicio de acceso a Internet, respetando los derechos a la intimidad y privacidad usuario.

Cuando un funcionario o contratista de prestación de servicios al que le haya sido autorizado el uso de una cuenta de usuario para acceso a la red local de la CGR finalice su vinculación con la DIARI, deberá seguir los procedimientos definidos para entregar su cuenta de usuario y accesos a servicios informáticos provistos por la CGR.

Los funcionarios de la DIARI deben abstenerse de hacer uso del servicio de internet para:

- Navegar en sitios con contenidos que no se relacionen con la actividad laboral desempeñada
- Descarga de archivos con contenido que no obedezca a las labores propias del cargo.
- Ejecutar acciones que afecten la disponibilidad de los recursos tecnológicos.
- La participación de juegos de entretenimiento en línea.
- Cualquier actividad que sea lucrativa o comercial de carácter individual o para negocio particular.
- Solicitar, almacenar, transmitir y/o difundir información ofensiva, inmoral, engañosa y/o fraudulenta.
- Proferir amenazas, abusos, difamaciones, injurias, calumnias, actos obscenos, pornográficos, profanos, discriminatorios o para violar derechos de autor, secretos empresariales o cualquier tipo de derecho intelectual de las personas.
- El envío o descarga de información sometida a derechos de autor (música, videos, obras literarias, pictóricas, imágenes) no debe realizarse sin la debida autorización del ente regulador.
- El acceso a sitios Web considerados como ilegales por la normatividad colombiana, la ley de delitos informáticos y aquellos prohibidos por la Ley de Infancia y Adolescencia.
- La descarga de programas o aplicativos que puedan comprometer la seguridad de información del equipo de cómputo y de la red de datos de la Entidad.
- El streaming de video o audio, salvo que este tipo de transmisión sea necesaria y se requiera en la ejecución de labores propias del cargo. En ningún momento el streaming se permite para fines de entretenimiento en plataformas como (Disney+, Netflix, Star+, Universal+, Hbo+, Amazon Prime, Discovery+, Tubi, Spotify, Claro Video, Claro Music, Apple Music, Deezer, Playstation Plus, Xbox, Nintendo, etc.)

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 32 de 71

El personal debe abstenerse de descargar programas que realicen conexiones automáticas o visores de sitios clasificados como pornográficos y la utilización de los recursos para distribución o reproducción de este tipo de material, ya sea vía web o por medios magnéticos.

Todos los funcionarios y contratistas de prestación de servicios que, en el desarrollo de sus tareas habituales u ocasionales, utilicen el servicio de acceso a Internet de la entidad son responsables del cumplimiento y seguimiento de las políticas de seguridad de la información.

Todo usuario es responsable de informar si cuenta con acceso a contenidos o servicios que no le estén autorizados o no correspondan a sus funciones dentro de la DIARI.

Los responsables de la administración de las redes de acceso a Internet de la CGR deben implementar los lineamientos necesarios para evitar la circulación de información o contenidos desde Internet hacia la red de la Entidad que puedan constituirse en riesgos para la seguridad de la Información.

Los responsables de la administración de las redes de acceso a Internet de la CGR deben implementar los lineamientos de seguridad de la información que reduzcan los riesgos de pérdida de confidencialidad, integridad y disponibilidad de la información de la Entidad.


La OSEI en compañía de la USATI debe garantizar que el acceso al servicio de internet por parte de personal externo y que se encuentre dentro de las instalaciones de la DIARI este configurado en segmentos de red totalmente independientes a los segmentos de red administrativos, para evitar accesos no autorizados a la información.

7.5.7 Carpetas compartidas

El uso de carpetas compartidas sin restricción representa una práctica insegura toda vez que compromete la confidencialidad, integridad y disponibilidad de la información allí ubicada y facilita la distribución de virus u otros códigos maliciosos, por lo tanto, los usuarios no deben contar con privilegios para compartir carpetas en sus equipos, a excepción de las que han sido designadas para uso interno, las cuales en ningún momento podrán contener información de tipo confidencial. Como alternativa se podrá utilizar los recursos dispuesto por Office 365 especialmente en SharePoint con su correspondiente auditoría de logs activada.

7.5.8 Uso de medios removibles

La política de uso de medios removibles, tiene como objetivo asegurar el uso de dispositivos de almacenamiento externo para controlar el intercambio, transporte, almacenamiento y uso de información contenida de la DIARI. Esta política aplica para los funcionarios, contratistas de prestación de servicios, proveedores y terceros siempre que hagan uso de medios removibles de almacenamiento tales como discos duros externos, memorias flash (USB, SD, microSD) CD, DVD, entre otros.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 33 de 71

Los medios removibles permiten guardar información y trasladarla a diferentes sitios con la facilidad de conectarlos en diferentes equipos, lo cual, conlleva a una posible fuga de información intencional o accidental, así como a una fuente de infección de virus informáticos.

Todos los medios removibles que se utilicen para almacenar información al interior de la DIARI deben tener una justificación y limitarse a operaciones de negocio muy específicas que no están cubiertas dentro de los procedimientos y recursos definidos en la CGR.

Los medios removibles que se utilicen al interior de la DIARI deben estar autorizados, con el aval del líder del proceso. Los medios deben guardarse en un espacio adecuado y seguro, los usuarios no deben dejar los medios extraíbles sobre los escritorios o cajones sin llave.

Se debe cifrar los medios removibles, si la información almacenada está clasificada como información pública clasificada, publica reservada o datos personales privados o sensibles a fin de garantizar la confidencialidad e integridad de la información.

Los medios removibles aprobados para uso al interior de la DIARI, no se deben conectar a equipos externos a la red de la Entidad o de uso personal. En caso de ser requerido debe ser autorizada por la USATI con el aval del Profesional asignado para la gestión de la Seguridad de la Información.


El funcionario o contratista de prestación de servicios que haga uso de los medios removibles aprobados en la DIARI, será responsable de la información contenida, de la protección física del medio removible y permitirá la ejecución de las tareas de análisis con el software antivirus sobre el medio conectado.

Los medios removibles que se utilicen para almacenamiento de copias de seguridad, deben manejarse de acuerdo a la política de copias de respaldo y en ningún caso ser utilizados como recurso de almacenamiento primario.

En caso de daño físico y/o lógico, extravió, pérdida o robo del medio removible, se debe reportar al Tecnólogo y al Profesional asignado para la gestión de la Seguridad de la Información.

Los medios removibles que no se utilicen por obsolescencia, deben ser objeto de borrado seguro mediante uso de herramientas especializadas para tal fin y los medios removibles con daño físico y/o lógico no se deben utilizar y serán deshabilitados físicamente para evitar el posterior acceso al dispositivo.

Cualquier excepción a la política del uso de medios removibles, deberá ser tratada por el Profesional asignado para la gestión de la Seguridad de la Información con la autorización de la USATI.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 34 de 71

7.6 Política Operativa de Dispositivos Móviles²⁴ de propiedad de funcionarios y contratistas de prestación de servicios

El ingreso y uso de dispositivos móviles al interior de la Sala Suricato de la DIARI está restringido para todas las personas; las demás instalaciones de la DIARI están exentas de esta restricción.

Cada funcionario es responsable de la información de la CGR y/o DIARI que gestiona en sus equipos móviles por lo cual deberá reportar cualquier amenaza a la seguridad de la información que repose en su dispositivo móvil.

El personal que configure cuentas de correo o accesos a otras herramientas dispuestas por la CGR para el cumplimiento misional de la DIARI deberá ser consciente que ante la pérdida del dispositivo móvil o amenaza a la seguridad de la información utilizada en la DIARI, se podrá solicitar a la OSEI el borrado remoto del dispositivo móvil, en los casos en que el dispositivo móvil sea suministrado por la CGR.

Todo dispositivo móvil que gestione o acceda a información de la CGR y/o -DIARI deberá contar con medidas de bloqueo de acceso tales como: contraseñas, patrones, huella u otro método que restrinja el acceso no autorizado.

Las aplicaciones que se requieran para el funcionamiento de los dispositivos móviles deben descargarse a través de los portales oficiales y de acuerdo a cada sistema operativo o marca del equipo, con el fin de limitar la exposición de la información de la CGR y/o DIARI a cualquier amenaza derivada de escalamiento de privilegios o malware introducido a través de aplicaciones.


La aplicación de chat permitida para el intercambio y comunicación de información de la CGR en dispositivos móviles es Kaizala de Microsoft en razón del alto grado de seguridad y control en la comunicación que puede ser administrado; toda aplicación de chat diferente no debe ser utilizada dentro del manejo de información de la CGR.

El funcionario que gestione o acceda información de la CGR y/o DIARI a través de su dispositivo móvil debe evitar el acceso a redes inalámbricas de uso público o compartido con el fin de evitar una posible captura y análisis del tráfico de red, que pudiera revelar contraseñas y/u otro tipo de información confidencial.

Todo funcionario al momento de finalizar su relación laboral con la DIARI debe eliminar toda información que pudiera reposar en su dispositivo móvil esto incluyendo chats, archivos descargados, fotografías, capturas de pantalla, etc.

De acuerdo con los niveles de clasificación legal de la información almacenada en el dispositivo móvil de la CGR y en uso de la DIARI, se determinará la necesidad de aplicar controles de cifrado, de datos, así como la ejecución de copias de respaldo periódicas.

²⁴ Dominio de control A6 Organización de la Seguridad de la Información, Anexo A Norma ISO 27001

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 35 de 71

La DIARI debe seguir el procedimiento de atención de incidentes de seguridad de la información y los procesos administrativos definidos por la entidad en caso de eventos de hurto o pérdida de dispositivos móviles que contengan información institucional.

La OSEI tiene la autorización de realizar la desactivación, borrado y retiro de los accesos del dispositivo a los sistemas de información de la DIARI, cuando el dispositivo móvil haya sido extraviado, robado o haya sido comprometida su seguridad, en los casos en los que el dispositivo móvil haya sido suministrado por la CGR.

Los dispositivos móviles propiedad de los funcionarios o contratistas de prestación de servicios autorizados para acceder a la información o los sistemas de información de la DIARI deben contar como mínimo con las siguientes medidas de protección:

- Solución antivirus.
- Sistema de bloqueo por clave, pin, patrón, huella o reconocimiento facial.
- Software ofimático descargado de las tiendas oficiales para cada sistema operativo móvil.

La OSEI adopta e implementa los mecanismos de seguridad adecuados para proteger la información contenida y transmitida desde los dispositivos móviles de los funcionarios, contratistas de prestación de servicios y terceros de la DIARI a los que se le autoriza el acceso a la red de datos de la entidad.


La DIARI de manera conjunta con la USATI realizará campañas de sensibilización periódicas a los funcionarios, contratistas de prestación de servicios y terceros de la DIARI encaminadas al uso responsable de dispositivos móviles.

Todos los funcionarios, contratistas de prestación de servicios y terceros autorizados deben cumplir las políticas de seguridad de la información de la entidad desde el momento en que se les autoriza el uso de dispositivos móviles interconectados a las redes de datos de la entidad.

7.7 Política Operativa de Controles Criptográficos²⁵

Las técnicas y sistemas de cifrado de información se utilizarán para la proteger la confidencialidad, autenticidad y/o la integridad de la información gestionada en la DIARI según la necesidad de protección, clasificación de la información y/o el análisis de riesgo efectuado sobre la misma, con el fin de asegurar una adecuada protección de su confidencialidad, autenticidad e integridad.

²⁵ Dominio de control A10 Criptografía, Anexo A Norma ISO 27001

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 36 de 71

7.7.1 Uso de Controles Criptográficos

Con el objeto de proteger la confidencialidad, autenticidad y/o la integridad de la información se deben utilizar controles criptográficos o mecanismos de cifrado simétrico o asimétrico²⁶ en los siguientes casos:

- Para la protección de credenciales de acceso a sistemas de información, aplicaciones web servicios y/o datos.
- Para la transferencia de información confidencial, fuera del ámbito de la DIARI.
- La conexión a sistemas de información, vistas materializadas o contenedores SFTP de otras entidades.
- Para la protección de la información cuando el resultado de la evaluación de riesgos, arroje resultados que permitan determinar que se encuentra en un nivel de riesgo alto y sea contemplado su dentro del plan de tratamiento por la dirección de la DIARI.

Todo control o mecanismo criptográfico utilizado en la DIARI deben emplear algoritmos de cifrado estándar de reconocida eficacia²⁷.

Las llaves de cifrado deben ser administradas por un funcionario principal el cual las dispondrá en un recurso compartido de acceso exclusivo para un funcionario secundario. Las credenciales de acceso a las llaves de cifrado serán custodiadas en la Dirección de la DIARI y permanecerán en un sobre sellado y rotulado con el fin de mantener su confidencialidad.

Toda llave de cifrado utilizada para labores propias de la protección de la información de la DIARI deberá ser creada con la información de usuario de red asignado por la OSEI.

Se debe mantener un histórico de llaves para permitir la recuperación de llaves de generaciones anteriores. El histórico debe gozar de los mecanismos de protección contra modificación, destrucción y copia o divulgación no autorizada.


Se debe gestionar de manera segura el ciclo de vida de las llaves de cifrado: solicitud, generación, utilización, conservación y disposición.

Las claves utilizadas en los controles criptográficos, se deben utilizar siguiendo las recomendaciones establecidas por las entidades emisoras de dicho control.

Se debe evaluar la implementación de mecanismos de cifrado para la transmisión de información a través de correo electrónico.

²⁶ Técnicas de criptografía simétrica, cuando dos o más actores comparten la misma clave y ésta se utiliza tanto para cifrar información como para descifrarla. Técnicas de llave pública o criptografía asimétrica, cuando cada usuario tiene un par de claves: una clave pública que puede ser revelada a cualquier persona y utilizada para cifrar y una clave privada (que debe mantenerse en secreto) utilizada para descifrar.

²⁷ Los algoritmos de cifrado son estándares y públicos. La fortaleza y eficacia del cifrado depende de garantizar la confidencialidad, integridad y disponibilidad de las llaves, por lo que se requiere que estas sean gestionadas. Una llave criptográfica comprometida, comprometerá toda la información que haya sido cifrada con esta.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 37 de 71

La información pública reservada almacenada en servidores y equipos de cómputo debe permanecer cifrada para evitar que personas no autorizadas accedan o modifiquen su contenido.

El cifrado de la información aplica para las líneas de comunicación, bases de datos, sistemas de autenticación, medios removibles, dispositivos móviles u otros de acuerdo a las necesidades del servicio.

En el caso de llaves de cifrado sean perdidas, estén dañadas o su seguridad está comprometida, se debe seguir el procedimiento de gestión de incidentes de seguridad de la información.

Las claves serán deshabilitadas cuando estas tengan riesgo de divulgación o cuando los funcionarios, contratistas de prestación de servicios y terceros autorizados culminen la relación laboral o contractual con la DIARI.

7.7.2 Generación de HASH para datos estructurados y no estructurados

La Unidad de Análisis establecerá los modelos de análisis de información y las bases de datos para generar las alertas de presunto daño fiscal; definiendo los periodos de la actualización, con el fin de establecer los ciclos de generación HASH y los tiempos de disposición de las bases de datos entre la Unidad de Información y la Unidad de Análisis de la DIARI.


Los registros de evidencia de los HASH y los archivos HASH de las fuentes de datos, serán dispuestos en un repositorio para conservarlos como soporte de las alertas de presunto daño fiscal.

La validación de autenticidad de los HASH será realizada por un profesional con experticia técnica en tareas criptográficas, designado por el jefe de la Unidad de Información de la DIARI.

La generación de HASH (forma manual o automática), registro y validación de congruencia y autenticidad de los HASH, será realizada por el profesional designado por el jefe de la Unidad de Información de la DIARI, según los diferentes momentos del ciclo de vida de la información, como son:

1. Recepción de las fuentes de información por parte de los sujetos de control así:
 - Datos estructurados -Servidores y Data Lake (storage account) de la CGR
 - Datos no estructurados - Servidor SFTP de la Unidad de Información
2. Al estructurar la base de datos origen
3. Al disponer la base de datos desde la Unidad de Información para la Unidad de Análisis
4. Antes de restaurar la base de datos – Unidad de Análisis
5. Al realizar las validaciones y cruces de información necesarias para desplegar las Alertas

La generación de HASH permitirá evidenciar la integridad de la información durante todo el proceso de análisis y estructuración de las alertas de presunto daño fiscal

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 38 de 71

7.8 Política Operativa de Seguridad Física y del Entorno²⁸

Todas las áreas físicas de la DIARI deben tener un nivel de seguridad acorde con el valor de la información que se procesa y administra, para ello deberá contar con perímetros de seguridad, control de acceso basado en tecnología, manejo de bitácoras, carnés de identificación para funcionarios y visitantes, cámaras de vigilancia, puertas de acceso, alarmas, detectores de incendio y cualquier otro mecanismo de seguridad física implementado por la CGR.

7.8.1 Seguridad Física de Áreas de Acceso Restringido

Todas las áreas destinadas al procesamiento de información, así como aquellas en las que se encuentren los equipos y demás infraestructura tecnológica de soporte a los sistemas de información y/o comunicaciones, son consideradas áreas de acceso restringido y deberán contar con control de acceso²⁹ e ingreso limitado bajo el principio de menor privilegio.

Se debe velar porque las contraseñas de sistemas de alarmas, puertas de accesos, biométricos y/o enroladores de usuarios o de cualquier otro mecanismo de acceso seguro, solo sean conocidas por los funcionarios autorizados. Los valores por defecto deben ser modificados al momento de entrada en operación de la DIARI.

En el evento de requerir acceso a las áreas restringidas por parte de personal externo, deberá contar con la autorización respectiva de ingreso y deberá contar con el acompañamiento de un colaborador de la DIARI mientras permanezca en las instalaciones.

Todo ingreso de los visitantes al centro de comunicaciones que están bajo custodia de la DIARI, debe quedar registrado en una bitácora de acceso.

Cada vez que se produzca un cambio en la planta de personal de la DIARI, la USATI debe modificar de manera inmediata los privilegios de acceso a las diferentes dependencias de la DIARI en especial primordialmente donde se haga procesamiento de datos e información y en el centro de comunicaciones.


Se debe monitorear, controlar y verificar periódicamente la eficacia de los mecanismos de seguridad física y control de acceso al centro de comunicaciones y demás áreas de procesamiento de información.

Las irregularidades en la conexión o uso de las redes cableadas e inalámbricas de la DIARI serán gestionadas de acuerdo al Procedimiento de Gestión de Incidentes de Seguridad de la Información.

Toda conexión no autorizada de equipos a la red de la DIARI será bloqueada, inhabilitada y se gestionará como un incidente de seguridad de la información.

²⁸ Dominio de control A11 Seguridad física y del entorno, Anexo A Norma ISO 27001

²⁹ Los controles de acceso deben ser estrictos para mitigar amenazas derivadas de actos accidentales, como malintencionados y no se otorgarán autorizaciones de acceso permanentes.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 39 de 71

Todo acceso a la red de la DIARI mediante elementos o recursos tecnológicos no institucionales deberá ser informado, autorizado a través de la OSEI o en su defecto la USATI.

Los únicos autorizados para hacer modificaciones o actualizaciones en los elementos y recursos tecnológicos, como destapar, agregar, desconectar, retirar, revisar y/o reparar sus componentes, son los designados por la OSEI.

7.8.2 Protección Contra Amenazas Externas y Ambientales

Para las instalaciones de procesamiento de datos e información y para el centro de comunicaciones se debe aplicar protecciones contra daño por incendio, humedad, temperatura inadecuada, explosión, vandalismo, descargas eléctricas y otras formas de desastre natural o artificial. En la medida de lo posible se debe contar con sistemas de monitoreo y alarmas en caso de detectarse condiciones ambientales inapropiadas. Estos sistemas se deben monitorear de manera periódica y contar con el debido mantenimiento.

No está permitido realizar conexiones o derivaciones eléctricas y de red de datos por personal no autorizado, que pongan en riesgo la disponibilidad de la información por fallas en el suministro eléctrico o suministro de datos a los equipos de cómputo.


No está permitido realizar mantenimientos a dispositivos electrónicos sin que la alimentación eléctrica sea suspendida por el tiempo de la intervención. Los brigadistas que laboran en la DIARI estarán capacitados para manejar correctamente cada uno de los equipos de protección como extintores y en cómo actuar ante situaciones de emergencia, incluyendo simulacros periódicos.

Los equipos de seguridad tales como extintores deben revisarse periódicamente y garantizar su vigencia de acuerdo a las disposiciones internas de la CGR.

Se debe velar porque los recursos de la plataforma tecnológica ubicados en el centro de comunicaciones de la DIARI, se encuentren protegidos contra fallas o interrupciones eléctricas y separados de líquidos inflamables o que corran riesgo de inundaciones e incendios.

Los funcionarios deben portar el carné que los identifica en un lugar visible durante su permanencia en las instalaciones de la DIARI, en caso de pérdida del carné o tarjeta de acceso a las instalaciones, deben reportarlo a la mayor brevedad posible ante la Unidad seguridad y aseguramiento tecnológico -USATI-.

Todo colaborador que haga parte de la planta de personal de proveedores que desempeñe funciones de soporte, mantenimiento técnico o actividades asociadas a la prestación de servicios por contrato debe utilizar prendas distintivas y carné que facilite su identificación. Su ingreso deberá ser previamente autorizado y no podrá disponer de elementos o recursos sin que medie una supervisión por parte de la persona que autoriza su ingreso.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 40 de 71

Cualquier funcionario de la DIARI que observe la presencia de personas ajenas a la dependencia sin un debido acompañante, debe informar de inmediato al personal de recepción de la DIARI y/o debe abordar a la persona, para proceder a su identificación o conducción a la oficina correspondiente o a la salida de la dependencia.


Los equipos de cómputo y servidores deberán estar conectados a un tomacorriente regulado y una fuente de alimentación ininterrumpible de energía (protección de UPS). Está prohibido conectar aparatos u otros equipos diferentes a computadores a los tomacorrientes regulados.

7.8.3 Seguridad de los Equipos

Los equipos de cómputo deben estar ubicados o protegidos para reducir el riesgo derivado de amenazas o peligros del entorno, y de las oportunidades de acceso no autorizado.


Se deben considerar las siguientes directrices para la protección de los equipos:

- Los equipos que manejan datos de otras entidades deben estar ubicados de forma tal que se reduzca el riesgo de acceso físico y visualización de la información por personas no autorizadas.
- Todas las estaciones de trabajo, a excepción de aquellas que se encuentran en áreas con estrictas medidas de control de acceso y ejecutan labores de procesamiento continuo deben ser apagadas al final de la jornada laboral o al finalizar una sesión de trabajo.
- Los equipos deben estar apagados correctamente antes de ser desconectados del tomacorriente, así como para efectuar cualquier mantenimiento, instalación o actualización física de los mismos.
- Todas las estaciones de trabajo deben tener configurado y en operación el bloqueo automático de pantalla que se active cuando el equipo no esté en uso y bloquee las sesiones de usuario cuando se detecte inactividad por parte del funcionario.
- Se deben adoptar controles para minimizar el riesgo de amenazas físicas potenciales, tales como robo, incendio, explosión, humo, agua, polvo, vibración, efectos químicos, interferencia con el suministro eléctrico, interferencia en las comunicaciones, radiación electromagnética y vandalismo.
- Se debe evitar el consumo de bebidas, alimentos o consumo de cigarrillos o similares sobre las superficies cercanas a los equipos de procesamiento de información, al interior de la sala de comunicaciones o en los centros de datos y cableado.
- Se debe monitorear las condiciones ambientales, como polvo, temperatura y humedad relativa, para controlar las condiciones que podrían afectar adversamente el funcionamiento de los equipos de procesamiento de información y comunicaciones o acortar su tiempo de vida útil.
- Se debe aplicar protección frente a descargas eléctricas y adaptar protectores a las fuentes de energía entrantes y a las líneas de comunicación.
- Las áreas donde se realizan operaciones críticas de la DIARI deben estar protegidas contra fallas en el suministro de energía y otras anomalías causadas por fallas en los servicios de suministro. Las áreas de procesamiento de

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 41 de 71

información crítica y las indispensables para la operación de la DIARI deben contar con circuitos alternos y equipo de respaldo para suministro de energía.

- Es necesario contar con servicios de mantenimiento periódico a estos equipos y realizar pruebas programadas a los mismos para estar siempre en posibilidad de mantener la operación.
- La reasignación de equipos tecnológicos deberá ajustarse a los procedimientos y competencias de la OSEI.
- La OSEI realizara revisiones periódicas para verificar los equipos conectados y el uso de los servicios de las redes cableadas e inalámbricas de la DIARI.
- Los funcionarios, contratistas de prestación de servicios y terceros son responsables por el acceso y buen uso de los equipos de cómputo que se les asigne para uso exclusivo de tareas propias a sus funciones.
- La pérdida o daño de elementos o recursos tecnológicos, o de algunos de sus componentes, debe ser informada de inmediato al responsable del activo, por el funcionario o contratista de prestación de servicios al propietario del activo.
- Evitar escribir o dejar contraseñas u otros datos sensibles a la vista.
- Los computadores portátiles deben ser asegurados con cables o guayas de seguridad para contrarrestar y/o evitar su pérdida.
- Los gabinetes, cajones y archivadores que contengan documentos y/o medios extraíbles con información clasificada o reservada deben quedar cerrados durante el tiempo de descanso, almuerzo y al finalizar la jornada laboral.
- Los documentos físicos que contengan información catalogada como clasificada o reservada y que deban ser desechados, deben ser destruidos mediante rasgado o triturado.
- La pantalla del computador (escritorio) no debe contener ningún tipo de archivo o acceso directo a archivos, salvo los accesos directos a las aplicaciones necesarias para el ejercicio de las funciones.
- Al levantarse del puesto de trabajo se debe bloquear la sesión de los equipos de cómputo mediante las teclas Windows+L, para proteger el acceso a las aplicaciones y servicios de la entidad evitando la suplantación por parte de un tercero.
- La OSEI debe aplicar políticas de directorio activo para activar el bloqueo de la sesión al identificar inactividad del usuario transcurridos (5) minutos.
- Al imprimir información clasificada como pública reservada o pública clasificada o que contiene datos personales semiprivados, privados o sensibles los documentos deberán ser retirados de forma inmediata de las impresoras para evitar divulgación no autorizada de la información.
- El papel usado para reciclaje no puede contener información clasificada como pública reservada o pública clasificada o que contiene datos personales semiprivados, privados o sensibles, estos deben ser destruidos.
- Los funcionarios, contratistas de prestación de servicios y terceros deben reportar si no cuentan con los mobiliarios suficientes o adecuados para el almacenamiento de la información o si fallan los mecanismos de cerrado.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 42 de 71

7.9 Política Operativa de Seguridad de las Operaciones³⁰

7.9.1 Procedimientos Operacionales y Responsabilidades

Los procedimientos de operación de los servicios que presta la DIARI, así como de la operación de infraestructura tecnológica a nivel de hardware y software deben estar definidos, documentados y a disposición de las personas que lo requieran según la función que cumplan dentro de la misma con el fin de garantizar su operación correcta y segura.

Los procedimientos de operación deben ser divulgados a las partes interesadas y actualizarse periódicamente o cada vez que se presente un cambio significativo.


Se deben controlar los cambios en los diferentes recursos de TI como sistemas de información, infraestructura, comunicaciones, hardware, software base, servicios, etc., con el objeto de minimizar la probabilidad de interrupción de la operación de la DIARI, para ello todo cambio debe coordinarse con la Oficina de Sistemas e Informática –OSEI- con una metodología o procedimiento de gestión de cambios implementada.

La DIARI se debe alinear con los procedimientos definidos por la Oficina de Sistemas e Informática -OSEI- con el fin de gestionar los cambios de manera controlada de tal forma que se tome en consideración como mínimo los siguientes requisitos:

- Evaluación, priorización y autorización de peticiones de cambio.
- Determinación de su impacto en los procesos de negocio y los servicios TI.
- Registro, priorización, categorización, análisis, autorización, planificación y programación de los cambios.
- Definición, diseño, documentación, ejecución de pruebas y análisis de sus resultados con el objeto verificar que el cambio corresponde a la solicitud presentada y que la probabilidad que presente fallas o afecte otros componentes o sistemas se reduce a niveles mínimos.
- Gestionar cambios de emergencia
- Hacer seguimiento e informar de cambios de estado.
- Asegurar que los cambios aprobados son implementados como está previsto.
- Establecer las alternativas de roll back.
- Cerrar y documentar los cambios.
- Gestionar las remediaciones sobre posibles vulnerabilidades posteriores al cambio.

Los administradores de infraestructura de la DIARI a nivel On-Premise y en la nube deben hacer seguimiento al uso de recursos y hacer los ajustes y proyecciones de los requisitos de capacidad futura para asegurar el desempeño requerido y mitigar los riesgos asociados al agotamiento de recursos o disminución de la capacidad operativa.

³⁰ Dominio de control A12 Seguridad de las operaciones, Anexo A Norma ISO 27001

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 43 de 71

En alineación con la Oficina de Sistemas e Informática –OSEI- se deben implementar mecanismos, controles y herramientas necesarias para asegurar que los recursos que componen dicha plataforma sean monitoreados con regularidad y proyectados para futuros requerimientos de capacidad de procesamiento y comunicación.

Con el fin de garantizar la continuidad y seguridad de las operaciones se deben establecer roles y responsabilidades en cada fase del desarrollo o modificación de los sistemas de información de la entidad.


Se deben proveer los mecanismos, controles y recursos necesarios para contar con niveles adecuados de separación lógica y/o física entre los ambientes de desarrollo, pruebas y producción para toda la plataforma tecnológica y sistemas de información, con el fin de mitigar el riesgo asociado al acceso no autorizado, prevenir cambios y pérdida de la integridad, confidencialidad y disponibilidad de la información utilizada en las herramientas o sistemas de información que pudieran afectar la operación de la DIARI.

Por lo anterior se deben tomar en consideración los siguientes factores:

- Todo paso de software y hardware de un ambiente a otro debe ser controlado y gestionado.
- Los usuarios deben contar únicamente con los privilegios necesarios en cada ambiente para la ejecución de sus funciones.
- No se deben realizar pruebas, instalaciones o desarrollos de hardware o software directamente sobre el entorno de producción.
- El ambiente de pruebas debe emular el ambiente de producción lo más estrechamente posible.
- El uso de la información catalogada como clasificada y reservada está restringida en los ambientes de desarrollo y prueba; en caso de que sea estrictamente necesario su uso este debe controlarse y en lo posible utilizarse mecanismos que permitan su enmascaramiento.
- Se debe hacer el borrado seguro de la información clasificada y reservada luego de haberse utilizado en los ambientes de desarrollo y prueba.
- Se debe establecer los roles y responsabilidades en cada fase del desarrollo o modificación de los sistemas de información de la DIARI.
- Se debe monitorear el cumplimiento de las condiciones establecidas para el ciclo de desarrollo y cambio a sistemas de información, mediante la definición y ejecución de procesos, procedimientos o guías pertinentes.

En los casos en que se autorice el uso de medios de almacenamiento removibles a través de los puertos USB se debe revisar e inspeccionar permanentemente su contenido para detectar y contener cualquier virus o código malicioso presente en estos medios. Los agentes antivirus deben estar configurados para revisar automáticamente cualquier medio externo que se conecte a los equipos de cómputo de la entidad.

Todo código malicioso detectado por las herramientas de antivirus debe ser aislado en repositorios seguros y controlados para evitar que estos puedan afectar al mismo equipo o a cualquier otro equipo en la red.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 44 de 71

La OSEI debe velar porque la plataforma tecnológica desde donde se prestan servicios a los procesos de la CGR junto con los equipos de cómputo usados por los funcionarios cuente con herramientas robustas de Antivirus y control de código malicioso debidamente instaladas y actualizadas.

La OSEI debe restringir el acceso a sitios en internet de: descarga de software, redes sociales, video a demanda, contenido inapropiado y ocio, por medio de herramientas de seguridad que lo permitan, esto con el fin de evitar la descarga y distribución de código malicioso en los equipos de cómputo o la saturación de los canales de comunicaciones por el alto volumen de tráfico por fuera de la misionalidad de la DIARI.

Todos los funcionarios y servidores de la DIARI deben hacer buen uso de la red y los recursos informáticos provistos por la CGR para el desarrollo exclusivo de sus funciones laborales, por lo tanto deben abstenerse de descargar e instalar software no autorizado, deshabilitar los agentes de antivirus o herramientas de seguridad instaladas en el equipo, enviar archivos ejecutables a través del correo y cualquiera otra acción que conduzca a la distribución de virus o código malicioso hacia los demás equipos de la red.

La OSEI es la encargada de garantizar y monitorear permanente que todos los equipos de cómputo de la entidad cuenten con herramientas de seguridad tipo antivirus, debidamente instaladas, funcionales y actualizadas.

La OSEI en compañía de la USATI deben restringir de manera técnica por medio de soluciones de seguridad informática el acceso al código fuente de los sistemas de información en producción, en desarrollo y en pruebas exclusivamente a los desarrolladores o administradores de estas plataformas que por sus funciones explícitas deban tener contacto con este.

En caso que ocurra, se genere o se requiera un cambio sobre el código fuente, este debe ser realizado por medio de la gestión de cambios implementada por la CGR y con las autorizaciones previas de los líderes de los procesos o de la información y del comité de cambios, también la gestión implicara la comunicación a los usuarios finales que gestionan tareas sobre el sistema de información predicho.

Los administradores de infraestructura deben asignar los permisos de acceso basados en la matriz de roles y perfiles.


Los administradores de infraestructura deben implementar políticas de firewall para restringir el acceso únicamente a los usuarios autorizados.

Se debe activar el control de versiones habilitando el registro de auditoría de cambios realizados al código fuente.

El líder del proceso debe realizar seguimiento continuo al control de cambios del código fuente.

Se debe implementar análisis de vulnerabilidades periódico por parte del SOC para desarrollo de código fuente.

Se debe implementar las mejores prácticas para desarrollo de código fuente al interior de la entidad y se debe exigir su implementación a terceros que prestan servicio de desarrollo para la entidad.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 45 de 71

7.9.2 Control de Software Operacional y Contra Código Malicioso

La DIARI aplica la configuración de los recursos informáticos para cada plataforma sobre la cual opera de acuerdo con las condiciones establecidas por la Oficina de Sistemas e Informática -OSEI-.

Se debe contar con un inventario detallado y actualizado del software legalmente adquirido y licenciado que se utiliza en el cumplimiento de la misionalidad de la DIARI.

Se prohíbe la instalación de software que no se encuentre dentro de las listas blancas de la -CGR-; para evitar el incumplimiento de esta política se realizará monitoreo periódico del software instalado en los equipos de cómputo.

Todo software no autorizado será desinstalado por el equipo de soporte técnico de la DIARI.

Si se identifica una necesidad particular para el uso de un software específico, se deberá solicitar al responsable de seguridad de la información de la DIARI y/o de la USATI la evaluación de seguridad para su compra o instalación.

La instalación de software, así como la custodia de los instaladores y soportes o evidencias de licenciamientos deberán estar bajo la administración de la Oficina de Sistemas e Informática –OSEI- o del administrador de la infraestructura tecnológica de la DIARI.

Se deben implementar controles a nivel técnico para evitar la instalación no autorizada de software tales como: el uso de usuarios administradores.


Se debe considerar el uso de herramientas para el control y administración del software instalado en los recursos informáticos e inventario automático y en línea.

Está prohibida la descarga e instalación de software por parte de los funcionarios de la DIARI, esta labor debe ser ejecutada por el equipo de soporte técnico de la DIARI, previa revisión de la seguridad de los instaladores por parte del equipo de seguridad de la información. Se deben realizar verificaciones periódicas del cumplimiento de la configuración con el estándar definido.

Se debe verificar periódicamente que el mecanismo que permite distribuir, instalar y mantener actualizado el software de protección en todas las estaciones de trabajo se encuentre operando apropiadamente en los equipos de la DIARI

Bajo ninguna circunstancia se debe deshabilitar el software de protección que mitiga el riesgo de contagio de software malicioso en los equipos de procesamiento de la información.

La Oficina de Sistemas e Informática –OSEI- proveerá el software antimalware requerido para los equipos de procesamiento de información de la DIARI, bajo ninguna circunstancia los usuarios que cuenten excepcionalmente con los permisos de administración de su equipo de cómputo deben hacer instalaciones de software antimalware; esta labor es estrictamente ejecutada por el equipo de soporte técnico de la OSEI o de la DIARI.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 46 de 71

Los funcionarios de la DIARI deben verificar a través del software antimalware oficial dispuesto por la CGR, los archivos y/o documentos que son abiertos o ejecutados por primera vez, especialmente los que se encuentran en medios de almacenamiento externos o que provienen del correo electrónico.

Todo funcionario debe asegurarse que los archivos adjuntos remitidos desde correos electrónicos, o repositorios de información provienen de fuentes conocidas con el fin de evitar la infección por malware proveniente de funcionarios o terceros, bien sea por desconocimiento o por premeditación. En el evento en que sospeche de los archivos o correo electrónicos recibidos repórtelo al equipo de seguridad de la información de la DIARI para que se ejecute su revisión.

Cualquier evento de presencia de malware en los equipos de cómputo debe ser reportado inmediatamente al equipo de seguridad de la información de la DIARI para su revisión y escalamiento.

Las aplicaciones de software en su mayoría ofimático solo se deben implementar después de pruebas extensas y exitosas en los ambientes segregados de pruebas.

7.9.3 Copias de Respaldo y Almacenamiento

La información y los datos de los diferentes procesos y actividades que forman parte de las funciones de la DIARI requiere ser respaldada, para ello se debe definir al interior de la DIARI y acordar con la Oficina de sistemas e Información -OSEI- la estrategia y frecuencia de la generación de las copias de respaldo.


Es responsabilidad de la -OSEI- garantizar los medios y recursos necesarios (hardware y software) para restaurar la información que le permita mantener los procesos de la DIARI en operación.

El administrador de Infraestructura de la DIARI realizará pruebas periódicas y aleatorias de restauración de la información mediante la rotación de los medios y en un ambiente de pruebas adaptado para tal fin, con el objetivo de garantizar que la información es efectivamente recuperable ante cualquier evento de pérdida que requiera de su restauración. Estas tareas deben ser debidamente documentadas en la bitácora de seguridad dispuesta para alojar esta información.

El Líder de seguridad de la Información de la DIARI validará que la OSEI almacene en sitios seguros con controles físicos y/o tecnológicos las copias de respaldo que permitan el cumplimiento de los estándares mínimos necesarios para preservar las copias durante los períodos definidos.

Las copias de respaldo de la información deben ser preservadas por el tiempo definido en las tablas de retención de respaldo, con base en requerimientos legales y de la misionalidad de la DIARI y aprobadas por los líderes de los procesos a los que pertenece la información.

La OSEI debe definir e implementar un procedimiento claro y detallado de copias de seguridad de la información alojada tanto en la infraestructura On-Premise como en la Nube con las respectivas retenciones, tiempos, responsables, formatos de seguimiento y control a la gestión de backups.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 47 de 71

Se debe llevar un registro de las copias de respaldo con el fin de realizar seguimiento a la realización de las actividades.

La DIARI debe definir los activos de Información a respaldar y la prioridad de los respaldos, teniendo en cuenta:

- Sistemas Operativos
- Máquinas Virtuales
- Configuración de equipos activos
- Aplicativos
- Bases de datos
- Repositorios, bitácoras o fuentes de información maestra
- Datos de usuario
- Correos electrónicos
- Archivos grabación de Llamadas
- Archivos grabación de cámaras de seguridad

Es responsabilidad de la OSEI, mantener y aplicar los procedimientos de respaldo de la información y es responsabilidad de la DIARI realizar el debido seguimiento sobre la gestión de la información de la cual es propietaria.

7.9.4 Registro y Seguimiento

Se debe habilitar, conservar, proteger, administrar y revisar regularmente los registros acerca de actividades del usuario relacionados con los eventos de seguridad de la información ocurridos sobre los recursos tecnológicos de la DIARI, tales como: redes, servidores, bases de datos, repositorios de sharepoint, modelos de análisis, carpetas, etc.


Es responsabilidad de los administradores de infraestructura On-Premise y en la Nube la activación de los registros de auditoría y establecer plan de respaldo de logs de auditoría, alineándose a las directrices establecidas por la -OSEI- en relación a la retención, respaldo y recuperación de registros de auditoría, teniendo en cuenta los componentes de la plataforma tecnológica que se encuentren en el ambiente de producción.

Los administradores de infraestructura On-Premise y en la Nube de la DIARI deberán proporcionar los registros de auditoría de las plataformas tecnológicas de manera periódica o cada vez que sea solicitado por el equipo de seguridad de la información de la DIARI

En la medida en que sea posible, los logs deberán incorporar la siguiente información ³¹:

- Identificador del usuario que realiza la acción.
- Identificación del elemento sobre el que se realiza la acción (ficheros, bases de datos, equipos, etc.).

³¹ Tomado del documento Políticas de seguridad para la pyme "gestión de logs "INCIBE 07/10/2020
<https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/gestion-logs.pdf>

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 48 de 71

- Identificación de dispositivos (Direcciones IP, MAC, protocolos de red, puertos, etc.).
- Fecha y hora de ocurrencia del evento.
- Tipología del evento.
- Actividades del sistema.
- Registros de intentos de acceso a los recursos y sistemas de información exitosos y rechazados.
- Cambios de configuración del sistema.
- Uso de privilegios.
- Uso de utilitarios y aplicaciones del sistema.
- Archivos a los que se tuvo acceso y el tipo de acceso.
- Alarmas accionadas por el sistema de control de accesos.
- Activación y desactivación de los sistemas de protección, tales como sistemas antivirus y sistemas de detección de intrusos.
- Registro de las transacciones ejecutadas por los usuarios de las aplicaciones.

Se debe verificar la correcta sincronización de los relojes de los diferentes sistemas, plataformas o componentes de la infraestructura tecnológica con el fin de que exista una correlación entre los registros de los eventos registrados por cada uno.


Se debe procurar la centralización de los logs de las plataformas, sistemas o componentes de TI de tal manera que se pueda hacer un monitoreo integral de las acciones ejecutadas por parte de los usuarios de la DIARI sobre los recursos tecnológicos.

Las instalaciones y la información de registro de eventos se deben proteger contra modificaciones y acceso no autorizado. Con el fin de evitar los cambios no autorizados de la información del registro de eventos generados. La OSEI en acompañamiento de la DIARI deben implementar mecanismos de protección para evitar las alteraciones a los tipos de mensajes registrados y archivos de logs también proteger o poner en custodia los archivos logs de auditoría, con el fin de recolectar y retener evidencia.

Dado que el administrador tecnológico tiene permisos de usuario privilegiado, puede estar en capacidad de manipular los logs en las instalaciones de procesamiento de información, la DIARI debe implementar y controlar mediante mecanismos de supervisión para:

- Proteger y revisar los logs de auditoría, para supervisar la actividad usuarios privilegiados.
- Implementar mecanismos de control que permitan la segregación de funciones donde el operador tecnológico no tenga privilegios de administración sobre los eventos de registros de auditoría de los usuarios administradores y logs presentados.

Es responsabilidad de todo funcionario, contratista de prestación de servicios y tercero, conservar y no borrar los registros de eventos (logs) de los equipos o servicios que estén a su cargo.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 49 de 71

Es responsabilidad de los propietarios de la información, solicitar y conocer que eventos que se han producido sobre los sistemas de información.

El administrador de sistemas de información, aplicaciones, infraestructura tecnológica e infraestructura de seguridad informática debe mantener un inventario de los registros de auditoría existentes y su ubicación.

Se deben establecer directrices de retención, respaldo y recuperación de los logs y registros de auditorías de los componentes de la plataforma tecnológica cuando aplique, ya que estos se constituyen en evidencia para la identificación de un incidente de seguridad.

De acuerdo con las directrices de retención, respaldo y recuperación, aplicar el borrado de los registros de logs consolidados en la herramienta utilizada para el respaldo de logs de auditoría.

7.9.5 Gestión de las Vulnerabilidades Técnicas


De acuerdo a las disposiciones que establezca la Mesa Técnica de Seguridad de la CGR, se debe llevar a cabo un análisis de vulnerabilidades con una periodicidad semestral y gestionar las vulnerabilidades encontradas. Se debe documentar y presentar un informe consolidado de las vulnerabilidades y de las acciones tomadas para su remediación.

La remediación de las vulnerabilidades técnicas de la infraestructura On-Premise y en la Nube se coordinarán con la Oficina de Sistemas e Informática -OSEI- y deberán ser realizadas a través del proceso de gestión de cambios de la CGR. La -OSEI- es el responsable de gestionar la remediación oportuna de las vulnerabilidades encontradas priorizando las de mayor criticidad o nivel de exposición, para esta gestión se deben establecer planes de remediación con sus respectivas fechas de implementación.

La Mesa Técnica de Seguridad en conjunto con la OSEI deberá definir, desarrollar e implementar los procedimientos y acciones necesarias para cumplir con los lineamientos enunciados en esta política. La DIARI debe contar suscripciones y/o consultas frecuentes a fuentes de información acerca de vulnerabilidades técnicas, preferiblemente de fabricantes y fuentes reconocidas, con el fin de comunicarlas a la Mesa Técnica de Seguridad de la información.

Los proveedores tecnológicos a cargo de labores de soporte de equipos y sistemas informáticos deben garantizar que estos se encuentren libres de código malicioso y vulnerabilidades técnicas, a su vez deben realizar revisiones frecuentes de vulnerabilidades junto a la gestión y respuesta oportuna de remediación según la criticidad de los hallazgos encontrados, las acciones realizadas deben ser registradas y estar a disposición de la DIARI.

Los métodos utilizados en la identificación y el análisis de vulnerabilidades deben ser controlados y confiables para no afectar la operación de los equipos y sistemas informáticos de la DIARI. Los resultados del análisis de la exploración de vulnerabilidades deben ser almacenados en repositorios seguros y de acceso restringido para propósito de gestión, control y seguimiento.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 50 de 71

La aplicación de parches de seguridad debe ser probada previamente en ambientes controlados de pruebas para garantizar la no afectación de los sistemas informáticos de producción. Estos parches deben provenir de fuentes legítimas y confiables.

Anualmente se debe realizar por lo menos una (1) prueba de hacking ético 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.

Todos los equipos de cómputo deben estar en el dominio de red de la CGR para poder aplicar las directrices de seguridad distribuidas desde el directorio activo.

La Mesa Técnica de Seguridad debe establecer el cronograma anual de escaneo de vulnerabilidades de todos los equipos y sistemas informáticos de la red y gestionar su oportuna ejecución.

La mesa técnica debe realizar el seguimiento y monitoreo a la oportuna gestión de las vulnerabilidades técnicas encontradas y la ejecución de los planes de remediación establecidos.

Es responsabilidad de la Mesa Técnica de Seguridad con los líderes de los procesos y áreas de la DIARI gestionar las medidas de mitigación para contrarrestar las vulnerabilidades que se identifiquen sobre los componentes o servicios de tecnología.

Es responsabilidad de la OSEI, mantener actualizado el sistema operativo y el software instalado en los computadores de escritorio, computadores portátiles, servidores, con el fin de prevenir incidentes de seguridad relacionados en los mismos que pongan en riesgo la disponibilidad y continuidad de los recursos informáticos


7.10 Política Operativa de Seguridad de las Comunicaciones ³²

7.10.1 Gestión de la Seguridad de las Redes


Las redes de comunicaciones de la DIARI se deben mantener y controlar adecuadamente para protegerlas de las amenazas y mantener la seguridad de los sistemas y aplicaciones que usan la red, incluyendo la información en tránsito para ello se deberá considerar:

- La red de datos de la DIARI debe estar segmentada y su acceso debe otorgarse por medio de listas de control de acceso (ACL) que incluirá solo al personal de operación autorizado. **Nota:** Un método de controlar la seguridad en redes es dividirlos en dominios lógicos independientes basados en criterios como la criticidad de los sistemas o recursos y el tipo de recursos y servicios.
- La autenticación de las máquinas en la red de la DIARI debe hacerse por IP y MAC.

³² Dominio de control A13 Seguridad en las comunicaciones, Anexo A Norma ISO 27001

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 51 de 71

- La red de datos de la DIARI debe contar con filtrado de conexiones entrantes y salientes a través de los switches y firewall.
- Las reglas del firewall utilizados en la - DIARI- deben estar configuradas de tal forma que permitan detectar cualquier actividad relacionada con el escaneo de puertos.
- La información el tráfico de la red de datos de la DIARI debe viajar cifrada (IPSEC, TLS, SSH, HTTPS) con el fin de evitar accesos no autorizados.
- El firmware de los router, IDS, firewall y demás dispositivos de la seguridad perimetral empleados en la red de la DIARI debe estar actualizados a la versión más reciente liberada por el fabricante.
- Se debe deshabilitar el uso de los servicios, protocolos y puertos no utilizados por el firewall, para ello el administrador de infraestructura de la DIARI debe identificar los servicios, protocolos y puertos permitidos por la CGR e inhabilitar o eliminar los que no sean necesarios para la operación.
- Bajo ninguna circunstancia está permitido el acceso a recursos informáticos de la red de la DIARI través de RDP sino media una conexión VPN S2S o S2C configurada por la OSEI.
- La configuración de los equipos de red tales como enrutadores, switches, firewall, sistemas de detección de intrusos y otros dispositivos de seguridad de red; debe estar documentada, respaldada por copias de seguridad y estar disponible para usuarios autorizados.
- Es responsabilidad del administrador de los recursos tecnológicos de la DIARI validar que los puertos físicos y lógicos y configuración de plataformas que soporten sistemas de información estén restringidos y monitoreados con el fin de prevenir accesos no autorizados.
- La OSEI es responsable de garantizar la disponibilidad de los recursos tecnológicos y la redes cableadas e inalámbricas y los servicios de red de la DIARI la cual administrará y controlará la cantidad de equipos conectados a las mismas de acuerdo a la capacidad, licenciamiento y otros componentes tecnológicos.
- La conexión a la red de datos para los equipos que no son de propiedad de la DIARI: (portátiles, celulares, tabletas), se debe realizar por medio de una conexión inalámbrica a una red diferente de la red administrativa y se concederá el acceso a internet con privilegios mínimos de navegación.
- La asignación del direccionamiento IP a los dispositivos de red, será controlada y centralizada por medio del servicio de DHCP.
- Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.
- La OSEI definirá los procedimientos técnicos de administración para proteger el acceso a las conexiones de la red y los servicios en red.
- La DIARI en compañía de la USATI y la OSEI deben establecer un procedimiento para que todos los usuarios de la Entidad cuenten con un identificador único (ID de usuario) para su uso personal, para lo cual se debe escoger una técnica de autenticación adecuada para validar la identidad de un usuario de la DIARI.
- La identificación automática del usuario se debe considerar como un medio para autenticar las conexiones de ubicaciones y equipos específicos.
- Se debe aplicar este procedimiento a todos los tipos de usuarios (incluyendo el personal de soporte informático, operadores, administradores de redes, programadores de sistemas y administradores de bases de datos, administradores de seguridad).
- Se deben utilizar los IDs de usuarios para rastrear las actividades hasta la última persona responsable.
- No deben realizarse desde cuentas privilegiadas, las actividades de usuarios finales.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 52 de 71

- Se requerirá autorización para utilizar un ID de usuario compartido para un grupo de usuarios o un trabajo específico.
- Para autenticación y verificación sólida de identidades, se deben utilizar métodos de autenticación alternativos para las claves secretas, por ej.: medios criptográficos, tarjetas inteligentes, dispositivos o medios biométricos.
- La OSEI en acompañamiento de la USATI deben asegurar que todos los medios físicos de transmisión empleados en las redes de la Entidad cumplan con los estándares necesarios que garanticen su calidad y óptimo funcionamiento durante el mayor tiempo posible.

La OSEI debe asegurar que toda solución de red cableada implementada en las instalaciones de la DIARI esté debidamente certificada.

La OSEI establecerá controles para evitar el acceso a los puertos físicos de diagnóstico y configuración, al igual que configurar puertos de administración local y puertos de administración remota con soporte 7x24.

La OSEI debe definir el tiempo mínimo de inactividad de las aplicaciones y las sesiones de red antes de su cierre.


Se debe verificar la reputación y confiabilidad de los sitios o páginas web publicadas en internet, a través del uso de herramientas de seguridad. El acceso desde cualquier sitio de la red a sitios web maliciosos o sospechosos, será restringido.

7.10.2 Transferencia de Información

Todos los funcionarios, contratistas de prestación de servicios y terceros que tengan acceso a la información de la DIARI, deben protegerla de divulgación no autorizada conforme a las Políticas de Seguridad de la Información de la CGR. Se deben usar los mecanismos y lineamientos de seguridad establecidos para el tratamiento de la información, así como los referenciados en la Guía de clasificación de activos de información y etiquetado de información de la CGR. La información sólo podrá ser usada para las actividades autorizadas dentro de los acuerdos suscritos o convenios entre la DIARI y las partes interesadas.

Los procesos de transferencia o transmisiones de la información entre la DIARI y las partes interesadas externas deberán contar con documentos técnicos de entendimiento que especifiquen los mecanismos y controles de transferencia que se emplearán en el proceso.

El intercambio o transferencia de información se efectuará con forme a las características del contrato o según los acuerdos de entendimiento técnico establecidos, que deben describir: Las responsabilidades y procedimientos para la transferencia segura de la información, el responsable y proceso a seguir en caso de presentarse un incidente de seguridad, los niveles de clasificación de la información a ser intercambiada.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 53 de 71

La transmisión de la información se desarrollará teniendo en cuenta la normatividad colombiana vigente, especialmente la Ley de Protección de Datos Personales (Ley 1581 de 2012 y decretos reglamentarios) y Ley de Transparencia (Ley 1712 de 2014).

La DIARI debe firmar acuerdos de confidencialidad o no divulgación con las entidades que lo requieran, dentro del marco de la transferencia de la información y cumplimiento de cualquier circular o acuerdo de transferencia establecido con las entidades, que garanticen la protección de la información durante y posterior al tiempo de ejecución del tiempo de tratamiento de la información.

La transferencia de información entre la CGR y las entidades públicas o privadas deberá realizarse a través de conexiones VPN Site to Site o SFTP, como alternativas de transferencia se podrá considerarse OneDrive o SharePoint de Microsoft.

Cualquier alianza o convenio de procesamiento de información con proveedores o con personal externo a la entidad debe contar con mecanismos de confidencialidad, integridad y auditabilidad de tal forma que cumpla con los estándares definidos por seguridad de la información de la CGR

Cualquier información que ingrese o salga de la DIARI por medio físico deberá tener los mecanismos de cifrado, así como la autorización y registro de los eventos que aseguren la trazabilidad de quien ejecuta la transferencia.


No se permite el envío de información de tipo confidencial, personal o sensible a través de canales de comunicaciones no seguros o por fuera de los ya establecidos en los procedimientos del SGS para proteger dicho tipo de información.

Todos los funcionarios, contratistas de prestación de servicios y terceros deben abstenerse de comunicar información de tipo personal, confidencial o sensible en sitios públicos, oficinas abiertas, áreas de reuniones o a través del uso de canales de comunicación no seguros.

Cada una de las partes involucradas en la transferencia de información debe analizar y mitigar los riesgos asociados con la pérdida de confidencialidad, integridad o disponibilidad. Se deben emplear canales de transmisión de datos (físicos o lógicos) que permitan brindar la seguridad y protección adecuada preservando la confidencialidad e integridad de la información, conforme a su nivel de clasificación.

Los contratistas de prestación de servicios y terceros deben contar con los lineamientos de seguridad suficientes para garantizar que la información que será transmitida electrónicamente a la DIARI se encuentre libre de virus o códigos maliciosos.

La OSEI con la USATI deben proveer los mecanismos de seguridad idóneos para inspeccionar la información recibida de terceros, verificando que se encuentre libre de virus o códigos maliciosos antes de que esta sea utilizada al interior de la DIARI.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 54 de 71

7.10.3 Mensajería Electrónica

El buzón de correo electrónico suministrado por la CGR a los funcionarios y contratistas de prestación de servicios de la DIARI es para la ejecución de las labores asociadas y/o derivadas de su cargo, por lo cual no está permitido el uso de la cuenta de correo para el registro en redes sociales, foros o plataformas extralaborales y no debe ser utilizado para actividades de tipo personal. Se exceptúan actividades relacionadas con capacitaciones brindadas por el Centro de Estudios Fiscales de la CGR donde el correo sea requerido para labores de registro y acceso a los recursos de capacitación.

El responsable del área o proceso al que pertenece el funcionario, contratista de prestación de servicios o tercero que presta sus servicios a la DIARI, debe autorizar el trámite para la solicitud de asignación de cuenta de correo electrónico ante la OSEI.

El servicio de correo electrónico oficial de la CGR es el establecido por la OSEI y será responsabilidad de los funcionarios, contratistas de prestación de servicios o terceros los incidentes de seguridad de la información que se deriven del uso de la cuenta de correo para los servicios no autorizados por la Entidad.

LA CGR debe contar con mecanismos técnicos idóneos que permitan analizar el contenido de los correos entrantes en busca de software malicioso, se deben inspeccionar previamente los archivos adjuntos en los correos, eliminando o enviando a cuarentena los archivos infectados o sospechosos.

El uso del servicio de correo electrónico debe tener un comportamiento ético y debe ser consecuente con todas las Políticas y procedimientos institucionales que apliquen para comunicaciones oficiales.


El correo electrónico institucional constituye un activo de información de la CGR por lo que se deben aplicar los procedimientos de gestión de información incluyendo períodos de retención y consulta bajo las leyes correspondientes.

Los mensajes y la información contenida en los buzones de correo son propiedad de la Contraloría General de la República -CGR-, todo funcionario es responsable del contenido que reposa en su buzón por lo cual debe mantener mensajes relacionados con el desarrollo de sus funciones.

El envío de información autorizada y asociada a la misionalidad de la DIARI que requiere ser remitida a otras áreas o entidades, debe realizarse de forma exclusiva desde la cuenta de correo electrónico que la CGR proporcione para el usuario.

Se consideran como inherentes al desarrollo de las funciones:

- Comunicación con terceros afines a la naturaleza de la entidad con el fin de poder acceder a la información relacionada con la especialidad o tareas desempeñadas.
- Acceso a servicios prestados por terceros y/o proveedores a la DIARI y/o CGR.
- Comunicación entre entidades públicas y/o privadas siempre y cuando estén vinculadas con las tareas encomendadas.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 55 de 71

La cuenta de correo electrónico asignada es de carácter individual; por consiguiente, se debe evitar su préstamo, así como el uso de buzones de correo ajenos. Está prohibida la suplantación de la identidad de otro funcionario.

Los usuarios de correo electrónico institucional tienen prohibido:


- El envío de cadenas de mensajes de cualquier tipo, ya sea comercial, político, religioso, amenazante, discriminatorio, pornográfico, político y demás que puedan contribuir a un ambiente de trabajo hostil o que degraden la condición humana y resulten ofensivas para los funcionarios de la CGR.
- Crear o remitir mensajes de correo en forma masiva que pueda contribuir a afectar el desempeño de la red y/o el servicio de correo.
- Enviar archivos que contengan extensiones ejecutables, esto con el fin de evitar infecciones por malware.
- Crear, almacenar o intercambiar mensajes o contenido en archivos adjuntos que violen las leyes de material protegido por la ley de derechos de autor, normas sobre seguridad de la información y protección de datos personales.
- Enviar o intercambiar información que atente contra la protección de los datos personales y sensibles afectando la intimidad del Titular como son los datos relativos a la salud, vida sexual o biométricos o que pueden generar discriminación como son el origen racial o étnico, orientación política, convicciones religiosas o filosóficas, pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promuevan intereses de cualquier partido político. Está prohibido el envío o intercambio de datos personales o sensibles de menores, incluso a través del correo electrónico cuando esta no valla cifrado.
- Crear, enviar, alterar, borrar mensajes suplantando la identidad de un usuario.
- Abrir, usar o revisar indebidamente la cuenta de correo electrónico de otro usuario, sin contar con la autorización formal del titular de la cuenta.

Está prohibido el uso del correo electrónico personal de los funcionarios para el envío o recepción de cualquier tipo de información relacionada con la entidad.

En los casos en los que se requiera envío o recepción de información pública clasificada con carácter reservado o confidencial, el usuario del servicio de correo electrónico debe aplicar el mecanismo de cifrado de datos establecido por la Mesa Técnica de Seguridad.

Sobre el tráfico de correo electrónico se deben aplicar medidas de seguridad para inspeccionar, detectar y restringir el ingreso o salida de código malicioso, las cuales deben ser aplicados tanto en el servidor de correo como en los agentes instalados en los equipos de cómputo de la entidad.

Los correos electrónicos deben respetar el estándar definido por la CGR, en cuanto a formato, firma, imagen y nota de confidencialidad. Esta última es una medida preventiva de divulgación no autorizada de contenidos de correo electrónico. Al finalizar la relación laboral de todo funcionario, contratistas de prestación de servicios o tercero que preste sus servicios a la -DIARI, deberá informar y realizar la devolución de las cuentas genéricas de correo electrónico al responsable del proceso para el cual laboraba.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 56 de 71

La OSEI deberá realizar copias de seguridad del buzón de correo electrónico cuando un funcionario o contratista de prestación de servicios se retira de la DIARI.

7.11 Política Operativa de Servicios de Computación en la Nube

En los procesos de contratación y uso de servicios de computación en la nube se deben identificar, valorar y gestionar los riesgos de seguridad asociados al tratamiento de información institucional, acceso a información personal, resistencia a ataques cometidos desde el ciberespacio, protección de secretos comerciales, riesgos legales, riesgos técnicos, riesgos de continuidad y riesgos asociados a la transmisión transfronteriza de la información institucional o personal. El análisis y gestión de los riesgos se debe realizar de acuerdo con el procedimiento de gestión de riesgos de la CGR. Los resultados del análisis y gestión de riesgos se deben documentar de acuerdo con el procedimiento de gestión de riesgo de la CGR.

En los contratos celebrados con proveedores de servicios de computación en la nube se debe incluir la necesidad de cumplir las políticas y requisitos de seguridad de la información de la CGR, el cumplimiento de los acuerdos de niveles de servicio, responsabilidades legales y derechos de propiedad intelectual sobre la información, leyes y regulaciones sobre la protección de la información de la CGR e información de carácter personal.

Los servicios en la nube utilizados por la DIARI en su operación deben seguir los lineamientos establecidos para la infraestructura On Premise y desplegar validaciones de cumplimiento de seguridad basado en la ISO 27001.

Los servicios en la nube utilizados por la DIARI no deben almacenar o disponer información que pueda poner en riesgo la seguridad nacional o desestabilizar las entidades del orden nacional que disponen su información para la operación de la DIARI.


La DIARI y la OSEI son los responsables de la identificación, gestión y tratamiento de los riesgos asociados al uso de servicios de computación en la nube.

La Mesa Técnica de Seguridad debe coordinar y garantizar la ejecución de pruebas de seguridad tipo Ethical Hacking sobre los servicios en la nube prestados por terceros, los hallazgos encontrados en estas valoraciones de seguridad deben ser gestionados y resueltos de inmediato por parte de los proveedores de servicios cuando sea aplicable.

Todos los usuarios de servicios de computación en la nube deben aplicar y cumplir los lineamientos de seguridad de la información que se definan en la CGR para el uso seguro de ese tipo de servicios de tratamiento de información.

Los proveedores de servicios en la nube deben garantizar que las ubicaciones geográficas en donde se almacene información de tipo personal cuenten con leyes de protección de datos personales ampliamente aplicados sobre los procesos, instalaciones y actividades implícitas dentro de la prestación del servicio.

Los proveedores de servicios en la nube deben contar con políticas, prácticas y controles robustos de seguridad tanto al interior de sus procesos como en la infraestructura y plataforma tecnológica sobre la cuál presten sus servicios, de

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 57 de 71

igual forma deben certificar que cuentan con las mejores prácticas internacionales de seguridad en pro de evaluar el cumplimiento de los requisitos de seguridad acordados contractualmente.

7.12 Política Operativa de Adquisición, Desarrollo y Mantenimiento de Sistemas de Información³³

La seguridad de la información es parte integral de los sistemas de información de la DIARI y debe ser considerada durante todo el ciclo de vida de desarrollo del software bien sea a través de desarrollo interno o dentro de un proceso de adquisición.

7.12.1 Responsabilidad y Propiedad de los Sistemas de Información y Desarrollos de Software

Todos los sistemas de información o desarrollos de software deben tener un responsable dentro de la Dirección de Información Análisis y Reacción Inmediata.

El responsable del sistema de información o desarrollo de software debe definir qué información puede ser eliminada de los ambientes de prueba y desarrollo, y solicitar los soportes de la eliminación a personal interno o de terceros como seguimiento y trazabilidad de la transparencia de la gestión de desarrollo.

El responsable del sistema de información o del desarrollo de software debe definir qué usuarios de la DIARI y externos podrán acceder a los mismos para que se gestione los permisos necesarios y suficientes a los recursos solicitados.


Todo usuario externo a la CGR deberá firmar un acuerdo de confidencialidad previo a la entrega de los accesos solicitados y los usuarios de la CGR externos de la DIARI deberán tener permiso de acceso que se concederá a través del Director (a) de la DIARI o los Jefes de la Unidad en la cual se opere y desarrolle el sistema de información o desarrollo de software.

Los desarrollos nuevos o inclusión de nuevas funcionalidades que impacten la operación de los sistemas de información deben someterse a pruebas unitarias de funcionalidad por parte de los propietarios o por aquellos que éste designe, para asegurar que cumplen con las funcionalidades requeridas. El equipo de seguridad de información de la DIARI validará que las funcionales de seguridad definidas ambas condiciones deben cumplirse antes del paso a producción.

Los propietarios de los sistemas de información deben aprobar las migraciones entre los ambientes de desarrollo, pruebas y producción de sistemas de información nuevos y/o de cambios, posterior a la evaluación y aval del resultado de las pruebas unitarias de funcionalidad y seguridad³⁴, teniendo en cuenta el documento Procedimiento de gestión de cambios de la CGR.

³³ Dominio de control A14 Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información, Anexo A Norma ISO 27001

³⁴ Dentro de las pruebas se podrán considerar la instalación, volumen, stress, rendimiento, almacenamiento, configuración, funcionalidad, seguridad y recuperación ante errores.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 58 de 71

Los responsables de los sistemas de información de la DIARI deben contar con un registro de versiones para administrar los cambios realizados en los sistemas de Información.

Todo software, aplicación, herramienta, utilidad, etc., elaborada por los funcionarios de la DIARI con recursos de la entidad es propiedad de la CGR.

7.12.2 Análisis y Especificación de Requisitos de Seguridad de la Información

La Dirección de Información Análisis y Reacción Inmediata debe verificar el uso de metodologías para el desarrollo de software, que incluyan la definición de requerimientos 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.

El responsable del sistema de información o desarrollo de software en acompañamiento con el equipo de seguridad de la información de la DIARI y de la OSEI deben identificar, establecer, valorar y documentar los posibles riesgos de seguridad que se puedan derivar de la adquisición o desarrollo considerando los requerimientos de seguridad necesarios para la entrada a producción del desarrollo.

Los desarrolladores deben certificar que todo sistema de información entregado para la DIARI utiliza herramientas, componentes o complementos licenciados. En el evento en que se use software libre este deberá ser reconocido en el mercado y debe ser utilizada su versión más reciente comunicando y documentando al equipo de seguridad de la DIARI, para que se hagan las validaciones y se evalúe de manera conjunta con la OSEI los controles de seguridad a implementar para remediar las vulnerabilidades identificadas.

Se debe considerar realizar una evaluación de los sistemas de información o desarrollos en busca de vulnerabilidades, manteniendo un registro de los resultados y las acciones correctivas a ejecutar.³⁵


Los administradores de infraestructura de la DIARI apoyados con la OSEI deben 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.

El equipo de seguridad de la información de la DIARI debe validar de manera conjunta con la OSEI que los componentes requeridos para la operación de los sistemas de información de la DIARI cuenten con las últimas actualizaciones de seguridad.

Los sistemas de información y cualquier desarrollo deben contar con manejo de roles con permisos de acceso y operaciones asociados a estos.

Los sistemas de información y cualquier desarrollo deben restringir toda ejecución de comandos directamente en el sistema operativo.

³⁵ Se podrán considerar análisis estático y dinámico de código.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 59 de 71

7.12.3 Separación de Ambientes

Los desarrolladores internos o externos deben mantener tres ambientes independientes: desarrollo, pruebas y producción de tal forma que el desempeño y la seguridad de un ambiente no influya en los demás.

Los ambientes de desarrollo, pruebas y producción deben considerar:

- En el ambiente de desarrollo y pruebas se podrá disponer de herramientas y utilitarios necesarios para el desarrollo de su actividad, sin embargo, estas estarán restringidas en los ambientes de producción.
- El ambiente de pruebas debe ser una réplica del ambiente de producción en lo que respecta a programas y condiciones de ejecución. No obstante, no se deberán utilizar para pruebas copias de datos de producción y las credenciales de control de acceso deben ser diferentes e independientes para cada uno de ellos.

El personal que realiza funciones asociadas a un ambiente específico (desarrollo, pruebas y producción) debe contar con perfiles de acceso que limiten sus actividades exclusivamente al ambiente en el que trabajan.

Los usuarios y los operadores de los sistemas de información no deben tener acceso a programas fuente o utilitarios propios del ambiente de desarrollo ni a líneas de comando que puedan colocar en riesgo la seguridad de la información, del sistema de información, de cualquier componente asociado al mismo y de la plataforma.


7.12.4 Datos de Prueba

Cada responsable de los sistemas de información o desarrollo de software debe definir qué tipo de datos o información es requerida para las pruebas operativas con el fin de someter la información que no sea de naturaleza pública a un proceso de protección, tales como enmascaramiento, ofuscación y/o disociación de datos, manteniendo la estructura necesaria para poder realizar las pruebas requeridas.

La información que se entregue para las pruebas deberá ser útil para las aplicaciones, pero deberá impedir procesos inversos donde el dato sea revertido a su estado original.

El responsable del sistema de información o desarrollo de software debe definir qué información puede ser eliminada de los ambientes de prueba y desarrollo, y solicitar los soportes de la eliminación a personal interno o de terceros.

Este procedimiento debe ser debidamente documentado en formatos de control y seguimiento de la gestión realizada para verificación por parte de la DIARI.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 60 de 71

7.12.5 Seguridad de las Aplicaciones en Redes Públicas

El equipo de seguridad de la información de la DIARI debe hacer un seguimiento de las vulnerabilidades técnicas publicadas en los boletines de seguridad nacional o internacional, con el fin de evaluar a que vulnerabilidades está expuesta la red de transmisión de datos, las aplicaciones, sistemas operativos y los sistemas de información; para que se tomen las medidas necesarias para mitigar el riesgo asociado³⁶

Los desarrolladores deben entregar las recomendaciones para asegurar los canales y puertos a utilizar en la transmisión de información relacionada con las transacciones en línea efectuadas por el sistema de información.

Si se requiere el uso de cifrado de datos dentro de las transacciones en línea efectuadas por el sistema de información este deberá ceñirse a los lineamientos descritos en la política del uso de controles criptográficos.

Todos los recursos tecnológicos de la DIARI deben contar con mecanismos de seguridad implementados a nivel de sistemas operativos, redes, bases de datos, aplicativos y demás componentes de las soluciones de tecnologías de la información.

El administrador de cada sistema de información es responsable de asegurar que las contraseñas que se transmitan a través de redes públicas estén protegidas contra acceso no autorizado mientras se encuentren en tránsito, para este caso se recomienda sean cifradas.

Toda transferencia de información que se realice con un tercero debe estar protegida con un mecanismo de cifrado punto a punto.

7.12.6 Desarrollo Seguro

Todos los posibles riesgos que contenga el desarrollo de una aplicación deben ser identificados, valorados y documentados por los desarrolladores, la DIARI, la USATI, la OSEI y el área o persona que solicita el desarrollo y todas las partes interesadas.

Basados en los resultados del análisis y valoración de riesgos, se deben validar los controles de seguridad a considerar como parte de la especificación del software.

³⁶ Para ello se podrá consultar los siguientes enlaces:

<http://nvd.nist.gov/nvd.cfm>

<http://nvd.nist.gov/download.cfm#XML>


<http://nvd.nist.gov/cvss.cfm?calculator>

<http://xforce.iss.net/xforce/alerts>

<http://www.qualys.com/research/alerts/>

<http://tools.cisco.com/MySDN/Intelligence/home.x>

<http://www.nessus.org/plugins/>

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 61 de 71

El desarrollador debe documentar claramente el diseño para cumplir cada uno de los requisitos de seguridad. Esta documentación describirá los mecanismos de seguridad, el diseño debe especificar claramente si tales mecanismos vienen de software a la medida, software de terceros o de la plataforma.

Todos los desarrollos realizados tanto interna como externamente deben cumplir las políticas y lineamientos técnicos, de seguridad u otros emitidos por la DIARI.

Para cada uno de los desarrollos la DIARI se debe establecer un plan de pruebas de seguridad que defina cómo se realizarán las pruebas o bien establecer como cada uno de los requerimientos de seguridad va a ser cumplido. El desarrollador ejecutará el plan de prueba en el ambiente de pruebas antes de la implementación final y proveerá los resultados obtenidos.

En los procesos de desarrollo de software se establece condiciones para transferencia de los derechos de propiedad intelectual de código fuente, de acuerdo con lo establecido en la Ley 23 de 1982 sobre Derechos de autor, artículos 28 y 30 de la Ley 1450 de 2011 "Plan Nacional de Desarrollo 2010-2014" y la Circular 07 de 2002 de la Dirección Nacional de Derechos de Autor.

La identificación de las necesidades y requisitos de funcionalidad, calidad y seguridad, se documentan entre la DIARI y la OSEI. Los requerimientos del software se deben validar durante el proceso de aceptación del desarrollo de software.


Los requerimientos deben incluir una descripción detallada de todos los roles (grupos, privilegios, autorizaciones) usadas en la aplicación. Los requerimientos deben indicar todos los activos y funciones que provee la aplicación. Los requerimientos deben especificar detallada y exactamente los derechos de acceso para cualquier activo y función de cada rol.

Los requerimientos deben detallar como se van a manejar los errores que ocurran dentro del procesamiento. Algunas aplicaciones deberían hacer lo mejor posible en caso de un error, mientras que otras deberían terminar su procesamiento inmediatamente.

Los requerimientos deben especificar que eventos son relevantes para la seguridad y necesitan ser registrados, como ataques detectados, intentos de conexión fallidos e intentos de exceder la autorización. Los requerimientos deben especificar también que información registrar con cada evento, incluyendo hora y fecha, descripción del evento, detalles de aplicación, y demás información útil.

Los requerimientos deben especificar qué debe ser cifrado (datos, conexión, base de datos, aplicación), como serán cifrados y cómo deben ser manejados todos los certificados y otras credenciales. Las aplicaciones deben usar algoritmos estándar implementados en una librería de cifrado que haya sido usada y probada ampliamente.

Los requerimientos deben especificar como protegerse de ataques de denegación de servicio. Todos los posibles ataques en la aplicación deben ser considerados, incluyendo bloqueos de autenticación, agotamiento de conexiones y otros ataques de agotamiento de recursos.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 62 de 71

Los requerimientos deben incluir un conjunto de vulnerabilidades específicas que no deben estar presentes en el software. A menos que sea especificado de otra manera, el software no debe incluir ninguna de las fallas descritas en la "Lista de OWASP sobre las 10 vulnerabilidades más críticas en aplicaciones Web". (Open Web Application Security Project, proyecto de código abierto dedicado a determinar y combatir las causas que hacen que el software sea inseguro).

Los cambios requeridos sobre el software de la DIARI deben ser controlados y deben establecer los requerimientos y los niveles de aceptación del cambio. Dentro de los requerimientos de los cambios es necesario analizar los riesgos asociados a la seguridad de la información y la identificación de los controles a implementar para su adecuada gestión.

En el desarrollo de software se lleva a cabo un control de versiones con los respectivos documentos de soporte, con el objeto de verificar el buen funcionamiento del software y el respectivo control de su ciclo de vida

Los desarrolladores son responsables de implementar las medidas de seguridad establecidas.

7.13 Política Operativa de Gestión de Incidentes de Seguridad de la Información³⁷

Es responsabilidad de la DIARI, aplicar el procedimiento y el instructivo de manejo de incidentes de seguridad, actualizarlo y evaluar las acciones de mejora que se identifiquen del tratamiento de los incidentes de seguridad que sean detectados.


Todo el personal sea contratista de prestación de servicios o funcionario de la DIARI o que, por su relación con la CGR, tenga acceso a la información, activos de información o infraestructura de esta, al momento de tener conocimiento directo o indirecto, acerca de un evento o incidente de seguridad de la información, debe reportarlo de manera oportuna a los líderes de procesos o al Líder de Seguridad de la Información de la DIARI.

La USATI según sea el caso (incidente de seguridad de la información o informática), es el área competente para la atención al incidente reportado y ejecutará las labores propias de su gestión.

La gestión realizada en pro de dar respuesta al incidente de seguridad debe quedar registrada en los formatos y en la herramienta de gestión destinada para tal fin. Durante el análisis del incidente de seguridad se debe obtener la mayor cantidad de información que permita establecer las circunstancias de tiempo, modo y lugar de ocurrencia y frente a la posibilidad de que se materialicen futuros incidentes de seguridad, se conservará una base de datos con la gestión de conocimiento.

La información de los incidentes de seguridad es insumo para cualquier investigación de tipo legal por lo cual se debe salvaguardar en repositorios seguros.

³⁷ Dominio de control A16 Gestión de Incidentes de Seguridad de la Información, Anexo A Norma ISO 27001

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 63 de 71

La investigación del incidente de seguridad deberá ejecutarse por un equipo mínimo de dos (2) personas, que brinde un panorama más amplio de la situación, la identificación de evidencia y la respectiva cadena de custodia; con base a ello se determinará si la DIARI cuenta con los recursos técnicos y humanos para ejecutar la labor o si el servicio deberá ser suministrado por terceros especializados.

7.14 Política Operativa de Relaciones con los Proveedores³⁸

En el marco de los acuerdos contractuales con proveedores y/o aliados comerciales se deben observar los aspectos relacionados con la Seguridad de la Información para llevar a cabo la gestión de los servicios.

El acceso, administración, uso o tratamiento seguro de la información por parte de los proveedores es importante para mitigar los riesgos que se puedan presentar en la ejecución de las actividades por parte del mismo, disminuyendo el impacto que la materialización de los riesgos pueda tener en los activos de información de la DIARI.

El propietario del activo de información debe definir la finalidad de la autorización de acceso, administración, uso o tratamiento a la información que se otorgue al proveedor y documentar la autorización del acceso a los datos de acuerdo con el fin previsto; así como la debida implementación de los controles requeridos para preservar las características de confidencialidad, integridad y disponibilidad de la información.

Se debe tener en cuenta el nivel de clasificación del activo de información al cual se otorgará el acceso, administración, uso o tratamiento para establecer los controles de seguridad apropiados.


En ningún caso se otorgará acceso, administración, uso o tratamiento al activo de información, sistemas de información o áreas seguras de la DIARI a proveedores, hasta no haber realizado la adecuada gestión de los riesgos, formalizada la relación contractual y firmada el acuerdo de confidencialidad.

Dentro de los acuerdos, contratos o convenios formalmente firmados entre la DIARI y los proveedores se deben definir claramente los requerimientos de seguridad y privacidad tales como:

- Información a tratar
- Niveles de clasificación
- Finalidad
- Autorizados para el tratamiento
- Controles a tener en cuenta antes, durante y después del tratamiento de los datos por parte del proveedor, con el respectivo consentimiento por parte de los titulares en los casos que aplique.

Todos los proveedores que accedan administren, usen o traten activos de información deberán conocer y cumplir con las políticas de seguridad y privacidad de la información de la DIARI, así mismo, en caso de que identifiquen una

³⁸ Dominio de control A15 Relación con los Proveedores, Anexo A Norma ISO 27001

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 64 de 71

amenaza que pueda llegar a vulnerar la información, deberán reportarla a la DIARI o al supervisor del contrato, así como contar con políticas y medidas de seguridad propias para proteger los activos de la DIARI

7.15 Política Operativa de Aspectos de Seguridad de la Información de la Gestión de Continuidad de Negocio³⁹

La Gestión de Continuidad del Negocio es el conjunto de estrategias y procedimientos definidas para contrarrestar las interrupciones en las actividades misionales de la entidad, para proteger sus procesos críticos contra fallas mayores en la plataforma tecnológica o contra desastres, asegurando que las operaciones se recuperen oportuna y ordenadamente, generando un impacto mínimo o nulo ante una contingencia.

Se deberán prevenir interrupciones en las actividades de la plataforma informática de la DIARI que vayan en detrimento de los activos críticos de TI afectados por situaciones no previstas o desastres, que respondan asertiva y oportunamente ante eventos que afecten la continuidad de las operaciones de los procesos de Gestión de información y Análisis de información.

Se deberá desarrollar e implantar un plan de continuidad para asegurar que los procesos misionales de TI de la CGR podrán ser restaurados dentro de escalas de tiempo razonables.

La CGR deberá tener definida dentro de su estrategia, un plan de acción que permita mantener la continuidad del negocio teniendo en cuenta los siguientes aspectos:


- Identificación y asignación de prioridades a los procesos críticos de TI de la CGR de acuerdo con su impacto en el cumplimiento de la misión de la entidad.
- Determinación de los requisitos para la seguridad de la información y la continuidad de la gestión de seguridad de la información de la DIARI en situaciones adversas, por ejemplo, durante una crisis o desastre.
- Documentación de la estrategia de continuidad del negocio.
- Documentación del plan de recuperación del negocio de acuerdo con la estrategia definida anteriormente.
- Plan de pruebas periódico de la estrategia de continuidad del negocio y el plan de contingencia de la plataforma tecnológica de la CGR.

La continuidad del negocio es coordinada por la Unidad de Seguridad y Aseguramiento Tecnológico e Informático - USATI, siendo los responsables de velar por la implantación de las medidas relativas a ésta. Igualmente, serán responsables de desarrollar las tareas necesarias para el mantenimiento de estas medidas.

La USATI, se encargará de la definición y actualización de las normas, políticas, procedimientos y estándares relacionados con la continuidad del negocio, igualmente velará por la implantación y cumplimiento de las mismas.

Para la CGR su recurso más importante es el recurso humano y por lo tanto será su prioridad y objetivo principal protegerlo adecuadamente en cualquier evento. Los niveles de recuperación mínimos requeridos, así como los

³⁹ Dominio de control A17 Aspecto de Seguridad de la Información de la Gestión de la Continuidad del Negocio, Anexo A Norma ISO 27001

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 65 de 71

requerimientos de seguridad, funciones y responsabilidades relacionados con el plan, deberán estar incorporados y definidos en los planes de contingencias.

Es responsabilidad de la OSEI en compañía de la USATI mantener, mejorar y probar periódicamente los procedimientos de contingencia, recuperación ante desastres y continuidad en la prestación de servicios de tecnología.

La DIARI a través de su Líder de Seguridad de la Información y su equipo, deberán realizar una verificación a intervalos regulares de los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.

7.16 Política Operativa de Cumplimiento⁴⁰

Es responsabilidad de todo funcionario, contratista de prestación de servicios y tercero aplicar y mantener los acuerdos de confidencialidad sobre la información a su cargo.


Todos los funcionarios de la DIARI se comprometen a cumplir las leyes, normas, políticas, directrices y procedimientos a los que está sometida la Entidad para la protección de la información a su cargo.

La DIARI identificará y mantendrá actualizada la relación de requisitos legales que le sean de aplicación en materia de seguridad de la información. De esta forma, podrá incluir en los contratos, licencias y acuerdos que establezca con terceros, el cumplimiento obligatorio por parte de estos de las normas de seguridad corporativas, las cláusulas relativas a la propiedad intelectual, los derechos de explotación, confidencialidad y no divulgación, así como los requerimientos de seguridad exigibles por imperativos legales o regulatorios que sean de aplicación.

El cumplimiento de las Políticas de Seguridad de la Información es de carácter obligatorio, cada uno de los funcionarios, contratistas de prestación de servicios y/o terceros debe comprender su rol y asumir su responsabilidad respecto a los riesgos en Seguridad de la Información y la protección de los activos de información a su cargo.

El incumplimiento de las Políticas de Seguridad de la Información que comprometa la confidencialidad, disponibilidad e integridad de la información puede resultar en una acción disciplinaria o en acciones legales que apliquen a la normatividad del Gobierno Nacional y Territorial en cuanto a seguridad y privacidad de la información.

⁴⁰ Dominio de control A18 Cumplimiento, Anexo A Norma ISO 27001

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 66 de 71

7.17 Política Operativa de Propiedad Intelectual⁴¹

Se podrá hacer la instalación de todo software incluido en las listas blancas⁴² definidas por la Mesa Técnica de Seguridad de la CGR.

Está permitido el uso de software licenciado y/o aquel que puede ser usado bajo licencias de uso comercial para entornos empresariales, siempre y cuando esta no infrinja ningún derecho de autor y sea revisado y autorizado por el grupo de seguridad de la información.

Todo software instalado y utilizado en los equipos propiedad de la DIARI o aquellos utilizados en nombre de ella, deben cumplir con los principios constitucionales, los acuerdos internacionales y la legislación nacional vigente sobre derechos de autor, y en todo caso está sujeto al respeto de los derechos o voluntad expresada por el autor en documentos físicos o digitales de licenciamiento.

Los funcionarios, contratistas de prestación de servicios y terceros no tendrán acceso a instalación de programas o a realizar copia de los productos de software puestos a su disposición para el desempeño de sus tareas.

Los funcionarios, contratistas de prestación de servicios y terceros son responsables por las sanciones disciplinarias, civiles y/o penales por el uso de software ilegal, productos no licenciados o no autorizados.

Los funcionarios, contratistas de prestación de servicios y terceros no deberán copiar total ni parcialmente libros, artículos, reportajes u otros documentos diferentes de los permitidos por la ley de derechos de autor.


La DIARI mantendrá un inventario actualizado del software autorizado donde se registrará como mínimo:

- Nombre del Software
- Tipo de licencia
- Cantidad de licencias
- Documentos soporte de la licencia
- Documento de transferencia de derechos de autor para los desarrollos internos o contratados.

La DIARI realizara revisiones periódicas internas para verificar que el software instalado este autorizado y debidamente licenciado.

⁴¹ Dominio de control A18 Cumplimiento, Anexo A Norma ISO 27001

⁴² Lista blanca: Es un registro que define el software autorizado para instalación, ejecución y uso sobre los equipos de cómputo conectados a la red de la entidad.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 67 de 71

7.18 Política Operativa de Protección para BYOD⁴³

Esta política se aplica a todos los dispositivos electrónicos personales tales como teléfonos inteligentes, tabletas y computadores portátiles que no pertenecen la CGR pero que son utilizados para las funciones propias del cargo de los servidores públicos de la DIARI que usen en sus dispositivos personales la información de la entidad: Empleados públicos de planta (carrera administrativa, provisionales, funcionarios de libre nombramiento y remoción), trabajadores oficiales, contratistas de prestación de servicios y demás personal, para acceder o almacenar información de la DIARI. A estos dispositivos se les conoce comúnmente dentro del área de seguridad informática como BYOD (Bring Your Own Device).

La política define las medidas necesarias para evitar que la información reservada o pública clasificada de la DIARI se vea comprometida en su integridad y confidencialidad al ser almacenada en dispositivos ajenos a la entidad.

La DIARI identificará y gestionará los riesgos inmersos en el uso de los equipos personales, estableciendo los límites y medidas de seguridad necesarias para evitar la afectación de la confidencialidad, integridad y disponibilidad de la información cuando es manejada a través de estos equipos. Para el uso de los equipos personales en modalidad BYOD se deben cumplir los siguientes lineamientos:

Se restringe el acceso a través de dispositivos móviles a la infraestructura tecnológica On Premise y en la nube de la DIARI, salvo los servicios de aplicaciones incluidas en Microsoft Office 365.


Los dispositivos personales que requieran acceder a internet deben hacerlo a través de una red diferente de la DIARI, en una zona independiente del Firewall desde la cual se restrinja el acceso a sistemas informáticos y redes internas de la entidad, junto con la habilitación de funciones de auditariedad y registro (logs) de todas las actividades realizadas desde estos dispositivos.

Sobre los dispositivos móviles personales tipo Smartphone y tabletas autorizados en modelo BYOD, se deben aplicar medidas de seguridad como la protección de acceso a través de contraseñas robustas, cifrado de memoria para los repositorios en donde se almacene información de la DIARI, el uso de antivirus y el control seguridad y reputación de las aplicaciones instaladas en dichos dispositivos; el funcionario es el responsable de garantizar que las aplicaciones instaladas en el dispositivo son confiables y que fueron descargadas de repositorios reconocidos y seguros.

El funcionario, contratista de prestación de servicios o tercero al que se autorice un BYOD debe garantizar bajo acuerdo de confidencialidad que la información de la DIARI reservada o información pública clasificada correspondiente a sus labores asignadas será almacenada de forma aislada a la información personal que guarde en su dispositivo.

En los BYOD utilizados por los funcionarios en la medida de la posible se debe manejar cifrado para la información de la DIARI de acuerdo con la política de controles criptográficos y lineamientos del Sistema de gestión de seguridad en materia de información.

⁴³ Dominio de control A6 Organización de la Seguridad de la Información, Anexo A Norma ISO 27001

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 68 de 71

El usuario al que se le autorice el uso de BYOD debe cumplir con la reglamentación vigente en materia de uso de software legal. El usuario es enteramente responsable de contar con todo el software de su dispositivo debidamente licenciado.

Todo dispositivo BYOD debe cumplir con todos los lineamientos de seguridad del Sistema de gestión de seguridad en materia de información.

La DIARI debe contar con la autorización del propietario del dispositivo para instalar software o agentes de administración para prevenir la divulgación de información reservada o publica clasificada de la CGR en caso de robo o extravío del dispositivo.

Todo dispositivo BYOD debe tener las aplicaciones de software debidamente actualizadas y en correcto funcionamiento para evitar la exposición de vulnerabilidades que una vez explotadas puedan permitir el acceso no autorizado o el ingreso y la manipulación externa de código malicioso. El propietario del dispositivo es responsable de suministrar y mantener al día dicho software.

Los jefes de las unidades de Información y Análisis de Información, respectivamente, con el líder de Seguridad de la Información de la DIARI determinarán para cuales procesos (Gestión de Información y Análisis de Información) y bajo qué circunstancias se autorizará el uso de dispositivos personales que no pertenecen a la entidad (BYOD) para almacenar o procesar información institucional reservada o información pública clasificada, así como la aplicación de las políticas de seguridad requeridas para proteger la información que se almacene y gestione en el dispositivo personal del funcionario, contratista de prestación de servicios o tercero.


La OSEI a través de la USATI definen las características y condiciones mínimas que requieren los equipos personales para que puedan acceder a la información o recursos informáticos de la DIARI, estas características contemplan el tipo de dispositivos, el procesamiento, la memoria, las versiones de sistema operativo, necesarias para que puedan operar con un desempeño adecuado luego de la aplicación de medidas de seguridad como el cifrado de repositorios de almacenamiento o uso de antivirus.

La OSEI verifica que los dispositivos cumplen las características y condiciones mínimas dispuestas en esta política, en caso contrario se debe rechazar la conexión de dicho dispositivo.

Los líderes de los procesos deben conocer y velar por que los lineamientos de seguridad de los dispositivos BYOD se apliquen preservando la seguridad de la información de la DIARI y respetando el derecho fundamental a la Intimidad y privacidad del propietario del dispositivo.

El propietario del dispositivo debe aplicar todas las medidas de seguridad mínimas exigidas por OSEI que estén a su alcance para preservar la integridad y el acceso restringido a la información que se encuentre en su dispositivo personal.

En caso de robo o pérdida de un dispositivo personal que ha tenido acceso a la red de la CGR, el propietario del mismo debe informar inmediatamente al responsable del área o proceso, a la OSEI, a la USATI y a la autoridad competente.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 69 de 71

Los líderes de los procesos de la DIARI con apoyo de la OSEI pueden realizar periódicamente revisiones a los equipos BYOD para certificar que están cumpliendo con las políticas de seguridad de la Información de la CGR, las revisiones preservaran el derecho fundamental a la Intimidad del usuario del BYOD y las normas sobre Protección de Datos de carácter personal.

Cualquier excepción a las políticas o lineamientos de este documento debe ser presentada, revisada y aprobada por la OSEI y la DIARI.

7.19 Política Operativa de Trabajo en Casa⁴⁴

Aplica a todos los funcionarios de carrera, libre nombramiento y remoción o provisionales que se encuentren autorizados para realizar actividades de trabajo en casa. Estos deberán preservar la confidencialidad de la información de la DIARI, los cuales están sujetos a los mismos requerimientos de seguridad establecidos para el trabajo en sitio obligándose a proteger y cumplir los acuerdos de confidencialidad durante y una vez terminada su relación laboral y/o contractual con la CGR.

La DIARI autoriza la realización de actividades laborales en modalidad de trabajo en casa conforme a las condiciones de seguridad establecidas por la Mesa Técnica de Seguridad.

Sobre las actividades laborales en modalidad de trabajo en casa la DIARI debe analizar los riesgos y la OSEI establecer controles tecnológicos de seguridad acordes con las políticas de seguridad y privacidad de la información de la DIARI.


El acceso a los servicios de red de los usuarios autorizado por la DIARI para que realicen trabajo en casa debe darse de manera remota mientras este activo el evento o situación crítica Local, Regional, Nacional o internacional, o cuando sea estrictamente necesario cumpliendo las políticas y controles de seguridad de la información establecidos en la conexión y en el tratamiento de la información.

Para realizar las actividades de trabajo en casa debe definirse:

El dispositivo de cómputo desde el cual realizara las actividades, este debe cumplir con las políticas y controles de seguridad de la información establecidos por la DIARI.

- El método de conexión para acceder a la información o sistemas de información.
- El alcance de las actividades a desarrollar y se determinaran como mínimo:
 - La información o sistemas de información a los que accederá.
 - El horario en el que realizara las actividades.

⁴⁴ Dominio de control A6 Organización de la Seguridad de la Información, Anexo A Norma ISO 27001

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 70 de 71

Antes de iniciar las actividades de trabajo en casa se deberá realizar un análisis de riesgos, a partir del cual se establezcan los controles para la protección de la información y los sistemas de información de la DIARI accedidos durante las actividades.

El área de Talento Humano determinará las condiciones de los contratos o acuerdos con los funcionarios, contratistas de prestación de servicios y terceros autorizados para laborar en la modalidad de trabajo en casa, determinando las condiciones, responsabilidades conforme las necesidades de la DIARI y la normatividad colombiana vigente.

Las Unidades de Análisis, información y Reacción Inmediata deben suministrar a la OSEI la información de los funcionarios o contratistas de prestación de servicios que realizarán actividades de trabajo en casa, para que se establezcan las condiciones técnicas y los accesos a la información o sistemas de información requeridos.

La DIARI en apoyo con la OSEI y la USATI son los responsables de implementar los controles de seguridad necesarios para llevar a cabo las actividades de trabajo en casa.

Los funcionarios, contratistas de prestación de servicios y terceros que se encuentren autorizados para el desarrollo de actividades de trabajo en casa, deben cumplir estrictamente con las responsabilidades y políticas de seguridad de la información de la DIARI.


En caso de pérdida, hurto o que se presuma que se ha vulnerado la seguridad del equipo de cómputo en el cual se desarrollan las actividades de trabajo en casa, será responsabilidad del funcionario, contratista de prestación de servicios o tercero informar de forma inmediata a la DIARI el evento, con el fin de establecer las medidas de seguridad adecuadas para la protección de la información contenida.

La OSEI es la responsable de implementar protocolos que den respuesta a situaciones de alerta de riesgo de seguridad o falla en los equipos autorizados para actividades de trabajo en casa.

La OSEI bajo la supervisión de la DIARI debe gestionar las conexiones remotas si está seguro de que se aplican correctamente las medidas de seguridad exigidas, tal como:

- Los equipos utilizados para el desarrollo de las actividades de trabajo en casa deberán contar con software operativo y ofimático debidamente licenciado y sistema de antivirus, el acceso a los recursos tecnológicos de la CGR se hará por medio de VPN para aquellos equipos que cumplan con las políticas de seguridad y tenga los agentes de antivirus debidamente operativos y actualizados.
- Los permisos de acceso a los usuarios en trabajo en casa deben ser correspondientes y restringidos hacia únicamente la información y las funciones necesarias para el desarrollo de las actividades laborales en coherencia con la política de control de acceso a la información.

Toda actividad propia a las funciones relacionadas con la DIARI, que generen un producto nuevo y realizado en la modalidad de trabajo en casa será propiedad intelectual de la DIARI.

	Sistema de Gestión y Control Interno - SIGECI			
	Macroproceso: Gestión del riesgo, seguridad y continuidad del negocio - RSC		Proceso: Gestión Integral de seguridad	
	Políticas Operativas de Seguridad de la Información en la Operación de los procesos Gestión de información y Análisis de información en la DIARI			
	Código: RSC 02 PO 001	Versión: 1.0	Fecha de Publicación en el Aplicativo SIGECI: 29/06/2022	Página 71 de 71

Los funcionarios que se encuentren autorizados para el desarrollo de actividades de Trabajo en casa deberán cumplir con las responsabilidades y condiciones acordadas, así mismo reportar a través de la mesa de servicio cualquier situación que pueda afectar el desarrollo de las actividades o ponga en peligro la información de la CGR.

La DIARI realizara campañas de sensibilización para las buenas prácticas de las actividades de trabajo en casa.

La OSEI es la responsable de facilitar los canales de comunicación y métodos de autenticación apropiados para controlar el acceso de usuarios remotos a la información y sistemas de información de la DIARI.

La Mesa Técnica de Seguridad es la responsable de establecer protocolos que den respuesta a situaciones de alerta como un daño o mal funcionamiento del equipo de cómputo asignado causado por un virus, una configuración incorrecta o un fallo de hardware de los equipos autorizados para labores de Trabajo en casa. Estas acciones deben quedar documentadas y hacer parte del registro de gestión de eventos e incidentes de seguridad de la CGR.

8. Anexos, plantillas y formatos

Formato Matriz Requisitos Legales aplicables en el SGS

9. Vigencia, derogatorias y transición

Este documento tiene vigencia a partir de la fecha de la comunicación a todos los servidores públicos y contratistas de prestaciones 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)
Nicolás G. Morales C, Profesional universitario Grado: 02, Argenis Soler Villanueva, Profesional universitario Grado: 02, Fredy Jiménez, profesional Especializado Grado 04, César Augusto Portilla Moya Asesor del Despacho 02 de la Unidad de Información de la Dirección de Información, Análisis y reacción inmediata- DIARI	Hoslander Sáenz, jefe Unidad de Información, de la Dirección de Información, Análisis y reacción inmediata - DIARI	Líder de Proceso Gestión Integral de Seguridad: Margarita María Márquez Figueroa, Directora de La Unidad de Seguridad. Aseguramiento Tecnológico e Informático - USATI Líder del Macroproceso de Gestión de Riesgos, Seguridad y Continuidad del Negocio: José Antonio Poveda Montes, Jefe Unidad de Seguridad, Aseguramiento, Tecnológico e Informático – USATI y Vanessa Varón Garrido- Directora Oficina de Planeación	Paola Tatiana Tovar, Contratista y Sandra Rodríguez, Profesional de la Oficina de Planeación	José Neheman Gómez Lozada, Asesor de Gestión Oficina Planeación	Vanessa Varón Garrido Directora Oficina de Planeación