CONTRALORÍA
GENERAL DE LA REPÚBLICA

100 AÑOS
Defender juntos los recursos públicos ¡Tiene Sentido!

Inducción/Reinducción Servidores Públicos de la CGR

Unidad de Seguridad y Aseguramiento Tecnológico e Informático
-USATI-

2023

NORMATIVIDAD DE LA USATI

ARTÍCULO 128, LEY 1474 DE 2011

Se crean dentro de la estructura de la Contraloría General de la República diversas dependencias, entre ellas la Unidad de Seguridad y Aseguramiento Tecnológico e Informático –USATI –, con el fin de fortalecer las acciones en contra de la corrupción.

Consulta el texto del artículo 128 de la Ley 1474 en https://cutt.ly/N9nVQI1

RESOLUCIÓN REG-205 DE 2012

Determina el funcionamiento interno de la Unidad de Seguridad y Aseguramiento Tecnológico e Informático –USATI–, y de sus direcciones.

Consulta el texto de la Resolución Reglamentaria REG-205 de 2012 en https://cutt.ly/D9mtLZp

RESOLUCIÓN OGZ-0765 DE 2020

Se designa a la **USATI** como Oficial de Protección de Datos Personales de la CGR.

Consulta el texto de la Resolución Organizacional OGZ-0765 de 2020 en https://cutt.ly/N9mypNS

RESOLUCIÓN OGZ-0817 DE 2022

Se establece el alcance del Sistema de Gestión de Seguridad y reglamenta el Gobierno de Seguridad de la Información y el rol de Oficial de Seguridad de la Información de la CGR (CISO, por sus siglas en inglés) y se dictan otras disposiciones.

Consulta el texto de la Resolución OGZ-0817 de 2022 en https://cutt.ly/A9LCILE

Consulta la normatividad asociada con la USATI, en https://cutt.ly/u9nVKvc

DATOS PERSONALES

LEY 1581 DE 2012

“Por la cual se dictan disposiciones generales para la protección de datos personales”.

LEY 1712 DE 2014

"Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones”.

DECRETO 1074 DE 2015

“Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio Industria y Turismo".

Ley 599 de 2000

Código Penal, Art. 269F sobre el delito de "violación de datos personales”.

Guía para la Gestión de Incidentes de Seguridad en el Tratamiento de Datos Personales -expedida por la SIC.

Circular Externa No. 003 de 2018

Registro Nacional de Bases de Datos, -expedida por la SIC.

Guía sobre el tratamiento de datos personales en las entidades estatales -expedida por la SIC.

Conoce más sobre lo que hace la USATI en https://cutt.ly/W9mgG0A

¿QUÉ HACE LA USATI?

- La USATI tiene un rol estratégico dentro de la seguridad de personas, bienes e información para toda la Entidad.
- Define e implementa políticas de seguridad de personas, bienes e información.
- Define e implementa la Política de Tratamiento de Datos Personales de la Entidad.
- Tiene a cargo los roles de Oficial de Seguridad de la Información de la CGR y de Oficial de Protección de Datos Personales de la CGR.
- Implementa, administra y gestiona la seguridad física de la CGR.

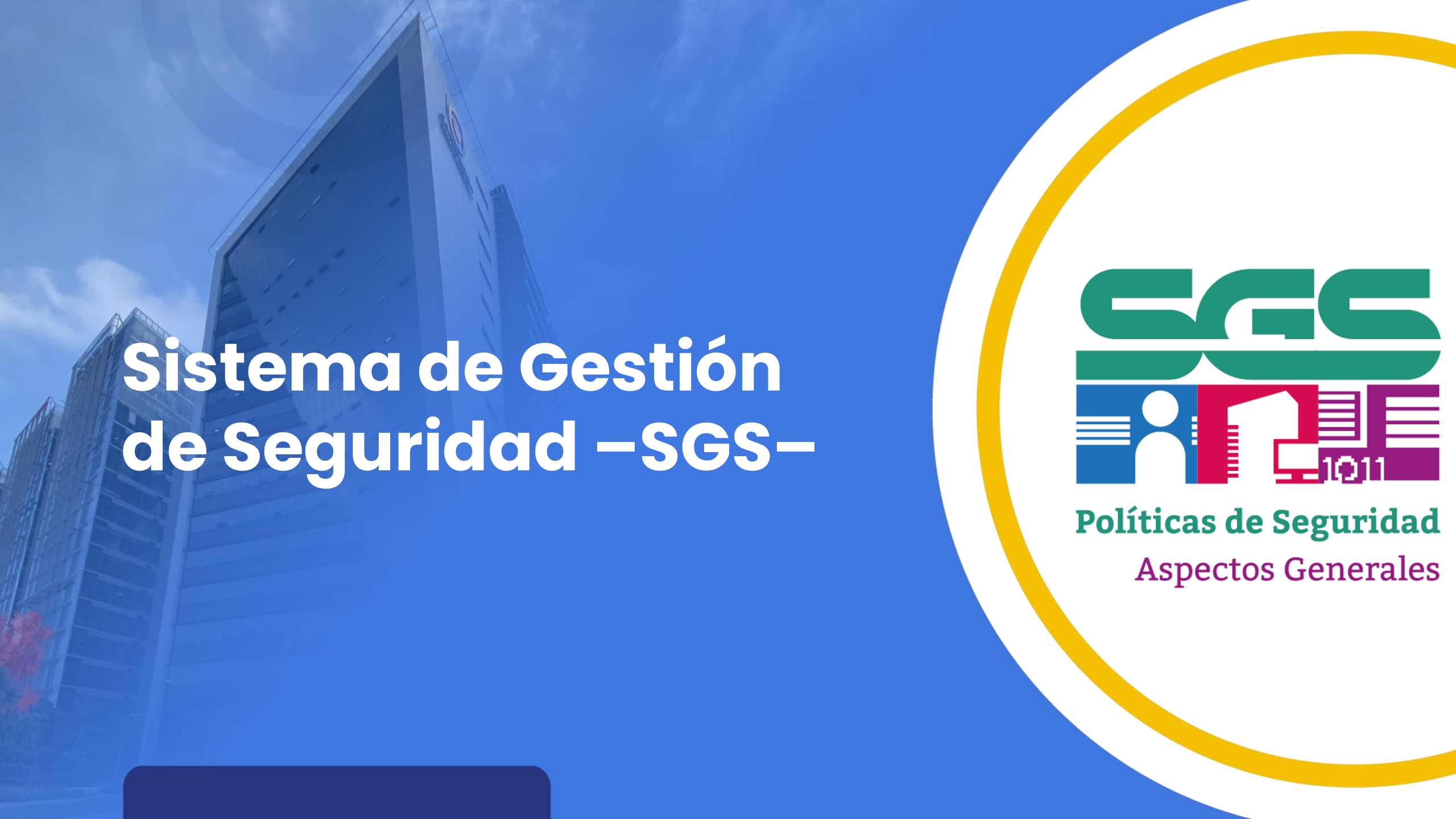
Conoce más sobre lo que hace la USATI en https://cutt.ly/W9mgG0A

SERVICIOS DE LA USATI

la USATI en su contexto legal y estructura tiene a su cargo la seguridad de personas, bienes e información institucionales.

Modelo del Sistema de Gestión de Seguridad - **SGS**

- Programa de Protección y Seguridad para los servidores públicos de la CGR en ejercicio de sus funciones.
- Coordinaciones de seguridad para las comisiones de servidores públicos a las diversas zonas del país.
- Gestión de incidentes de seguridad de personas, bienes e información.
- Análisis de hojas de vida de contratistas y terceras partes.
- Visitas de acompañamiento y seguimiento en las Gerencias Departamentales Colegiadas.
- Trámite y expedición de carné y de paz y salvos de elementos de seguridad.



Sistema de Gestión de Seguridad –SGS–

Políticas de Seguridad

Aspectos Generales

Sistema de Gestión de Seguridad –SGS –

Es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de personas, bienes e información institucionales.

Comprende las políticas de seguridad institucionales, procesos, procedimientos, guías, y otros tipos documentales, relacionados con la seguridad de las personas, los bienes y la información de la Entidad, siendo el marco de referencia para el quehacer seguro de las actividades institucionales.

Para mayor información y aspectos relacionados, consulta los siguientes vínculos:

- https://www.contraloria.gov.co/web/guest/politicas-de-seguridad-y-condiciones-de-uso
- https://congenrep.sharepoint.com/sites/IntranetUSATI

Políticas de Seguridad Institucionales

Propósito de las Políticas de Seguridad Institucionales

1. Establecer un marco de referencia para el gobierno de seguridad de personas, bienes e información en la CGR.
2. Establecer el marco general de seguridad para el tratamiento de Datos Personales.
3. Establecer un nivel estratégico de seguridad para que sea adoptado en el nivel táctico y operativo dentro de la Entidad.

Tipos de Políticas de Seguridad Institucionales

- Seguridad de Personas
- Seguridad de Bienes
- Seguridad de la Información
- Tratamiento de Datos Personales

Políticas que tienen mayor impacto en el quehacer institucional:

Como servidores públicos de la CGR, debemos conocer y aplicar todas las 31 Políticas de Seguridad Institucionales y su normatividad relacionada; no obstante, las que mayor impacto tienen en el quehacer institucional diario, son las siguientes:

Política de Datos Personales
(Página 3)

Política de Control de Acceso
(Página 13)

Política de Escritorio Limpio y Pantalla Limpia
(Página 16)

Política de Seguridad de los Bienes
(Página 12)

Política de Gestión de Incidentes
(Página 28)

Política de responsabilidad por los Activos
(Página 10)

Política de seguridad de Personas
(Página 9)

Consulta todas nuestras Políticas de Seguridad Institucionales en: https://cutt.ly/99mVOoQ

Compromiso de Confidencialidad:

Es tu deber como servidor público o contratista, conocer y aceptar el **Compromiso de Confidencialidad** de la **CGR**.

¿Qué es el Compromiso de Confidencialidad ?

Es un documento por medio del cual te comprometes a:

No divulgar, ni compartir información de la CGR;

Cumplir, respetar y preservar la **confidencialidad**, **integridad** y **disponibilidad** de la información que conoces en virtud de tus funciones.

¿Cuál es su Importancia?

Es muy importante, ya que busca proteger la información que administra la **CGR**, la cual es el activo que sustenta la operación de la Entidad y es propiedad exclusiva de la **CGR**.

¡Recuerda!

El incumplimiento total o parcial del compromiso de confidencialidad puede dar lugar al inicio de acciones disciplinarias y/o penales y/o la aplicación de las sanciones previstas en la ley.

Conoce, diligencia y acepta el *Compromiso de Confidencialidad* de la CGR en https://cutt.ly/t9mNp1H

Programa de Protección y Seguridad de los Servidores Públicos de la CGR.

¿Cómo se crea el Programa de Protección y Seguridad de los Servidores Públicos de la CGR?

Conforme lo establecido en los artículos 7º y 8º del Decreto 2037 de 2019, la CGR expide la Resolución Organizacional OGZ-0758 de 2020 que *crea el "Programa de Protección y Seguridad del Contralor General de la República, los excontralores generales de la República y demás servidores de la Contraloría General de la República; se adoptan lineamientos técnicos para el programa y se modifica la conformación y funciones del Comité de Seguridad".*

Consulta el texto de los artículos 7º y 8º del Decreto 2037 de 2019 en https://cutt.ly/E9mj0Bw
Consulta el texto de la Resolución Organizacional OGZ-0758 de 2020 en https://cutt.ly/k9mkdyh

¿Cuáles son los niveles de riesgo de los servidores públicos de la CGR?

MÍNIMO

- Hecho de nacer.
- Conducta responsable e irresponsable.

ORDINARIO

- Vivir en sociedad.
- Hechos naturales.

EXTRAORDINARIO

- No tiene deber jurídico de tolerar.
- Presente, excepcional, concreto, especifico, claro, desproporcionado, serio, importante.

EXTREMO

- Vulnera la vida de integridad persona.
- Grave e inminente.

Para mayor información, consulta la Guía de Buenas Prácticas y Recomendaciones de Seguridad y Autoprotección de la CGR en https://cutt.ly/J9mKPkA

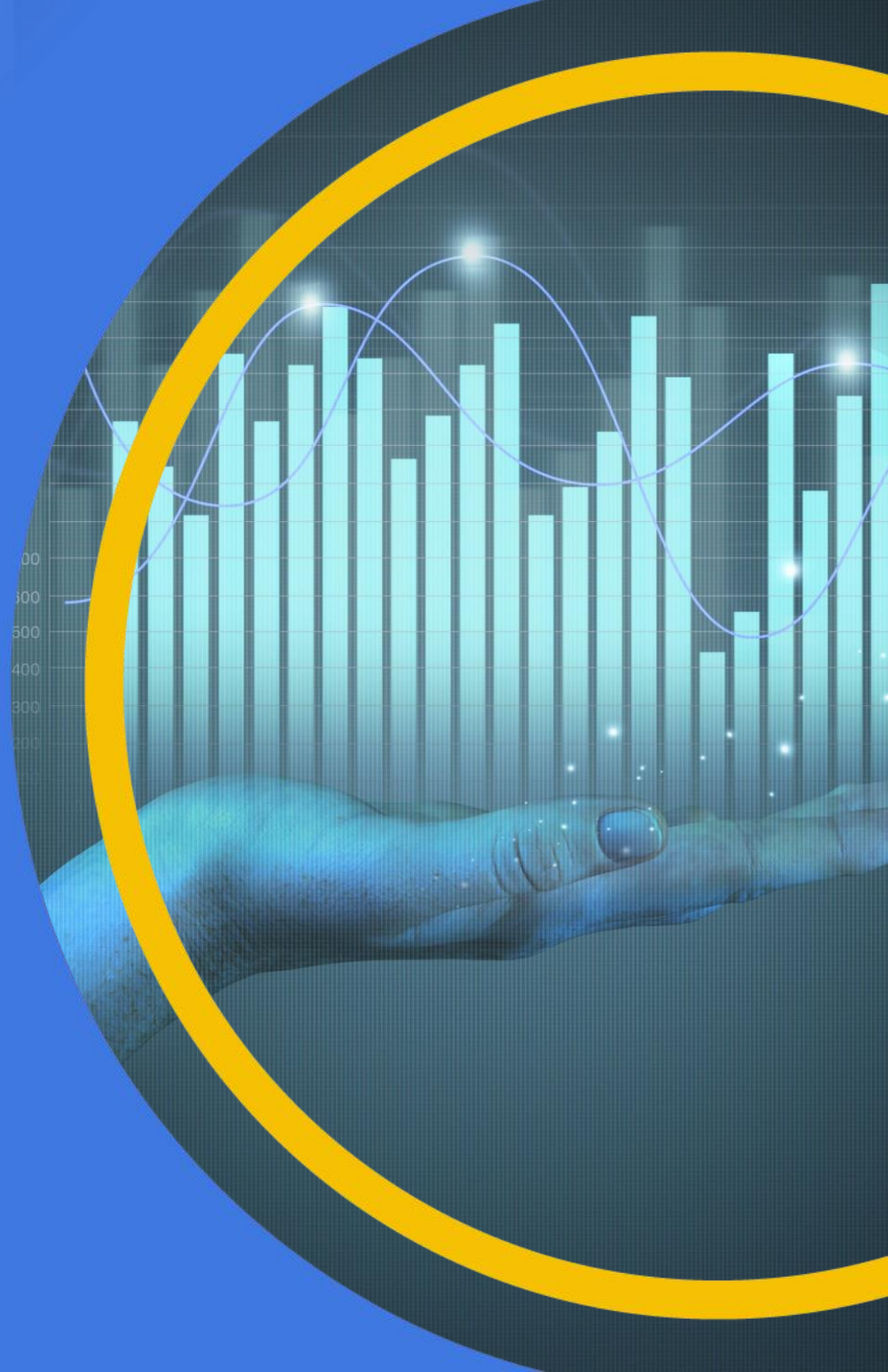
Ruta para uso del Programa de Protección y Seguridad de los Servidores Públicos de la CGR

Cuando consideres que tu vida, seguridad e integridad personal se encuentran en riesgo, siempre y cuando la posible amenaza está relacionada con las funciones desarrolladas y asignadas por la CGR.

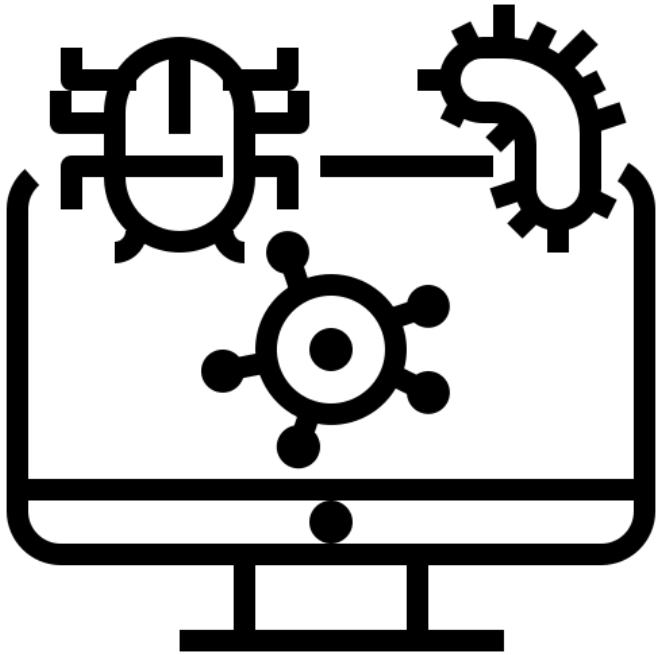
Para activar esta ruta de atención, realiza los siguientes pasos:

- Debes interponer la denuncia ante Fiscalía General de la Nación.
  Consulta dónde y cómo denunciar ante la Fiscalía General de la Nación en https://cutt.ly/29mmrw6
- Comunica a tu jefe inmediato el evento presentado, entregando copia de la denuncia interpuesta ante la Fiscalía General de la Nación.
- Tu jefe inmediato debe reportar el caso ante el Jefe de la USATI, adjuntando la copia de la denuncia y a través de los mecanismos establecidos, a la mayor brevedad posible.
- Espera a que el analista de seguridad asignado por la USATI te contacte, para continuar el proceso correspondiente.

Seguridad de la Información



¿Qué es un MALWARE?



MALWARE viene del término ***"malicious software"***, que designa a todo tipo de programa o código malicioso diseñado, específicamente, para infectar un sistema de cómputo y así realizar determinados actos perjudiciales y, en muchas ocasiones, ilegales.

¿Cómo se puede infectar mi dispositivo?

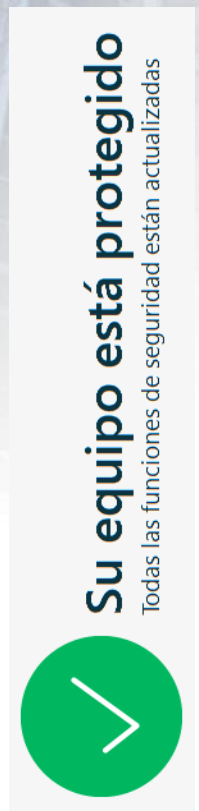
Un computador(sea portátil, de escritorio o servidor) o, incluso, un celular o tableta, puede ser infectado de múltiples maneras.

- **Al abrir un archivo adjunto o seguir un enlace de un correo no solicitado.**
- Al visitar algún sitio web legítimo que haya sido infectado.
- **Al instalar cualquier programa gratuito, sin leer sus opciones o estar debidamente autorizado.**
- Al insertar en el equipo un dispositivo USB infectado.
- Al seguir un enlace infectado de un contacto o en las redes sociales, tales como: Twitter, WhatsApp y Facebook, entre otras.
- Al visitar páginas maliciosas a las cuales fuimos dirigidos por malas búsquedas en el navegador.

¿Cómo nos podemos proteger?

Para contrarrestar esta situación, debes tomar las siguientes medidas:

- Revisa que tenga el **antivirus institucional** instalado y actualizado (si es en un equipo de la CGR).
- Revisa que tenga el aplicativo de seguridad **PCSecure** instalado y habilitado en el equipo de cómputo (si es en un equipo de la CGR).
- NO ABRAS ningún anexo, ni hagas clic sobre ningún vínculo que provenga de un correo que consideres sospechoso.
- Reenvía al buzón **usati.incidentes@contraloria.gov.co** el correo que contiene el archivo adjunto (extensión, ".TBZ", ".7z" y similares), ***sin enviarlo ni reenviarlo a nadie más.***



¿Cómo nos podemos proteger?

IMPORTANTE:

Una vez llega al correo
usati.incidentes@contraloria.gov.co
el mensaje que enviado se valida y si NO ES un correo malicioso, se te informa.

SI ES un correo malicioso, NO se te informará, sino que se procederá a hacer el proceso respectivo.

Consulta cómo detectar posibles correos maliciosos en
https://cutt.ly/69m3xs7

Su equipo está protegido
Todas las funciones de seguridad están actualizadas

CONTRALORÍA GENERAL DE LA REPÚBLICA

100 AÑOS

Defender juntos los recursos públicos ¡Tiene Sentido!

Herramienta de Seguridad PCSecure

El punto verde que aparece en la pantalla del equipo de cómputo institucional, en la parte superior izquierda, significa que la **herramienta de seguridad** PCSecure se encuentra instalada y activa.

¿Por qué no se debe instalar software no autorizado o ilegal en los PC de la Entidad?

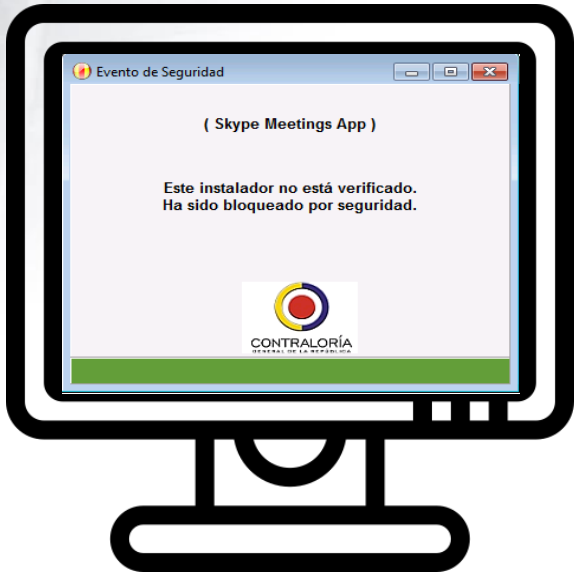
Para dar cumplimiento a lo establecido en la ***Circular No. 12 del 2 de febrero de 2007*** expedida por la Dirección Nacional de Derecho de Autor -DNDA-.

Esta información debe ser presentada cada año por parte del Jefe de Control Interno, suscrita por el Señor Contralor General de la República.

Mayor información: https://cutt.ly/n1pD2lg

DIRECCIÓN NACIONAL DE DERECHO DE AUTOR

Unidad Administrativa Especial
Ministerio del Interior



Bloqueos de Seguridad

Para solicitar cualquier desbloqueo de seguridad, publica la solicitud a través del aplicativo institucional *Mesa de Servicio*, anexando la imagen específica del bloqueo que está presentando el sistema, adjuntando la siguiente información:

- Las direcciones IPv4 e IPv6 del equipo de cómputo.
- El usuario con el que te identificas en la red institucional.
- Qué es lo que necesitas hacer (instalar un software, navegar por determinada página, entre otros).
- Por qué requieres hacerlo.
- Durante cuánto tiempo necesitas este desbloqueo, ya que no puede ser permanente.

Revisa la manera de consultar las direcciones IPv4 e IPv6 del computador en *https://cutt.ly/j9m8kl0*

Ingresa a la Mesa de Servicios Institucional en el banner de aplicaciones que encuentra en *https://congenrep.sharepoint.com/sites/ClicOnline*

¡Recuerda!

Tanto el equipo de cómputo asignado por la CGR y la red por la que se conecta a Internet dentro de nuestras instalaciones, son propiedad para la Entidad, para su uso de en desarrollo de tus actividades laborales y misionales.

Por lo tanto, solo se dará autorización para navegar y utilizar software que esté relacionado con tu quehacer laboral.

Desde la USATI, brindamos algunas recomendaciones para generar contraseñas seguras

Recuerda que tu usuario y contraseña son personales e intransferibles, ya que las actuaciones que se hagan a través de ellas son tu responsabilidad; por eso, no las prestes, ni las dejes a simple vista. ¡Ayúdanos a mejorar la seguridad de nuestros sistemas de información institucionales!

Tu contraseña debe tener más de 8 caracteres.

Debe tener como mínimo, una mayúscula, un número, un caracter especial(*_-#,)

Evita contraseñas fáciles de identificar, como cumpleaños, el nombre de tus hijos o tu pareja, o el de tu mascota.

Tampoco uses contraseñas de estructura sencilla, como números o letras consecutivas.

Aprende cómo crearla mirando el siguiente vinculo: https://cutt.ly/49ZrYzg

Ruta a seguir en caso de posibles incidentes de seguridad de la información

Cuando consideres que la información institucional que administras, almacenas o requieres se encuentra en riesgo.

Para activar esta ruta de atención, consulta los siguientes documentos, disponibles en el Sistema de Gestión y Control Interno –SIGECI–:

- Procedimiento de Gestión Integral de Incidentes de Seguridad (GIIS), que puedes consultar en https://cutt.ly/n9m40F2

- Manual para la Gestión Integral de Incidentes de Seguridad (GIIS) , que puedes consultar en https://cutt.ly/49m48De

Seguridad de bienes y Seguridad Electrónica

Seguridad Física y Electrónica

En la Contraloría General de la República contamos con 5 subsistemas de seguridad electrónica, los cuales apoyan la seguridad integral (personas, bienes, información) en la Entidad:

Para conocer más sobre nuestros arcos detectores de metal, visita el sitio https://cutt.ly/09Zfytq

Cámaras de seguridad

El objetivo de las cámaras de seguridad que se encuentran en la CGR a nivel nacional es vigilar las áreas restringidas, los bienes *Institucionales* y servir de apoyo con valor probatorio, en caso de que suceda un posible incidente que afecte la seguridad en las instalaciones.

Con el fin de minimizar los posibles incidentes de seguridad en las instalaciones, debes tener en cuenta (entre otros):

- Dar cumplimiento a la Política de Escritorio Limpio y Pantalla Limpia (https://cutt.ly/99mVOoQ, Página 16).
- Tener el debido cuidado con los objetos personales e institucionales, evitando dejarlos desatendidos encima del escritorio, en los baños u otras áreas.
- Bloquear el equipo de cómputo institucional cuando dejes desatendido tu puesto de trabajo, así sea por un momento.

Botones de Emergencia

El botón azul que se encuentra cerca a las puertas, sólo se debe utilizar para desbloquearlas en caso de evacuación o emergencia; no para abrirlas y mantenerlas abiertas.

La palanca roja que se encuentra en las zonas de tránsito se debe utilizar para alertar –de manera temprana– ante el riesgo de incendio; ya sea un connato, o el incendio propiamente dicho.

Al accionar la palanca, se encienden las luces estroboscópicas y se activa la alarma sonora.

El uso indebido de cualquiera de los 2 botones de emergencia podrá acarrear sanciones disciplinarias y legales, ya que el hacerlo pone en riesgo la seguridad institucional.

Acceso Biométrico

El objetivo del enrolamiento biométrico es minimizar los riesgos de suplantación, evitando que personas no autorizadas ingresen a las instalaciones de la CGR poniendo en riesgo la seguridad integral, por lo cual, para el ingreso a las instalaciones de la Entidad, se debe realizar el ENROLAMIENTO de la huella biométrica, accediendo, por una única vez, al vínculo https://bit.ly/3kybhZi o escaneando con tu celular el siguiente código QR:

Cuando el servidor público se enrola, el sistema **NO** toma la foto de la huella; convierte en 0 y 1 la información dactilar y almacena estos 0 y 1 para compararlos posteriormente y permitir el acceso; esta información sólo sirve en el Sistema de Control de Acceso de la CGR.

Carnetización

La Real Academia de la Lengua Española define el carné o carnet como

"Del fr. carnet.
m. Documento expedido a favor de una persona, generalmente en forma de tarjeta y provisto de su fotografía, que sirve ***para acreditar su identidad, su pertenencia a un colectivo o su facultad para realizar una actividad.****"* *(negrita extratextual).* http://dle.rae.es/?id=7br6WFG

Por lo tanto, el carné institucional está diseñado para identificarnos dentro de las instalaciones de la CGR, minimizando el riesgo de que alguien no autorizado (que no tenga carné) acceda a áreas que no debe.

Fuera de nuestras instalaciones, el carné institucional está diseñado para identificarnos como servidores públicos de la CGR ante los Sujetos de Control y demás autoridades pertinentes, cuando éstas así lo requieran.

Consulta cómo solicitar el Carné Institucional en el siguiente vínculo
https://cutt.ly/e9ZgvNH

Porte obligatorio del *Carné Institucional*

El porte ***obligatorio y en lugar visible*** del carné institucional (junto con la tarjeta de proximidad, donde aplique) mientras permanezcas dentro de las instalaciones de la Entidad, se encuentra reglamentado mediante el memorando SIGEDOC 2015IE0002119, la Resolución Reglamentaria No. 0227 del 23 de mayo de 2013, modificada por la Resolución Organizacional OGZ-0812-2022.

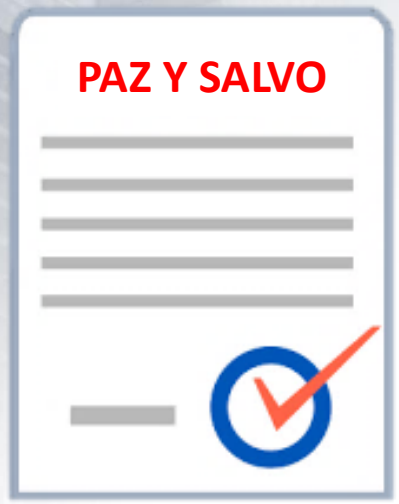
Es decir; ANTES DE INGRESAR a las instalaciones de la Entidad debes tener puesto y mantener EN LUGAR VISIBLE el carné institucional MIENTRAS estás en cualquiera de las sedes de la CGR.

Ingresa al Sistema de Gestión Documental SIGEDOC para consultar el Memorando SIGEDOC No. 2015IE0002119 a través de la Intranet, dando clic en https://sigedoc.contraloria.gov.co/SGD_WEB/main/login.jsp

Consulta el texto de la Resolución Reglamentaria No. 0227 del 23 de mayo de 2013 en https://cutt.ly/R9EVND3

Consulta el texto de la Resolución Organizacional OGZ-0812-2022 en https://cutt.ly/E9E8vqT

Al tener una novedad administrativa, solicita el paz y salvo



Cuando tengas una novedad administrativa que implique un cambio en el carné institucional (traslado de dependencia, retiro, entre otros) debes solicitar el *Paz y Salvo de Elementos de Seguridad*; para ello, remite a la USATI el acto administrativo correspondiente y entrega en la USATI (piso 03 de la Sede de Nivel Central) el carné institucional (y tarjeta de proximidad, si aplica).

En las Gerencias Departamentales, puedes hacer esta entrega al Gerente Departamental Colegiado, o a la persona que apoya las labores relacionadas con el Talento Humano en la Gerencia Departamental (conocida coloquialmente como *"Enlace de Talento Humano"*).

Consulta más información sobre el Paz y Salvo en el sitio asignado en la intranet a la USATI, en https://cutt.ly/K9ZdoFt

Ruta a seguir en caso de posibles incidentes en la seguridad de bienes, seguridad física y electrónica.

Cuando consideres que los bienes institucionales, la seguridad física de las instalaciones o la seguridad electrónica se encuentran en riesgo en cualquiera de las instalaciones de la CGR.

Para activar esta ruta de atención, realiza los siguientes pasos:

- Comunica a tu jefe inmediato el evento presentado, informando las características de modo (cómo sucedieron los hechos); tiempo (cuándo se ejecutaron los hechos –día, mes año, hora y minuto de inicio y de fin de los hechos); y lugar (dónde se ejecutó el hecho), lo más detallado, concreto, preciso y conciso posible.

- Tu jefe inmediato debe reportar el caso ante el Jefe de la USATI a través de los mecanismos establecidos, a la mayor brevedad posible.

- Espera a que el analista de seguridad asignado por la USATI te contacte para continuar el proceso correspondiente.

Desde la Unidad de Seguridad y Aseguramiento Tecnológico e Informático –USATI–, propendemos por la seguridad de las personas, bienes e información institucionales, por lo cual te recomendamos conocer las Políticas de Seguridad Institucionales, acatar las recomendaciones y directrices específicas emanadas desde esta Unidad, y seguirnos a través de nuestra red social institucional Yammer, buscando el

#USATI

o a través de https://cutt.ly/km3vuCY

Consulta más información sobre los servicios, productos, Políticas de Seguridad Institucionales y demás información relacionada con la seguridad de personas, bienes e información, en https://congenrep.sharepoint.com/sites/IntranetUSATI

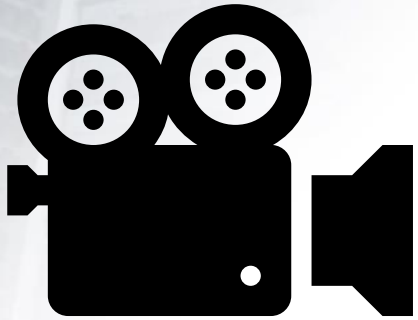
¡MuchasGracias!

CONTRALORÍA
GENERAL DE LA REPÚBLICA

100 AÑOS

Defender juntos los recursos públicos ***¡Tiene Sentido!***

Videografía y Créditos



Aunque la mayoría de las imágenes y videos son construcción propia de la USATI, otras se han tomado de los siguientes sitios:

https://www.youtube.com/watch?v=V4d7J62Nl-g

http://www.raeinforma.com/