****

|  |  |
| --- | --- |
| **PROCESO :** | INFORMÁTICA Y TECNOLOGÍA  |
| **ACTIVIDAD :** | **POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y PROTECCIÓN DE LA PRIVACIDAD** |
| **CÓDIGO :** | **IT-PO-001** |
| **VERSIÓN :** | **4** |

1.

CONTENIDO

[1. GLOSARIO 2](#_Toc142230588)

[2. ABREVIATURAS 5](#_Toc142230589)

[3. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y PROTECCIÓN DE LA PRIVACIDAD 5](#_Toc142230590)

[4. OBJETIVO 6](#_Toc142230591)

[5. ALCANCE 7](#_Toc142230592)

[6. POLÍTICAS SECUNDARIAS Y CONTROLES DE SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y PROTECCIÓN DE LA PRIVACIDAD. 7](#_Toc142230593)

[7. REVISIÓN, MEJORA CONTINUA Y ADOPCIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y PROTECCIÓN DE LA PRIVACIDAD 9](#_Toc142230594)

[8. INCUMPLIMIENTO A LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y PROTECCIÓN DE LA PRIVACIDAD Y SUS RESPECTIVAS POLÍTICAS SECUNDARIAS Y CONTROLES ASOCIADOS. 10](#_Toc142230595)

[9. DIRECTRICES, LINEAMIENTOS, LEYES Y REGULACIONES QUE RIGEN LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y PROTECCIÓN DE LA PRIVACIDAD, POLÍTICAS SECUNDARIAS Y CONTROLES DE SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y PROTECCIÓN DE LA PRIVACIDAD. 10](#_Toc142230596)

[10. CONTROL DE CAMBIOS 11](#_Toc142230597)

[11. DOCUMENTOS RELACIONADOS 11](#_Toc142230598)

# GLOSARIO

* **Confidencialidad:** (inglés: Confidentiality). Propiedad de la información de no ponerse a disposición o ser revelada a individuos, Entidades o procesos no autorizados.[[1]](#footnote-2)
* **Contratista(s):** El que toma a su cargo, la ejecución de alguna cosa.[[2]](#footnote-3)
* **Contrato prestación de servicios:** Son contratos de prestación de servicios los que celebren las Entidades estatales para desarrollar actividades relacionadas con la administración o funcionamiento de la Entidad.[[3]](#footnote-4)
* **Disponibilidad:** (inglés: Availability). Propiedad de la información de estar accesible y utilizable cuando lo requiera una Entidad autorizada.[[4]](#footnote-5)
* **Integridad:** (inglés: Integrity). Propiedad de la información relativa a su exactitud y completitud.[[5]](#footnote-6)
* **MinTIC:** Ministerio de Tecnologías de la Información y las Comunicaciones.[[6]](#footnote-7)
* **Modelo de Seguridad y Privacidad de la Información:** El Modelo de Seguridad y Privacidad de la Información – MSPI, conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.[[7]](#footnote-8)
* **Riesgo:** (inglés: Risk). Efecto de la incertidumbre sobre los objetivos. Un efecto es una desviación de lo esperado: positivo o negativo. La incertidumbre es el estado, incluso parcial, de deficiencia de información relacionada con la comprensión o conocimiento de un evento, su consecuencia o probabilidad. El riesgo a menudo se caracteriza por la referencia a posibles "eventos" (Guía ISO 73: 2009) y "consecuencias" (Guía ISO 73: 2009) o una combinación de estos. El riesgo a menudo se expresa en términos de una combinación de las consecuencias de un evento (incluyendo cambios en las circunstancias) y la "probabilidad" asociada (Guía ISO 73: 2009) de ocurrencia. En el contexto de los sistemas de gestión de seguridad de la información, los riesgos de seguridad de la información pueden expresarse como un efecto de incertidumbre sobre los objetivos de seguridad de la información. El riesgo de seguridad de la información está asociado con el potencial de que las amenazas exploten las vulnerabilidades de un activo de información o grupo de activos de información y, por lo tanto, causen daños a una organización.[[8]](#footnote-9)
* **Seguridad de la información:** (inglés: Información Security). Preservación de la confidencialidad, integridad y disponibilidad de la información. Adicionalmente, otras propiedades como la autenticidad, la responsabilidad, el no repudio y la confiabilidad también pueden estar involucradas.[[9]](#footnote-10)
* **Servidor(es) Público(s):** Persona con una vinculación laboral al estado, que ejerce funciones públicas que están al servicio del estado y de la comunidad. Llámese también servidor público.[[10]](#footnote-11)
* **Sistema de Gestión:** (inglés: Management System). Conjunto de elementos interrelacionados o interactivos de una organización para establecer políticas y objetivos y procesos para alcanzar esos objetivos. Un sistema de gestión puede abordar una sola disciplina o varias disciplinas. Los elementos del sistema incluyen la estructura, roles y responsabilidades, planificación y operación de la organización. El alcance de un sistema de gestión puede incluir la totalidad de la organización, funciones específicas e identificadas de la organización, secciones específicas e identificadas de la organización, o una o más funciones en un grupo de organizaciones.[[11]](#footnote-12)
* **Sistema de Gestión de la Seguridad de la Información:** (inglés: Información Security Management System). Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.[[12]](#footnote-13)

# ABREVIATURAS

* **CREG:** Comisión de Regulación de Energía y Gas
* **MIPG:** Modelo Integrado de Planeación y Gestión.
* **SGSI:** Sistema de Gestión de Seguridad de la Información.

# POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y PROTECCIÓN DE LA PRIVACIDAD

La Comisión de Regulación de Energía y Gas – CREG, consciente de la existencia de riesgos en seguridad y privacidad de la información y ciberseguridad, que afectan la confidencialidad, integridad y disponibilidad de los datos e información que maneja, se compromete a gestionar y mejorar de manera continua el Modelo de Seguridad y Privacidad de la Información – MSPI enmarcado en las mejores prácticas del mercado a nivel de seguridad y privacidad de la información y bajo las directrices y lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC.

Para dar cumplimiento a la [Misión](https://creg.gov.co/publicaciones/8838/mision-y-vision/) de la Comisión de Regulación de Energía y Gas – CREG, se han definido, desarrollado y socializado un total de siete (7) políticas secundarias y sus controles respectivos para su aplicación, los cuales se encuentran especificados en el documento: “**Manual de políticas secundarias y controles de seguridad de la información, ciberseguridad y protección de la privacidad”**, alineados con los cambios tecnológicos y marcos normativos vigentes.

# OBJETIVO

Definir y establecer los principios de seguridad y privacidad de la Información y ciberseguridad en la Comisión de Regulación de Energía y Gas – CREG, para la preservación de la confidencialidad, integridad, disponibilidad y no repudio de los datos, así como para la información con respecto a las normas asociadas a la familia ISO27001 en conjunto con su Anexo A y las directrices y lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC.

# ALCANCE

Identificación y definición de las directrices y lineamientos con los cuales debe contar la Política de Seguridad de la Información, ciberseguridad y protección de la privacidad para preservar la Confidencialidad, Integridad, Disponibilidad y No repudio de los datos y los activos de información. Aplica para todos los funcionarios, contratistas, terceros o partes interesadas de la Entidad.

# POLÍTICAS SECUNDARIAS Y CONTROLES DE SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y PROTECCIÓN DE LA PRIVACIDAD.

De acuerdo con la definición realizada por la Comisión de Regulación de Energía y Gas – CREG a nivel de su Política de seguridad de la información, ciberseguridad y protección de la privacidad, se decide mejorar de manera continua el Modelo de Seguridad y Privacidad de la Información – MSPI.

Con el MSPI se busca proteger con lineamientos claros el proceso de regulación de la prestación de los servicios públicos domiciliarios de energía eléctrica, gas combustible y servicios públicos de combustibles líquidos y en general las demás funciones de la Entidad.

Se establecen las siete (7) políticas secundarias de seguridad que avalan y soportan el Modelo de Seguridad y Privacidad de la Información en la Comisión:

* Política para información de autenticación.
* Política para la privacidad y protección de la información de identificación personal.
* Política para la restricción de acceso a la información.
* Política para la autenticación segura.
* Política para el enmascaramiento de datos.
* Política para las copias de seguridad de la información.
* Política para seguridad física y del entorno.

El cumplimiento de las anteriores políticas secundarias garantizará que:

* Los deberes y las responsabilidades frente a la seguridad de la información, ciberseguridad y protección de la privacidad de los datos e información serán definidas, establecidas, publicadas y aceptadas por cada uno de los funcionarios, contratistas, terceros o partes interesadas que posean vínculo con la Comisión de Regulación de Energía y Gas – CREG.
* Se protegerán y salvaguardarán todos los datos e información que se generen, administren, procesen, modifiquen, transmitan y/o se custodien de acuerdo con los procesos definidos para la prestación del servicio a la ciudadanía, asociados a la regulación de los servicios públicos domiciliarios en el cumplimiento de las funciones de la Comisión de Regulación de Energía y Gas – CREG. Lo anterior con el objetivo de minimizar impactos financieros, operativos y/o legales debido a un uso incorrecto de los datos e información, por lo cual se diseñan y aplican los controles acorde con la clasificación de los datos e información.
* Se protegerán los datos, información y activos de información de las amenazas originadas, ya sea por parte del personal custodio, responsable o usuario de esta.
* Se protegerán las instalaciones físicas donde se procesan y almacenan los datos e información, la infraestructura tecnológica y las redes de datos que soportan y brindan servicio para el desarrollo de los procesos críticos, misionales, de apoyo y de evaluación y control.
* Se definirán e implementarán control de acceso tanto lógico como físico a los datos e información, sistemas, bases de datos, aplicaciones y recursos de red y para garantizar que la seguridad, ciberseguridad y protección de la privacidad sea parte integral del ciclo de vida de los sistemas de información y aplicaciones respectivas.
* Se garantizará el cumplimiento por parte de los funcionarios, contratistas y terceros.

# REVISIÓN, MEJORA CONTINUA Y ADOPCIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y PROTECCIÓN DE LA PRIVACIDAD

La presente política de seguridad de la información, ciberseguridad y protección de la privacidad será revisada al menos una (1) vez al año o cuando se presente alguna condición que afecte la seguridad de los datos e información de la Comisión de Regulación de Energía y Gas – CREG, en búsqueda permanente de la mejora continua.

La respectiva adopción de la presente política es responsabilidad y compromiso del nivel directivo, táctico y técnico (operativo), quienes garantizarán el continuo cumplimiento de lo descrito en el presente documento; así como también lo descrito en el “**Manual de políticas secundarias y controles de seguridad de la información, ciberseguridad y protección de la privacidad”**, que es en donde se establecen los requisitos de seguridad y privacidad de los datos e información y de sus activos de información.

En consecuencia, los cambios que se generen en esta política serán notificados a las partes interesadas a través de los canales autorizados.

# INCUMPLIMIENTO A LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y PROTECCIÓN DE LA PRIVACIDAD Y SUS RESPECTIVAS POLÍTICAS SECUNDARIAS Y CONTROLES ASOCIADOS.

El incumplimiento tanto de la Política de Seguridad de la Información, Ciberseguridad y Protección de la Privacidad, así como de las políticas secundarias y controles de seguridad de la información, ciberseguridad y protección de la privacidad serán considerados como un incidente de seguridad de la información y de acuerdo con el caso, podrá dar lugar a un proceso disciplinario y  para los contratistas  las acciones contractuales que haya lugar, sin perjuicio de la iniciación de otro tipo de acciones a las que hubiere lugar acorde con lo establecido por la Ley.

# DIRECTRICES, LINEAMIENTOS, LEYES Y REGULACIONES QUE RIGEN LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y PROTECCIÓN DE LA PRIVACIDAD, POLÍTICAS SECUNDARIAS Y CONTROLES DE SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y PROTECCIÓN DE LA PRIVACIDAD.

La presente Política de Seguridad de la Información, Ciberseguridad y Protección de la Privacidad, así como las mencionadas políticas secundarias y controles de seguridad de la información, ciberseguridad y protección de la privacidad que ha desarrollado y adoptado la Comisión de Regulación de Energía y Gas – CREG se orientan por los lineamientos definidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, acorde a lo incorporado en los documentos CONPES 3854 de 2016 y 3995 de 2020, Resolución No. 500 de 2021 y el Decreto No. 338 de 2022 expedido por Presidencia de la República.

# CONTROL DE CAMBIOS

|  |  |  |  |
| --- | --- | --- | --- |
| **Descripción del cambio** | **Responsable** | **Fecha Modificación** | **Nueva Versión** |
| Creación del documento. | Líder de seguridad de la información | 04/10/2015  | 0 |
| Revisión de la política y de los objetivos de Seguridad de la Información | Líder de seguridad de la información | 24/08/2017 | 1 |
| Revisión de la política y de los objetivos de Seguridad de la Información | Oficial de Seguridad de la Información | 09/09/2019 | 2 |
| Revisión de la política y de los objetivos de Seguridad de la Información | Oficial de Seguridad de la Información | 18/11/2021 | 3 |
| Ajustes, actualización y alineación a la norma ISO/IEC 27001:2022 | Oficial de Seguridad de la Información | 01/12/2023 | 4 |

# DOCUMENTOS RELACIONADOS

N.A.

1. https://www.iso27000.es/glosario.html [↑](#footnote-ref-2)
2. https://www.funcionpublica.gov.co/glosario/-/wiki/Glosario+2/Contratista [↑](#footnote-ref-3)
3. https://www.funcionpublica.gov.co/glosario/-/wiki/Glosario+2/Contrato+de+Prestaci%C3%B3n+de+Servicios [↑](#footnote-ref-4)
4. https://www.iso27000.es/glosario.html [↑](#footnote-ref-5)
5. https://www.iso27000.es/glosario.html [↑](#footnote-ref-6)
6. https://www.mintic.gov.co/portal/inicio/ [↑](#footnote-ref-7)
7. https://www.mintic.gov.co/gestionti/615/articles-5482\_Modelo\_de\_Seguridad\_Privacidad.pdf [↑](#footnote-ref-8)
8. https://img1.wsimg.com/ [↑](#footnote-ref-9)
9. https://www.iso27000.es/glosario.html [↑](#footnote-ref-10)
10. https://www.funcionpublica.gov.co/glosario/-/wiki/Glosario+2/Servidor+P%C3%BAblico [↑](#footnote-ref-11)
11. https://www.iso27000.es/glosario.html [↑](#footnote-ref-12)
12. https://www.iso27000.es/glosario.html [↑](#footnote-ref-13)