

DECISIÓN DE PRESIDENCIA N°003

Política de Seguridad de la Información y Ciberseguridad



Grupo Energía Bogotá



DECISIÓN DE PRESIDENCIA No.003

Política de Seguridad de la Información y Ciberseguridad

ALCANCE DE LA DECISIÓN

Adoptar la Política de Seguridad de la Información y Ciberseguridad del Grupo Energía Bogotá S.A. ESP, teniendo en cuenta lo dispuesto en el Código de Ética y Conducta del GEB y sus filiales y subsidiarias, el cual establece que “Toda la información generada durante el desarrollo de las actividades empresariales del GEB es considerada como un activo valioso, por lo cual su protección es de vital importancia.

GEB entiende que el acceso a la información debe cumplir con los principios de transparencia, buena fe, no discriminación, celeridad, eficacia, calidad y divulgación proactiva. Por lo tanto, los Colaboradores deben adoptar todas las medidas apropiadas para salvaguardar su confidencialidad, garantizar su acceso, su comprensión y manejo adecuado de la información que conozcan durante el desarrollo de sus funciones y competencias”.

ANTECEDENTES

El 12 de diciembre de 2022 en el Comité de Presidencia fue aprobada la Política Corporativa de Seguridad de la Información y Ciberseguridad del Grupo Energía Bogotá S.A. ESP, en ejercicio del mejoramiento continuo y buscando adoptar medidas de prevención y aseguramiento de la información, como activo fundamental para la organización.

Se decide adoptar el marco de trabajo de ciberseguridad de la National Institute of Standards and Technology (NIST) de Estados Unidos (Cybersecurity Framework), con el fin de protegerse de las amenazas en materia de afectación a la seguridad de la información y ataques cibernéticos. Este marco se adopta por corresponder a la mejor práctica internacional que tiene la industria de la seguridad de la información y ciberseguridad, como medida de mitigación de los riesgos de afectación a la seguridad de la información y ciberseguridad, por ende, la continuidad del negocio.

OBJETO

Establecer el marco de actuación para la protección de la información, los datos personales y los ciberactivos, con la finalidad de aportar al cumplimiento de los objetivos estratégicos, mantener un adecuado nivel de seguridad de la información y ciberseguridad en las tecnologías de la información y la operación, así como aportar al desarrollo y resiliencia del grupo empresarial.

ALCANCE

La presente política debe ser aplicada por el Grupo Energía Bogotá S.A. ESP. Y las sociedades controladas que lo integran, de acuerdo con la normatividad aplicable en cada una de las jurisdicciones donde tienen domicilio.



DECISIÓN DE PRESIDENCIA No.003

Política de Seguridad de la Información y Ciberseguridad

DECLARACIÓN DE COMPROMISOS

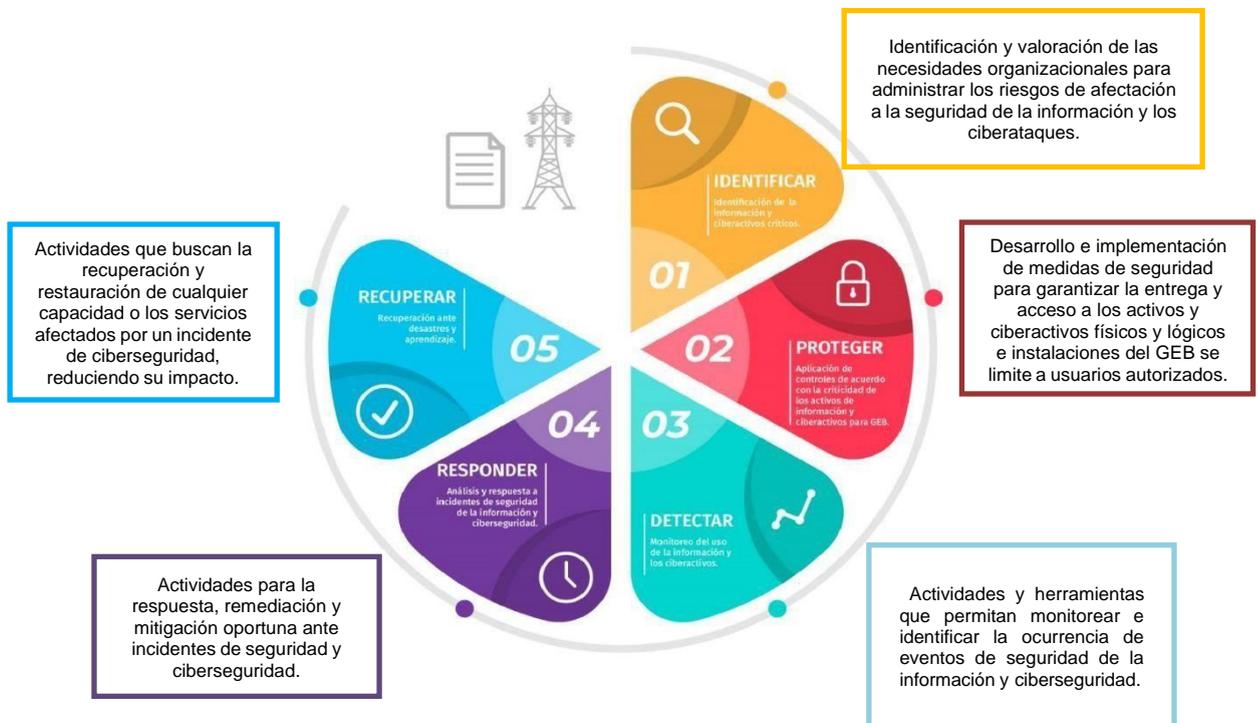
1. Promover **cultura y conciencia sobre el uso seguro de la información y del ciberespacio**.
2. **Proteger los activos** de información y ciberactivos de la infraestructura tecnológica, así como de la infraestructura en operación.
3. Promover la **cooperación de manera solidaria** con los organismos y agencias gubernamentales de cada país donde se hace presencia, generando canales de comunicación, que permitan al Grupo contribuir a un ambiente controlado del uso y la seguridad de la información y la ciberseguridad.
4. **Crear mecanismos de cooperación** entre el GEB y sus filiales y subsidiarias, que permitan lograr eficiencias administrativas, tecnológicas y económicas que, a su vez, apalanquen la implementación de estrategias para la protección de la información y los ciberactivos.
5. **Gestionar los riesgos de Seguridad de la Información y ciberseguridad** que puedan impactar la confidencialidad, integridad, calidad, disponibilidad y privacidad de la información.
6. Potenciar el **desarrollo de capacidades de prevención, detección, contención, respuesta, recuperación y defensa en seguridad de la información y ciberseguridad**.
7. **Adoptar prácticas y cumplir normativas de la industria** en el ámbito de la seguridad de la información y ciberseguridad, que permitan identificar, proteger, detectar, responder y recuperar la infraestructura tecnológica y operativa ante cualquier ataque o afectación a la misma.
8. Transmitir y promover la aplicación de los estándares y buenas prácticas en seguridad de la información y ciberseguridad a los proveedores, terceros, aliados y demás partes involucradas, que puedan acceder a información y/u operación del GEB o sus filiales.

ASPECTOS FUNDAMENTALES PARA SU IMPLEMENTACIÓN

Con la definición y adopción de las etapas para la implementación de herramientas que contribuyan a mantener la Seguridad de la Información y Ciberseguridad, las cuales se presentan a continuación, se asegura el cumplimiento de las declaraciones de compromisos de esta política.

DECISIÓN DE PRESIDENCIA No.003

Política de Seguridad de la Información y Ciberseguridad



ETAPA DE IDENTIFICAR

- Identificar y administrar los activos de información, tanto tecnológica como operativa, datos personales, ciberactivos y sistemas que permitan a la organización alcanzar los objetivos empresariales.
- Valorar los riesgos de afectación a la seguridad de la información y potenciales ataques de ciberseguridad, con el fin de identificar los controles adecuados y efectivos para su mitigación.
- Establecer, divulgar y aprobar los procedimientos y procesos para administrar y monitorear requisitos legales, regulatorios y operativos.

ETAPA DE PROTEGER

- Desarrollar e implementar medidas de seguridad adecuadas para identificar, contener, recuperar y mitigar el impacto de un posible evento de seguridad cibernética.
- Definir y ejecutar controles que aseguren una adecuada gestión de los riesgos al acceso de los activos por parte de personal no autorizado.
- Definir y desarrollar programas de capacitación y sensibilización relacionados con los lineamientos de seguridad y ciberseguridad, dirigidos a los colaboradores del GEB y sus filiales y subsidiarias, así como a terceras partes interesadas que se consideren pertinentes.
- Comunicar a los colaboradores sus deberes, obligaciones y responsabilidades en materia de seguridad de la información y ciberseguridad.
- Proteger la confidencialidad, integridad y disponibilidad de la información que se encuentre en tránsito y reposo en los sistemas del Grupo.
- Proteger los activos a través de la gestión de tecnologías de seguridad.
- Gestionar los riesgos de seguridad y ciberseguridad para la operación, apalancando el cumplimiento de los objetivos estratégicos.

ETAPA DE DETECTAR

- Desarrollar e implementar los mecanismos de monitoreo necesarios para identificar la ocurrencia de un evento de seguridad y de ciberseguridad, tanto de manera preventiva como detectiva.
- Verificar la eficacia de los controles implementados, a través de pruebas y/o evaluaciones.
- Definir y mantener actualizados tableros de control que permitan obtener y visualizar alertas sobre ataques (potenciales o reales) sobre la infraestructura tecnológica y operativa del GEB y sus filiales y subsidiarias.

ETAPA DE RESPONDER

- Establecer mecanismos y controles para dar respuesta ante incidentes de seguridad y ciberseguridad con el fin de mitigar el impacto que pueda generar.
- Definir metodologías de respuesta ante incidentes de seguridad y ciberseguridad que puedan afectar el normal funcionamiento de la operación.

ETAPA DE RECUPERAR

- Gestionar los planes de recuperación y restablecimiento de cualquier capacidad o servicio que se haya visto afectado debido a un incidente de seguridad y ciberseguridad.
- Adoptar lecciones aprendidas de acuerdo con la ejecución del plan de respuesta ante incidentes de seguridad y ciberseguridad.

PROCESO MEDIANTE EL CUAL SE IMPLEMENTARÁ

Los compromisos de la presente política se implementarán a través del proceso de Gestión de Tecnología.

DECISIÓN DE PRESIDENCIA No.003

Política de Seguridad de la Información y Ciberseguridad

RESPONSABLES DE LA POLÍTICA

La junta directiva y el presidente del GEB, son responsables de la aprobación de la presente política.

Son responsables del cumplimiento de la política: filiales y subsidiarias, colaboradores, contratistas, así como los demás grupos de interés que accedan a la información de GEB, sus filiales y subsidiarias.

La Dirección de tecnología del corporativo, o quien haga sus veces, es responsable de liderar la gestión para la implementación, seguimiento, monitoreo, control, actualización y el mejoramiento continuo de la presente política, así como de la alienación con la estrategia corporativa. Dentro del alcance de su gestión incluye la evaluación periódica de la misma, con el fin de establecer su pertinencia y funcionalidad, realizando los ajustes necesarios en caso de requerirse.

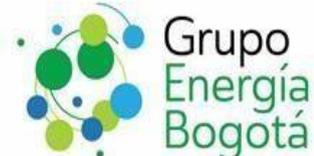
Las filiales y subsidiarias deben implementar la presente política de acuerdo con la naturaleza, tamaño, complejidad y estructura de sus operaciones.

Las áreas de comunicaciones del GEB, filiales y subsidiarias son responsables de comunicar y difundir la presente política a través de los medios disponibles para que sea conocida en todos los grupos de interés de la organización.

La violación por acción u omisión de las disposiciones consignadas en este documento, con cualquier conducta que afecte o pueda afectar los criterios de seguridad: confidencialidad, integridad, disponibilidad y privacidad de la Información, podría acarrear medidas disciplinarias, de acuerdo con lo estipulado en el Código de Ética y Conducta y el Reglamento Interno de Trabajo del GEB.

CONTROL DOCUMENTAL

| | Nombre | Cargo | Área |
|-----------------------|--------------------------------|--|---|
| Elaborado por: | Damaris Lizeth Navarrete Arias | Asesora Seguridad de la Información y Ciberseguridad | Gerencia de Tecnología |
| | Jose Fernando Galvis | Gerente de Tecnología | Gerencia de Tecnología |
| | Maria Virginia Torres | Directora de Abastecimiento y servicios | Dirección de Abastecimiento y servicios |
| Revisado por: | Nestor Fagua | Vicepresidente Jurídico | Vicepresidencia Jurídica |
| Aprobado por: | Juan Ricardo Ortega | Presidente | Presidente |



DECISIÓN DE PRESIDENCIA No.003

Política de Seguridad de la Información y Ciberseguridad

VIGENCIA

| No. de Decisión Previa | Fecha de versión | Tipo de Acción | Razón de la actualización y descripción de última versión |
|------------------------|------------------|----------------|--|
| 004 | 20/04/2018 | Derogación | Aprobación de la Política de Seguridad de la Información y Ciberseguridad del Grupo Energía Bogotá S.A. ESP |
| DP-002-2021 | 20/05/2021 | Derogación | De acuerdo con lo definido en comité de presidencia, los modelos se incorporarán en documentos del SGI, por lo cual esta política deroga el modelo Seguridad de la Información y Ciberseguridad del Grupo Energía Bogotá S.A. ESP definido en el 2021. |