PROMIGAS	**Política Corporativa de Seguridad de la Información y Ciberseguridad**	
Versión: 13	Código: GNA-1656	Estado: Vigente
Elaboró: Vanessa Rosales Gonzalez	Revisó: Henry De la Hoz	Aprobó: Jimena Arango Pilonieta
Cargo: Profesional	Cargo: Profesional	Cargo: Gerente

TABLA DE CONTENIDO

1. OBJETO

1.1 OBJETIVO GENERAL

Definir los lineamientos para proteger los activos de información de Promigas y empresas vinculadas, gestionando y cumpliendo los principios generales que preservan la información mediante la definición de manuales, normas y procedimientos y la identificación de riesgos y controles que fijan roles y responsabilidades de los actores clave, que intervienen en el Sistema de Gestión de Seguridad de la información (SGSI).

1.2 OBJETIVOS ESPECÍFICOS

- Establecer los lineamientos para mantener la confidencialidad, integridad, disponibilidad y privacidad de la información y ciberseguridad en Promigas y empresas vinculadas.
- Definir de qué manera la información debe ser protegida de forma homogénea con base en la valoración de los activos críticos de información de Promigas y empresas vinculadas.
- Garantizar la gestión de riesgos de seguridad de la información y ciberseguridad en Promigas y empresas vinculadas.
- Establecer e implementar los controles que preserven la confidencialidad, integridad, disponibilidad y privacidad de la información en Promigas y empresas vinculadas.
- Fijar roles y responsabilidades de autoridades de control en materia de los pilares de seguridad de la información y ciberseguridad de Promigas y empresas vinculadas.
- Garantizar la aplicación de los requisitos de seguridad de la información y ciberseguridad en la continuidad del negocio y la recuperación ante desastres en Promigas y empresas vinculadas.
- Definir el marco general para gestionar el Sistema de Gestión de Seguridad de la Información (SGSI) que se adapte a los requerimientos del negocio y que esté acorde a los lineamientos establecidos en esta política corporativa.

2. ALCANCE

Esta política es corporativa, por lo cual aplica a Promigas y empresas vinculadas; y por tanto a todos los funcionarios directos, temporales, proveedores y contratistas que en el ejercicio de sus funciones utilicen información y servicios tecnológicos de Promigas y empresas vinculadas, sin importar su ubicación y deberán adoptarla de acuerdo con la naturaleza,

tamaño complejidad y estructura de sus operaciones.

Para aquellos casos en los que no es posible aplicarla, total o parcialmente, deben reportarse tan pronto se conozcan cualquier impedimento, al líder del proceso correspondiente, al Profesional de Seguridad Información, al Coordinador de seguridad de la información o a la gerencia de riesgos y cumplimiento.

Cuando esta Política hace alusión a "PROMIGAS" o a la "Compañía", se refiere a PROMIGAS y las empresas vinculadas, es decir a aquellas empresas sobre las cuales Promigas posee control, según lo definido en la Norma de Administración de Documentos **GNA-002-S1**.

3. DEFINICIONES

Ver Glosario de Seguridad de la Información **PIA – 1661** de Promigas.

4. CONDICIONES GENERALES

Las amenazas que vulneran la seguridad de la información y ciberseguridad pueden afectar la reputación de Promigas y sus empresas vinculadas, así como sus activos de información y operaciones. Conscientes de las consecuencias y como compromiso para proteger la disponibilidad, confidencialidad, integridad y privacidad de la información, Promigas desarrolló esta política corporativa y ha establecido, implementado, mantiene y mejora continuamente un sistema de gestión de seguridad de la información y ciberseguridad.

Este documento recoge los principios y normas internas que son la base de la Política de Seguridad de la Información y Ciberseguridad para Promigas y sus empresas vinculadas, y sirven para implementar los procedimientos asociados.

La implementación de nuevos procesos de negocio que generen información física o electrónica deben cumplir con las directrices definidas en esta política y con lo establecido en la Política de Informática **PNA-744,** o documento equivalente para cada compañía según aplique, con el propósito de proteger la información.

Lo dispuesto en esta política aplica de manera general para todo el manejo de la información, incluyendo garantizar el principio de seguridad en el tratamiento de datos personales conforme a lo establecido en la ley estatutaria 1581 de 2012 y su decreto

reglamentario según lo definido en la Política de Protección de Datos Personales GNA-1651, o documentos equivalentes para cada compañía según les corresponda, para todo lo anterior se toma como base la siguiente normatividad:

- **NTC-ISO-IEC 27001**: Esta norma específica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información, dentro del contexto de la organización. La presente norma también incluye los requisitos para la valoración y el tratamiento de riesgos de seguridad de la información, adaptados a las necesidades de la organización. Los requisitos establecidos en esta norma son genéricos y están previstos para ser aplicados a todas las organizaciones, independientemente de su tipo, tamaño o naturaleza.
- **ISO/IEC 27000**: es un grupo de estándares internacionales titulados: Tecnología de la Información Técnicas de Seguridad - Sistemas de Gestión de la Seguridad de la Información - Visión de conjunto y vocabulario. Tiene como fin ayudar a organizaciones de todo tipo y tamaño a implementar y operar un Sistema de Gestión de la Seguridad de la Información (SGSI).
- **ISO/IEC 27701**: Estándar que especifica los requisitos y proporciona orientación para establecer, implementar, mantener y mejorar continuamente el Sistema de Gestión de privacidad de la información.
- **Ley 1581 de 2012** (Habeas Data): Por la cual se dictan disposiciones generales para el tratamiento y la protección de datos personales.
- **Ley 1273 de 2009**: Protección de la información y de los datos y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.
- **Ley SOX:** Ley estadounidense emitida en 2002 que tiene como objetivo mejorar el ambiente de control interno de las empresas que cotizan en las bolsas de valores de los estados unidos; definir y formalizar responsabilidades sobre su cumplimiento para la prevención de errores contables y de reporte.
- **SEC** (*Securities and Exchange Commission - "SEC*", por sus siglas en inglés): Organismo del Gobierno Federal de Estados Unidos que ejerce supervisión sobre los participantes clave en el mercado de valores y cuya misión es proteger a los inversionistas, mantener el mercado de valores ordenado, eficiente y protegido contra el fraude, mantener información relevante sobre el mismo y facilitar la creación de capitales.
- **Framework de Ciberseguridad NIST**: Marco de trabajo basado en estándares, directrices y prácticas existentes para que las organizaciones gestionen el riesgo de ciberseguridad.

5. CONTENIDO

5.1 DECLARACIÓN DE COMPROMISO

Promigas está comprometida con la política de seguridad de la información y ciberseguridad, promoviendo una cultura de cumplimiento y control de acuerdo con los principios establecidos por el sistema de gestión de seguridad de la información y ciberseguridad, por lo anterior se busca:

Prevenir los daños a la imagen y reputación a través de la adopción y cumplimiento de la política de seguridad de la información y ciberseguridad.

Promover continuamente una cultura de seguridad de la información y ciberseguridad.

Gestionar de manera estructurada y estratégica los riesgos de seguridad de la información y ciberseguridad asociados al negocio y su relacionamiento con terceros.

Igualmente, cada colaborador, funcionario temporal, contratista y proveedor, es responsable por aplicar los lineamientos definidos en esta política y por ajustar sus actuaciones de acuerdo con los valores corporativos y lineamientos establecidos en seguridad de la información y ciberseguridad, de igual forma es responsable de reportar los incidentes de los que pudiera llegar a tener conocimiento.

5.2 ACTUALIZACION

Esta política es revisada y actualizada por la Coordinación de Seguridad de la Información y la Gerencia de Riesgo y Cumplimiento es responsable de aprobar las directrices señaladas en este documento. El comité de seguridad de la información y ciberseguridad podrá emitir recomendaciones sobre las propuestas de ajustes o cambios en la Política de seguridad de la información- **GNA 1656.**

Para efectos de asegurar su vigencia, suficiencia y nivel de eficacia, este documento se debe mantener actualizado cada vez que surjan temas que lo ameriten o por lo menos una vez al año

5.3 CUMPLIMIENTO DE LA POLÍTICA

El cumplimiento de los principios, directrices, procedimientos contenidos en esta Política son obligatorios y cualquier excepción debe ser notificada a seguridad de la información y documentada como un riesgo en el que incurre la compañía y debe ser formalmente aceptada por el Líder del proceso.

Cada colaborador, funcionario temporal y proveedor, es responsable por aplicar los criterios definidos en esta política y por ajustar sus actuaciones de acuerdo con los valores corporativos y lineamientos establecidos en seguridad de la información, de igual forma es responsable de reportar los incidentes de los que pudiera llegar a tener conocimiento.

5.4 PRINCIPIOS

La información es uno de los "Activos" más importantes y debe ser utilizada en forma acorde con los requerimientos del negocio y sólo por la persona autorizada para ello. Con el fin de dar cumplimiento con los objetivos establecidos y como parte de la Política de Seguridad de la Información y Ciberseguridad, se han establecido los siguientes principios fundamentales:

- **Confidencialidad:** la información del negocio y de terceras partes debe ser protegida, independientemente del medio o formato en que se encuentre.
- **Integridad:** La información del negocio debe preservar su integridad independientemente del medio en el que se encuentre, así sea temporal o permanente, o de la forma en que sea transmitida.
- **Disponibilidad:** La información del negocio debe estar disponible cuando sea legítimamente requerida.

5.5 GOBIERNO PARA LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Promigas y sus empresas vinculadas deben estructurar las funciones y responsabilidades frente al Riesgo de Seguridad de la Información y Ciberseguridad y frente a la gestión en esta materia, de acuerdo con la Política Corporativa para la Gestión Integral de Riesgos. Este marco de referencia define el esquema de las tres líneas, considerando, (i) la gestión por líneas de negocio, (ii) una función de gestión de riesgo de Seguridad de la Información

independiente, y (iii) una revisión independiente, así:

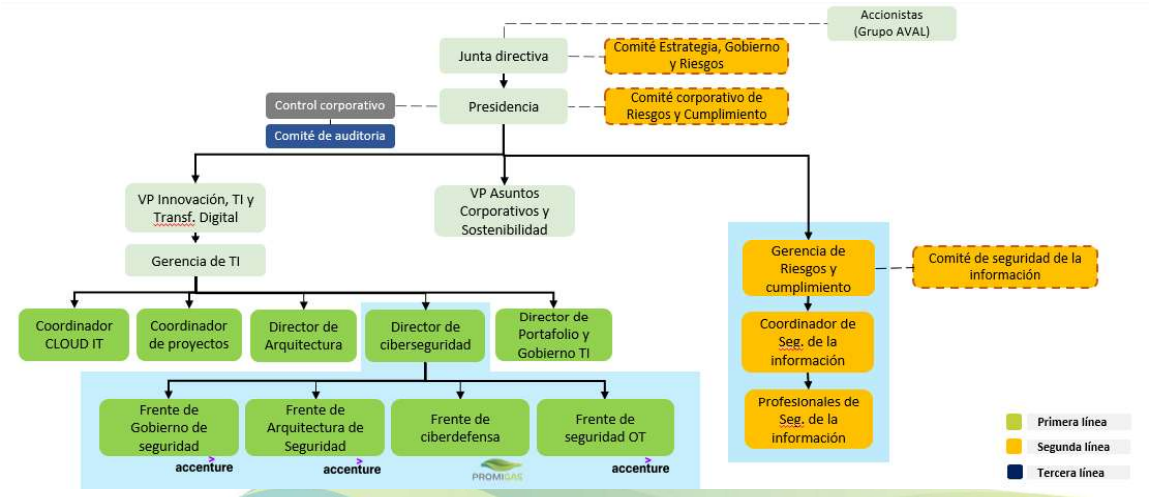

Imagen 1 Organigrama con las responsabilidades de Seguridad de la Información y Ciberseguridad y la distinción de las 3 líneas

Primera línea: La primera línea la constituyen las áreas de Seguridad TI y todos los colaboradores de Promigas y empresas vinculadas.

La Política de seguridad de la información y ciberseguridad reconoce que los colaboradores que hacen parte de la primera línea, es decir los colaboradores responsables de la seguridad TI y demás colaboradores ejecutores de procesos o proyectos, como los responsables en primera medida, de identificar, evaluar, administrar, monitorear y reportar los riesgos e incidentes de seguridad y ciberseguridad inherentes a las, actividades, procesos, productos y sistemas relacionados con su labor. Quienes conforman esta línea deben conocer sus actividades y procesos, y disponer de los recursos suficientes para realizar eficazmente sus tareas. Así mismo, deben cumplir con políticas y procedimientos definidos por la Organización, contribuyendo a una sólida cultura en Seguridad de la Información y Ciberseguridad.

Segunda línea: Esta línea está conformada por La Gerencia de Riesgos y Cumplimiento de Promigas y de manera específica está representada por la Coordinación de seguridad de la información, la cual debe establecer los lineamientos en esta materia y realizar un seguimiento continuo al cumplimiento de todas las obligaciones de Riesgo en Seguridad de

la Información y Ciberseguridad.

La segunda línea es responsable de presentar los resultados de gestión directamente al Comité de Seguridad de la Información y Ciberseguridad o a la Alta Dirección. Así mismo, debe contar con recursos suficientes para realizar eficazmente todas sus funciones y desempeñar un papel central y proactivo en el Sistema de Gestión de Seguridad de la Información. Para ello, debe estar plenamente familiarizado con las políticas y procedimientos vigentes, sus requisitos legales y reglamentarios y los riesgos de Seguridad de la Información derivados del negocio, incluyendo temas específicos de Ciberseguridad.

Tercera Línea: Conformada por los equipos de Auditoría Interna, juega un papel importante al evaluar de forma independiente la gestión y los controles de los riesgos de la seguridad de la información y ciberseguridad, así como las políticas, estándares y procedimientos de los sistemas, rindiendo cuentas al Comité de Auditoría. Las personas encargadas de auditorías internas que deben realizar estas revisiones deben ser competentes y estar debidamente capacitadas y no participar en el desarrollo, implementación y operación de la estructura de riesgo/control. Esta revisión puede ser realizada por el personal de auditoría o por personal independiente del proceso o sistema que se examina, pero también puede involucrar actores externos debidamente calificados.

5.6 ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN

Para dar cumplimiento al objetivo de la Política Corporativa de Seguridad de la Información y Ciberseguridad, se han definido los siguientes actores clave para la gestión de la seguridad de la información, de manera que contribuyan a la implementación y operación del Sistema de Gestión de Seguridad de la Información definido para la compañía:

Actor	Actividades De Ejecución	Actividades De Supervisión
Junta Directiva	• Velar porque se cuente con los recursos técnicos y humanos suficientes para gestionar adecuadamente la seguridad de la información y la ciberseguridad. • Exigir con el cumplimiento de las normas y regulaciones	• Supervisar la seguridad de la información y ciberseguridad en Promigas y empresas vinculadas, comprendiendo los riesgos y asegurando que estos sean gestionados.

Actor	Actividades De Ejecución	Actividades De Supervisión
	gubernamentales de seguridad de la información y ciberseguridad. • Participar en programas de concientización y capacitación en temas de Seguridad de la Información y Ciberseguridad.	
Alta Dirección	• Proveer principios, directrices y lineamientos Corporativos de Seguridad de la información y Ciberseguridad, tomar las acciones preventivas y correctivas pertinentes para Promigas y empresas vinculadas. • Identificar, evaluar e incluir los requerimientos de Seguridad de la Información y Ciberseguridad en las iniciativas corporativas realizadas para las entidades. • Promover la aplicación y apropiación de buenas prácticas de seguridad de la información y ciberseguridad. • Asegurar la apropiación de los recursos requeridos para la implementación y operación del sistema de gestión de seguridad de la información. • Fortalecer la cultura de Seguridad de la Información de los colaboradores de Promigas y sus empresas vinculadas, funcionarios temporales, contratistas y terceras partes, que administren activos de información.	• Monitorear el cumplimiento a nivel corporativo de las políticas del Sistema de gestión de seguridad de la información y ciberseguridad en cada entidad. • Conocer el nivel de madurez del SGSI y avances en la mitigación de riesgos y cierre de brechas de seguridad de la información y ciberseguridad.
Comité de Riesgos y Cumplimiento (Ver conformación del comité en el Anexo 1 del Manual de Gestión	• Fomentar el desarrollo de la Organización de Seguridad de la Información. • Informar principios, directrices y lineamientos Corporativos de	• Velar porque se realice seguimiento y se cumplan los lineamientos definidos de Seguridad de la Información. • Velar porque la Coordinación

Actor	Actividades De Ejecución	Actividades De Supervisión
Integral de Riesgos GMA-1932)	Seguridad de la información y Ciberseguridad, verificar el desarrollo de proyectos Corporativos de Seguridad de la información y Ciberseguridad y tomar las acciones preventivas y correctivas pertinentes. • Socializar actividades y proyectos que sean de interés común y/o impacten a Promigas y/o empresas vinculadas. • Aprobar las directrices que crean convenientes, en cada una de empresas vinculadas, para el mejoramiento de la Gestión de Seguridad de la Información.	de Seguridad de la información ejecute y controle la política de Seguridad de la Información y ciberseguridad. • Conocer el resultado de la Gestión de Seguridad de la Información y ciberseguridad realizada por parte de Promigas y las empresas vinculadas. • Conocer los Incidentes de Seguridad de la Información presentados en las compañías que hayan tenido impacto significativo, identificados mediante las diferentes fuentes de reporte y los planes de acción llevados a cabo para la mitigación de estos. • Conocer el nivel de madurez del SGSI y avances en la mitigación de riesgos y cierre de brechas de seguridad de la información y ciberseguridad.
Comité de Seguridad de la Información y Ciberseguridad (Ver conformación del comité en el Anexo 1 del presente documento)	• Aprobar la viabilidad de implementar cambios tecnológicos a los elementos que conforman la Arquitectura de Seguridad Informática. • Aprobar el cronograma anual de pruebas de penetración con base en la propuesta elaborada por el Profesional Seguridad de la Información.	• Verificar el nivel de seguridad de la información por medio del análisis de los indicadores de gestión, para así proponer acciones correctivas o de mejora en caso de que se requiera. • Velar por la ejecución de los Proyectos de Seguridad de la Información y Ciberseguridad

Actor	Actividades De Ejecución	Actividades De Supervisión
	• Escalar al Comité de Riesgos y Cumplimiento los temas relevantes tratados en el Comité de Seguridad de la Información y Ciberseguridad. • Revisar y determinar las acciones a tomar ante los incidentes de seguridad de la información e informática detectados o reportados. • Socializar actividades y proyectos que sean de interés común y/o impacten a Promigas y/o sus empresas vinculadas. • Generar retroalimentación de las jornadas de seguridad y diagnósticos de los SGSI realizados y contribuir a la mejora continua de la postura de Seguridad de la Información. • Definir principios, directrices y lineamientos Corporativos de Seguridad de la Información y Ciberseguridad. • Definir requerimientos de Seguridad de la Información y Ciberseguridad en las iniciativas corporativas realizadas para las compañías.	periódicamente y requerir las acciones correctivas respecto a aquellos que lo ameriten. Velar porque las actividades cumplan con la política, procedimientos y estándares de seguridad de la Información y ciberseguridad. • Realizar seguimiento al nivel de madurez del SGSI y avances en la mitigación de riesgos y cierre de brechas de seguridad de la información y ciberseguridad. • Realizar seguimiento a la estrategia corporativa de seguridad de la información y ciberseguridad.
Gerente de Riesgo y Cumplimiento	• Aprobar la Política de Seguridad de la Información y Ciberseguridad; y velar por su implementación, mantenimiento y correcto funcionamiento. • Participar activamente la definición del plan estratégico de seguridad de la información y ciberseguridad. • Coordinar con las áreas las actividades y proyectos encaminados al fortalecimiento del programa de gestión de seguridad de la	• Velar por la actualización de los documentos de seguridad de la información. • Aprobar los lineamientos de mejora en los procesos del Sistema de Gestión de Seguridad de la Información y Ciberseguridad.

Actor	Actividades De Ejecución	Actividades De Supervisión
	información. • Solicitar los recursos requeridos para la implementación y operación del sistema de gestión de seguridad de la información. • Cumplir con las demás responsabilidades que sean definidas para la Alta Gerencia.	
Coordinador de Seguridad de la Información	• Velar por la implementación, mantenimiento y correcto funcionamiento de la Política de Seguridad de la Información y Ciberseguridad. • Apoyar la definición del plan estratégico de seguridad de la información y ciberseguridad de la compañía en función de los objetivos del negocio. • Liderar el Comité de Seguridad de la Información y Ciberseguridad y adoptar las mejores prácticas sugeridas en este. • Coordinar la definición y ejecución de las actividades del Plan Anual de Concientización en Seguridad de la Información y Ciberseguridad. • Propiciar la actualización del inventario de riesgos de Seguridad de la Información. • Coordinar la adopción y el cumplimiento de los lineamientos establecidos por el corporativo. • Apoyar a la primera línea en el proceso de identificación de riesgos y controles, la determinación de su criticidad y verificación del cumplimiento de los planes de acción	• Conocer los Incidentes de Seguridad de la información y las medidas que se han implementado para mitigarlos. • Monitorear el resultado de las evaluaciones de Riesgos. • Monitorear indicadores clave de desempeño sobre la gestión de seguridad de información y Ciberseguridad.

Actor	Actividades De Ejecución	Actividades De Supervisión
	establecidos en la gestión de incidentes de seguridad de la información y ciberseguridad. • Coordinar los procesos de medición del nivel de madurez del SGSI y la definición y seguimiento a planes de acción para su mejora continua. • Definir y ejecutar el Plan Anual de Monitoreos de Seguridad de la Información. • Liderar, coordinar y apoyar a los líderes de proceso en la actualización de activos de información. • Coordinar y hacer seguimiento a la definición y ejecución del Plan Anual de Pruebas de Seguridad.	
Profesional de Seguridad de la información	• Participar activamente en la definición del plan estratégico de seguridad de la información y ciberseguridad de la compañía en función de los objetivos del negocio. • Adoptar y socializar las mejores prácticas sugeridas en el Comité. • Proponer y ejecutar planes de divulgación y concientización en seguridad de la información y ciberseguridad. • Coordinar la actualización del inventario de riesgos de Seguridad de la Información. • Adoptar y velar por el cumplimiento de los lineamientos establecidos por el corporativo. • Ejecutar con la primera línea el proceso de identificación de riesgos y controles, la determinación de su criticidad y verificación del cumplimiento de los planes de acción	• Conocer los Incidentes de Seguridad de la información y las medidas que se han implementado para mitigarlos. • Monitorear el resultado de evaluación de Riesgos. • Definir y monitorear indicadores clave de desempeño sobre la gestión de seguridad de información y Ciberseguridad.

Actor	Actividades De Ejecución	Actividades De Supervisión
	establecidos en la gestión de incidentes de seguridad de la información y ciberseguridad. • Fomentar la ejecución de planes, proyectos o iniciativas para la preparación de las compañías ante incidentes de seguridad de la información y ciberseguridad. • Registrar y clasificar incidentes de seguridad y reportarlos a las instancias que correspondan de acuerdo con el nivel de criticidad. • Generar conceptos de seguridad en proyectos de implementaciones tecnológicas. • Mantenerse actualizado sobre los temas relacionados con la seguridad de la información.	
Gerente de TI	• Definir el plan estratégico de tecnologías de la información y los presupuestos necesarios para su ejecución. • Asegurar la toma de decisiones relacionadas con la seguridad técnica y apalancar las iniciativas que se desprendan de la mejora continua de la postura de seguridad en Promigas y empresas vinculadas. • Realizar análisis de riesgos de seguridad informática a los aplicativos, productos, sistemas operativos, herramientas, redes y dispositivos de acceso físico. • Proponer mejoras a la Política Corporativa de Seguridad de la Información y Ciberseguridad. • Asegurar y velar por la	• Propender por que se revise la seguridad informática de los programas que se implementan a instalar en las compañías. • Asegurar la implementación de medidas de seguridad informática requeridas para mantener un adecuado uso de la información corporativa a través de dispositivos móviles.

Actor	Actividades De Ejecución	Actividades De Supervisión
	implementación de arquitecturas de seguridad informática establecidas. • Realizar un diagnóstico periódico de la seguridad informática en la compañía. • Velar por la ejecución de planes tácticos para el fortalecimiento de la madurez del SGSI, mitigación de riesgos y vulnerabilidades de seguridad sobre plataforma tecnológica. • Asegurar la existencia de procesos, recursos y tecnologías para mantener adecuadamente la gestión de la seguridad técnica alineado a las políticas corporativas de seguridad de la información y ciberseguridad.	
Director de Ciberseguridad	• Liderar la definición del plan estratégico de Ciberseguridad Y Seguridad de la Información asegurando presupuestos necesarios para su ejecución. • Asegurar las comunicaciones, los sistemas y los activos de la empresa de amenazas internas y externas. • Realizar análisis de riesgos de seguridad informática a los aplicativos, productos, sistemas operativos, herramientas, redes y dispositivos de acceso físico. • Proponer mejoras a la Política Corporativa de Seguridad de la Información y Ciberseguridad. • Asegurar y velar por la implementación de arquitecturas de seguridad informática establecidas. • Realizar un diagnóstico periódico de la seguridad informática en la	• Propender por que se revise la seguridad informática de los programas que se implementan a instalar en las compañías. • Asegurar la implementación de medidas de seguridad informática requeridas para mantener un adecuado uso de la información corporativa a través de dispositivos móviles.

Actor	Actividades De Ejecución	Actividades De Supervisión
	compañía. • Velar por la ejecución de planes tácticos para el fortalecimiento de la madurez del SGSI, mitigación de riesgos y vulnerabilidades de seguridad sobre plataforma tecnológica. • Asegurar la existencia de procesos, recursos y tecnologías para mantener adecuadamente la gestión de la seguridad técnica alineado a las políticas corporativas de seguridad de la información y ciberseguridad.	
Coordinador de Ciberdefensa / Coordinador de Infraestructura	• Identificar los riesgos de seguridad en el recurso que administra y gestionar la implementación de controles mitigatorios. • Informar al Profesional de Seguridad de Información sobre nuevos riesgos identificados y de manera particular sobre nuevos riesgos de Ciberseguridad. • Participar en el Comité de Seguridad de la Información y Ciberseguridad. • Adoptar y socializar las mejores prácticas sugeridas en el Comité. • Apoyar el proceso de identificación de riesgos y controles, así como en su evaluación y valoración. • Implementar y operar los controles de seguridad informática y ciberseguridad. • Garantizar el cierre oportuno de brechas de seguridad sobre la plataforma tecnológica. • Liderar el diseño y ejecución de actividades y estrategias en las diferentes etapas de la respuesta a	• Analizar los Incidentes Significativos de Seguridad de la información y ciberseguridad detectados o identificados a través de las distingas fuentes de reporte e implementar los planes de remediación • Velar porque se adopte medidas para responder a los incidentes presentados y para prevenir futuros incidentes. • Adoptar las mejores prácticas vigentes en el mercado con respecto a respuestas a incidentes. • Definir y monitorear indicadores clave de desempeño sobre la gestión de seguridad informática y Ciberseguridad.

Actor	Actividades De Ejecución	Actividades De Supervisión
	incidentes de seguridad informática o ciberseguridad.	
Responsables de la información (Es quién requiere la información para llevar a cabo su proceso de negocio)	• Identificar claramente el valor de la información bajo su responsabilidad para poder clasificarla y protegerla. Así mismo conocer los riesgos a los que podría estar expuesta y velar porque se provean los mecanismos necesarios para que estos riesgos se mitiguen a niveles aceptables, considerando costo-beneficio para su área de negocio y la organización. • Con el apoyo de la segunda línea, identificar los controles clave para mitigar los riesgos identificados. • Llevar a cabo la ejecución de los controles para mitigar los riesgos (Autocontrol). • Reportar a las áreas de seguridad TI y de seguridad de información, cualquier evento o incidente de seguridad de información y de manera particular cualquier evento material de Ciberseguridad. • Definir y ejecutar los planes de acción para mitigar los riesgos de seguridad de la información a su cargo.	• Vigilar y velar que su equipo de trabajo dé cumplimiento a la política de seguridad de la información y ciberseguridad, así como a los estándares y procedimientos que de esta se desprenden.
Usuarios de la información (Demás sujetos que utilizan la información)	• Poner en práctica los lineamientos y estrategias de Seguridad de la Información y Ciberseguridad, que garanticen la protección de la información de las compañías. • Tratar la información del negocio de acuerdo con el nivel de confidencialidad definido. • Reportar eventos inesperados o	• Identificar riesgos en los recursos sobre los cuales tiene acceso y generar sugerencias para mejorar las condiciones de seguridad implementadas.

Actor	Actividades De Ejecución	Actividades De Supervisión
	inusuales que puedan potencialmente llegar a afectar los principios de confidencialidad, integridad y disponibilidad de los activos de información. • Participar activamente en todas las iniciativas de concientización y capacitación de seguridad de la información y ciberseguridad.	

5.7 LINEAMIENTOS CORPORATIVOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD.

Mediante los siguientes puntos se describen a alto nivel y de forma general los lineamientos de seguridad de información y ciberseguridad con las que se establecen las directrices para mantener la confidencialidad, integridad, disponibilidad y privacidad de la información y ciberseguridad en Promigas y empresas vinculadas. Adicionalmente, esta política se complementa con el documento Manual de Seguridad de la Información **GMA-2099** a través del cual se especifican y amplían las directrices por cada dominio del Sistema de Gestión de Seguridad de la Información.

5.7.1 Propiedad intelectual.

LA INFORMACIÓN DEL NEGOCIO ES UN ACTIVO VITAL DE PROMIGAS Y POR LO TANTO DEBE SER PROTEGIDO.

Teniendo en cuenta la Política de Propiedad Intelectual **GNA-1841**, la información de PROMIGAS, sin importar su presentación, medio o formato, en el que sea creada o utilizada para el soporte a las actividades de negocio, se califica como información del negocio o activo de información que debe ser clasificada.

La Seguridad de la información y ciberseguridad del negocio es el conjunto de medidas de protección que toma la compañía contra la divulgación, modificación, hurto o destrucción

accidental o maliciosa de su información. Dichas medidas de protección se basan en el valor relativo de la información y el riesgo en que se pueda ver comprometida.

Los responsables de la información son los responsables de asegurar que la información del negocio cuenta con la protección apropiada para así preservar la Confidencialidad, Integridad, Disponibilidad y Privacidad de la información.

PROMIGAS debe disponer de los medios necesarios para asegurarse de que cada colaborador o tercero preserve y proteja los activos de información de una manera consistente y confiable. Cualquier persona que intente inhabilitar, vencer, o sobrepasar cualquier control de seguridad será sujeto de las acciones disciplinarias correspondientes.

LA PROPIEDAD DE LA INFORMACIÓN SE DEBE MANTENER.

La Propiedad Intelectual se define como cualquier patente, derecho de autor, invención o información que es propiedad de PROMIGAS. Todo el material que es desarrollado mientras se trabaja para la compañía se considera que es de su propiedad intelectual y de uso exclusivo de la misma, por lo tanto, debe ser protegido contra develado, apropiación o uso que menoscabe la competitividad de PROMIGAS, así mismo se debe asegurar el cumplimiento a las disposiciones previstas en la Política de Propiedad Intelectual **GNA-1841**.

5.7.2 Responsables de la información.

CADA ACTIVO DE INFORMACIÓN DE PROMIGAS DEBE TENER UN RESPONSABLE DESIGNADO QUE DEBE VELAR POR SU SEGURIDAD CON BASE EN LOS RIESGOS A LOS QUE ESTÁ EXPUESTA.

PROMIGAS utiliza información para desarrollar su actividad misional. Esta se crea y se dispone a quienes intervienen en los diferentes procesos para que pueda desarrollar y cumplir sus respectivas metas dentro del marco del negocio.

La información que PROMIGAS utilice para el desarrollo de sus objetivos de negocio debe tener asignado un responsable, quien la utiliza en su área y es el responsable por su correcto uso. Así, es quien toma las decisiones que son requeridas para la protección de su información y determina quiénes son los usuarios y sus privilegios de uso. En PROMIGAS

actuarán como responsables de la información, los vicepresidentes, gerentes, directores, coordinadores y demás titulares de las diferentes dependencias o a quienes éstos deleguen.

5.7.3 Administración del riesgo en seguridad de la información y ciberseguridad.

LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD A QUE ESTÁ EXPUESTA LA INFORMACIÓN DE PROMIGAS DEBEN SER IDENTIFICADOS, EVALUADOS Y MITIGADOS ACORDE CON SU VALOR, PROBABILIDAD DE OCURRENCIA E IMPACTO EN EL NEGOCIO.

La información del negocio se debe proteger con base en su valor y en el riesgo en que se pueda ver comprometida. Por lo tanto, la Organización debe realizar periódicamente un análisis del estado del negocio frente a la seguridad de la información y ciberseguridad.

Con los niveles de riesgo y la valoración de la información, cada responsable de proceso debe realizar una evaluación formal de riesgos, considerándolos como riesgos de negocio y utilizando la misma metodología de valoración de riesgos, para que estos sean identificados, evaluados y se apliquen las acciones necesarias para subsanarlos o mitigarlos acorde con los niveles de riesgo permitidos por la compañía.

Cada usuario de la información debe estar enterado de los procedimientos de reporte de riesgos que puedan tener impacto en la seguridad de la información de PROMIGAS, y se requiere que reporten inmediatamente cualquier sospecha u observación de un incidente a la seguridad de la información y la ciberseguridad.

5.7.4 Cumplimiento de regulaciones.

PROMIGAS DEBE CUMPLIR CON LAS REGULACIONES LOCALES E INTERNACIONALES DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD.

Esta política está acorde y apoya el cumplimiento de las leyes y regulaciones locales e internacionales aplicables relativas a la privacidad, la Seguridad de la Información y ciberseguridad. Por lo tanto, tales requerimientos deben ser incluidos en el desarrollo del Sistema de Seguridad de la Información y Ciberseguridad y se deben establecer acciones específicas para mantener alineada permanentemente a PROMIGAS con tales

disposiciones.

Todas las áreas, dentro de sus procesos deban cumplir con los requisitos reglamentarios y contractuales, así como con la reglamentación aplicable, para lo cual seguir las directrices establecidas en la Política de Cumplimiento Normativo **GNA-2024** o el equivalente en cada compañía.

5.7.5 Capacitación y creación de cultura en seguridad de la información y ciberseguridad.

PROMIGAS HA ESTABLECIDO UN PLAN PERMANENTE PARA GENERAR CONCIENCIA SOBRE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD PARA LOS USUARIOS Y TERCEROS.

La compañía cuenta con un programa permanente que permita asegurar que los usuarios y terceros están informados acerca de sus responsabilidades en Seguridad de la Información y ciberseguridad y de las continuas amenazas que ponen en riesgo la información que maneja.

Los colaboradores y terceros deben estar enterados de los procedimientos de seguridad de la información y ciberseguridad que deben aplicar adicionalmente a los que se requieren para realizar su función de trabajo. Como parte de su programa de capacitación, el nuevo personal vinculado a la compañía debe recibir durante el período de inducción, capacitación sobre los requerimientos de seguridad de la información y ciberseguridad de PROMIGAS. La participación en las capacitaciones sobre seguridad de la información es de obligatorio cumplimiento para todos los colaboradores de Promigas y sus empresas vinculadas.

5.7.6 Seguridad en el personal.

PROMIGAS DEBE PROVEER LOS MECANISMOS NECESARIOS PARA ASEGURAR QUE SUS EMPLEADOS CUMPLAN CON SUS RESPONSABILIDADES EN SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD DESDE SU INGRESO HASTA SU RETIRO.

Los empleados que ingresen a PROMIGAS deben seguir un proceso de selección, y una vez vinculados, tendrán acceso la presente Política y al Manual de Seguridad de la Información **GMA-2099** para su conocimiento y debido cumplimiento.

Los contratos de los empleados deben incluir cláusulas que indiquen las responsabilidades correspondientes para con la seguridad de la Información y ciberseguridad y el cumplimiento del código de ética, haciéndole conocer las consecuencias en caso de no ser seguidas y cumplidas.

Se debe mantener un registro por empleado de su conocimiento y entendimiento de la Política de Seguridad de la Información y ciberseguridad, mediante la certificación de la capacitación anual sobre seguridad de la información y ciberseguridad.

5.7.7 Terceros que acceden información de Promigas local o remotamente en los aplicativo locales o en el ciberespacio.

LOS TERCEROS QUE UTILIZAN LOCAL O REMOTAMENTE INFORMACIÓN DE PROMIGAS DEBEN CUMPLIR CON LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD.

El uso de la información de PROMIGAS por parte de terceros ya sea que se encuentre en los aplicativos locales o en el ciberespacio, y se acceda de manera ya sea local o remotamente, debe ser formalizado por medio de acuerdos y/o cláusulas que hagan obligatorio el cumplimiento de la presente Política y asimismo lo previsto en el documento de **Seguridad de la información en la relación con proveedores y contratistas PPA-2112**. En los contratos se debe incluir la obligación de proteger la información de PROMIGAS, los requisitos de seguridad para mitigar los riesgos sobre la información y ciberseguridad y consecuencias a que estarían sujetos en caso de incumplirla.

Cada relación con un tercero debe tener un representante (tales como gerente, director o sus delegados en el rol de administrador de contrato) dentro de PROMIGAS, que vele por el correcto uso y la protección de la información del negocio. Para los terceros con accesos a plataforma tecnológica crítica o que incluyan uso de privilegios administrativos, la Gerencia de TI, en coordinación con el representante correspondiente, deberá realizar periódicamente una revisión formal de los derechos de acceso de los usuarios de entes externos que acceden a ésta.

5.7.8 Identificación y autenticación individual.

TODOS LOS USUARIOS QUE ACCEDEN LA INFORMACIÓN DE PROMIGAS DEBEN DISPONER

DE UN MEDIO DE IDENTIFICACIÓN Y EL ACCESO DEBE SER CONTROLADO A TRAVÉS DE UNA AUTENTICACIÓN PERSONAL.

Cada usuario es responsable por sus acciones mientras usa cualquier recurso de información de PROMIGAS ya sea local o en el ciberespacio. Por lo tanto, la identidad de cada usuario de los recursos informáticos deberá ser establecida y autenticada de una manera única y no podrá ser compartida.

Los usuarios de PROMIGAS una vez creados y asignadas sus autorizaciones en los Sistemas de Información, podrán acceder a la información mediante su usuario y clave de autenticación. Dependiendo del valor de la información y del nivel de riesgo, PROMIGAS definirá medios de autenticación apropiados, que no podrán ser compartidos (como la clave de acceso) y dichos medios de autenticación contienen información confidencial que no debe ser revelada o almacenada en lugares que puedan ser accedidos por personas no autorizadas.

5.7.9 Control y administración del acceso a la información local o en el ciberespacio.

EL USO DE LA INFORMACIÓN DE PROMIGAS DEBE SER CONTROLADO PARA PREVENIR ACCESOS NO AUTORIZADOS. LOS PRIVILEGIOS SOBRE LA INFORMACIÓN DEBEN SER MANTENIDOS EN CONCORDANCIA CON LAS NECESIDADES DEL NEGOCIO, LIMITANDO EL ACCESO SOLAMENTE A LO QUE ES REQUERIDO.

Se deben establecer mecanismos de control de acceso físico y lógico para asegurar que los activos de información se mantengan protegidos localmente y en el ciberespacio de una manera consistente con su valor para el negocio y con los riesgos de pérdida de Confidencialidad, Integridad, Disponibilidad y Privacidad de la información.

Los derechos de acceso no deben comprometer la segregación de tareas y responsabilidades. El acceso realizado localmente y/o en el ciberespacio a la información de la compañía deberá ser otorgado sólo a usuarios autorizados, basados en lo que es requerido para realizar las tareas relacionadas con su responsabilidad. El acceso a los recursos de PROMIGAS debe ser restringido en todos los casos, y se debe dar específicamente bajo las premisas de necesidad de conocer y menor privilegio posible.

5.7.10 Clasificación de la información.

TODA LA INFORMACIÓN, INDEPENDIENTE DEL MEDIO EN QUE SE ENCUENTRE, SERÁ CLASIFICADA EN UNA DE LAS SIGUIENTES 3 CATEGORÍAS: RESTRINGIDA, INTERNA Y PÚBLICA, DE ACUERDO CON EL ESTÁNDAR DE CLASIFICACIÓN DE INFORMACIÓN ESTABLECIDO POR LA COMPAÑÍA.

Al igual que otros activos, no toda la información tiene el mismo uso o valor, y por consiguiente requiere diferentes niveles de protección. Toda la información de PROMIGAS será clasificada por el responsable de la Información con base en un análisis de alto nivel del impacto al negocio en seguridad de la información y ciberseguridad, que determine su valor relativo y nivel de riesgo a que está expuesta. La metodología definida para clasificar la información se encuentra plasmada en el Procedimiento de Clasificación de la información **GPA-1978.**

Según los riesgos que se identifiquen, el responsable de la información y el Profesional de Seguridad de la Información, determinarán los controles que sean necesarios para proveer un nivel de protección de la información apropiado y consistente con alcance a PROMIGAS y sus empresas vinculadas, sin importar el medio, formato o lugar donde se encuentre. Estos controles deben ser aplicados y mantenidos durante el ciclo de vida de la información, desde su creación, durante su uso autorizado y hasta su apropiada disposición o destrucción.

De acuerdo con la clasificación de la información y los riesgos a los que esté expuesta, se deben implementar controles de cifrado durante los procesos de transmisión y almacenamiento de la misma, conforme a lo establecido en el Manual de Controles Criptográficos **PMA-2030**.

5.7.11 Continuidad de la seguridad.

TODOS LOS RECURSOS DE INFORMACIÓN CRITICOS Y LOS PROCESOS ASOCIADOS YA SEAN LOCALES O EN EL CIBERESPACIO, DEBEN CONTAR CON UN PLAN DE CONTINUIDAD DEL NEGOCIO Y ESTAR PREPARADOS PARA ATAQUES A LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD. LA CONTINUIDAD DE LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD SE MANTIENE DURANTE SITUACIONES DE CONTINGENCIA.

La información debe estar disponible para su uso autorizado cuando PROMIGAS la requiera en la ejecución de sus tareas regulares. Por lo que, se deben desarrollar, documentar, implementar y probar periódicamente procedimientos para asegurar una recuperación razonable y a tiempo de la información crítica de la compañía, tanto localmente como en el ciberespacio, sin disminuir los niveles de seguridad establecidos. Esto debe ser independiente tanto del medio tecnológico que utilice PROMIGAS como de la posibilidad de que la información se dañe, se destruya o no esté disponible temporalmente.

PROMIGAS establecerá medidas que permitan detectar y mitigar los efectos de ataques en seguridad de la información y ciberseguridad como son los de negación de servicios y el ingreso de código malicioso no autorizado. Estas medidas estarán fundamentadas en procedimientos y elementos que permitan mantener informada a PROMIGAS de la existencia de estas amenazas, detectar los ataques de manera inmediata y ejecutar las acciones consiguientes.

5.7.12 Seguridad física.

TODAS LAS ÁREAS FÍSICAS DEL NEGOCIO DEBEN TENER UN NIVEL DE SEGURIDAD ACORDE CON EL VALOR DE LA INFORMACIÓN QUE SE PROCESA Y ADMINISTRA EN ELLAS. LA INFORMACIÓN CONFIDENCIAL O SENSITIVA AL NEGOCIO DEBE MANTENERSE EN LUGARES CON ACCESO RESTRINGIDO CUANDO NO ES UTILIZADA. TODOS LOS FUNCIONARIOS DEBEN CUMPLIR CON LAS DIRECTRICES PARA LA PROTECCIÓN FÍSICA DE LA INFORMACIÓN RESTRINGIDA O CONFIDENCIAL QUE USEN.

Las áreas físicas construidas para soportar toda la operación del negocio deberán estar provistas de los controles adecuados (por ejemplo: puertas, cerraduras, lectores de tarjetas, biométricos, cámaras de seguridad, entre otros) según el valor de la información que contienen.

Los recursos informáticos de PROMIGAS deben estar físicamente protegidos contra amenazas de acceso no autorizado y amenazas ambientales para prevenir exposición, daño o pérdida de los activos e interrupción de las actividades de negocio.

La información clasificada como restringida con alta confidencialidad no se dejará desatendida o sin control, por lo que PROMIGAS desarrollará normas corporativas que

permitan prevenir que la información crítica del negocio sea accedida sin autorización, dentro de lo cual está comprendido la implantación y cumplimiento de las directrices de Escritorio Limpio y Pantalla Limpia.

5.7.13 Administración de alertas.

PROMIGAS DEBE SER ALERTADA EN EL MISMO INSTANTE EN QUE EXISTAN VIOLACIONES A LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD.

Las situaciones o acciones que violen la presente Política deben ser detectadas, registradas e informadas a los funcionarios de la Coordinación de Seguridad de la Información o la Gerencia de Riesgos y Cumplimiento de manera inmediata (alertas). Se debe desarrollar estrategias para el manejo de eventos e incidentes que dé prioridad a dichas alertas y las resuelva conforme a la criticidad de la información para PROMIGAS. En estas estrategias se debe incluir la definición de una organización de reacción inmediata, con el objetivo de atender éstas y otras situaciones que la compañía considere como críticas. Lo relacionado con la gestión de incidentes y eventos de seguridad debe atenderse conforme a lo establecido en el Plan de Respuesta a Incidentes Informáticos **GPA-1664**.

5.7.14 Auditabilidad de los eventos de seguridad de la información y ciberseguridad.

LOS REGISTROS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD DE PROMIGAS DEBEN SER REVISADOS PERMANENTEMENTE PARA ASEGURAR EL CUMPLIMIENTO DEL MODELO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD.

Los responsables de la Información deben definir los eventos considerados como críticos (por ejemplo: intentos de acceso fallidos al sistema de información, borrado o alteración de información, entre otros) y los respectivos registros de seguridad de la información y ciberseguridad que deben ser generados.

Los registros de seguridad de la información y ciberseguridad deben ser activados, almacenados y revisados permanentemente, y las situaciones no esperadas deben ser reportadas de manera oportuna a los responsables, así como a los niveles de seguridad requeridos. Los registros y los medios que los generan y administran deben ser protegidos por controles que eviten modificaciones o accesos no autorizados, para preservar la integridad de las evidencias.

5.7.15 Conectividad.

TODAS LAS CONEXIONES A REDES PÚBLICAS DEBEN SER AUTENTICADAS PARA PREVENIR QUE LA INFORMACIÓN SEA DEVELADA O ALTERADA.

Las conexiones a la red privada de PROMIGAS deben realizarse de una manera segura para preservar la confidencialidad, integridad, disponibilidad y privacidad de la información trasmitida sobre la red. Igualmente, todos los accesos de salida al ciberespacio y a otras topologías privadas deben realizarse sobre redes aprobadas por PROMIGAS.

Los usuarios de la información y terceros que se conecten a la red privada deben cumplir con la presente Política antes de que se realice la conexión. Esto aplica igualmente a cualquier conexión actual o futura en la red de PROMIGAS, que utilice redes públicas.

Se requiere la aprobación del responsable de la Información para poder acceder remotamente la información de PROMIGAS, y dichos accesos deben cumplir con la Política de Identificación y Autenticación.

5.7.16 Uso aceptable de los recursos informáticos del negocio local y en el ciberespacio

LOS RECURSOS INFORMÁTICOS PROVISTOS LOCALMENTE Y EN EL CIBERESPACIO SON PARA USO EXCLUSIVO DEL NEGOCIO.

Los recursos informáticos de PROMIGAS tanto locales como en el ciberespacio, son exclusivamente para propósitos del negocio y deben ser tratados como activos dedicados a proveer las herramientas para realizar el trabajo requerido. Usuarios de la información y terceros que intenten acceder a información para la que no tienen un requerimiento autorizado de negocio, están violando la presente Política.

Todos los usuarios deben emplear los recursos de información de la empresa de acuerdo con las normas de seguridad de la información y ciberseguridad establecidas. Está prohibido el acceso no autorizado, la divulgación de información restringida, el uso de software no aprobado y cualquier actividad que comprometa la seguridad de los sistemas. Los usuarios deben proteger sus credenciales, evitar el uso personal excesivo de los activos y notificar inmediatamente cualquier incidente de seguridad

En el uso de la información de PROMIGAS no se debe presumir privacidad, por lo que cuando ésta sea utilizada se podrán crear registros de la actividad realizada, que pueden ser revisados por PROMIGAS de acuerdo con lo dispuesto en el Manual de Seguridad de la Información **GMA-2099**, que debe ser conocido y aceptado por todos los funcionarios.

PROMIGAS se reserva el derecho de restringir el acceso a cualquier información en el momento que lo considere conveniente. Personal seleccionado por la compañía podrá utilizar tecnología de uso restringido como la de monitoreo de red, datos operacionales y eventos en seguridad de la información.

Ningún hardware o software no autorizados serán cargados, instalados o activados en los recursos informáticos, sin previa autorización formal de la Gerencia de TI y concepto emitido por el área de Seguridad de la Información.

Para acceder a la información de PROMIGAS tanto local como en el ciberespacio a través de medios tales como los dispositivos o accesos móviles, se deben implementar los controles necesarios para reducir los riesgos introducidos por estas prácticas.

5.7.17 Seguridad de información y ciberseguridad en los procesos de administración de sistemas.

CADA PROCESO DE ADMINISTRACIÓN DE SISTEMAS DE PROMIGAS DEBE CUMPLIR CON LA PRESENTE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD.

Actividades, normas y responsabilidades en seguridad de la información y ciberseguridad deben ser incluidas dentro de cada uno los procesos de administración de sistemas de la compañía, para lograr el cumplimiento de esta Política.

Independientemente de la autoría o responsabilidad de los nuevos desarrollos y los requeridos en procesos de soporte, el área de desarrollo de la Gerencia de TI debe crear y mantener una metodología que controle el ciclo completo de desarrollo y mantenimiento seguro de sistemas. Los requerimientos de seguridad de la información y ciberseguridad deben ser identificados previos al diseño y desarrollo de los sistemas de tecnología de la información y ciberseguridad. Durante el desarrollo, estos requerimientos deben ser incluidos dentro de los sistemas y si una modificación es requerida, ésta debe cumplir

estrictamente con los requerimientos de desarrollo seguro y seguridad de la información que han sido previamente establecidos. El nivel de Seguridad de un sistema no puede verse disminuido, por lo que la información y los sistemas en producción no serán utilizados para desarrollo, prueba o mantenimiento de aplicaciones.

Todos los Recursos Informáticos que se implementen en la compañía, deben seguir la configuración de los parámetros de seguridad de acuerdo con las normas y estándares establecidos en el documento Especificaciones de Seguridad **PIA-018** o documento equivalente en cada compañía. No se pueden implementar nuevos componentes tecnológicos sin que previamente se incluyan todas las medidas de seguridad requeridas. Para ello, se deben implantar las facilidades disponibles en el equipo, en cuanto a seguridad se refiere y adaptarlas en función de las normas y los estándares definidos.

El uso de la virtualización y la computación en la nube en la compañía deberá llevarse a cabo teniendo los controles necesarios para mitigar los riesgos introducidos por estas tecnologías.

La implantación de un sistema nuevo o cambio significativo a los existentes debe ser revisada por medio de una evaluación de riesgo, que permita la detección de riesgos, la ubicación de controles apropiados que los mitiguen y la operación segura.

La realización de un cambio tecnológico a nivel local o en el ciberespacio que no considere los requerimientos de seguridad de la Información y ciberseguridad hace que PROMIGAS este expuesta a riesgos. Por lo tanto, cada cambio tecnológico debe asegurar el cumplimiento de la Política de Seguridad de la Información y ciberseguridad y sus respectivas normas subyacentes, y en caso de exponer a la compañía a un riesgo en seguridad de la información y/o ciberseguridad, éste debe ser identificado, evaluado, documentado, asumido y controlado por el respectivo responsable de la Información.

5.8 MODELO DE EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Para la identificación de riesgos y la aplicación de controles de seguridad de la información y ciberseguridad, Promigas adopta el modelo de evaluación de seguridad de la información y ciberseguridad. Este modelo tiene como propósito evaluar el nivel de madurez del sistema de gestión de seguridad de la información e identificar las oportunidades de mejora que permitan fortalecerlo, basados en los dominios y controles propuestos en la norma NTC-

ISO 27001:2013 y en el Framework de Ciberseguridad NIST.

5.9 SANCIONES POR INCUMPLIMIENTO

El incumplimiento a esta política y normas subyacentes por acción u omisión traerá consigo consecuencias legales de conformidad con lo previsto en el reglamento interno de trabajo, la constitución y la ley.

6. DOCUMENTOS DE REFERENCIA Y ANEXOS

Se enuncian los documentos de Promigas relacionados con esta Política:

ANEXO 1 Comité de Seguridad de la Información y ciberseguridad.
PIA-1661 – Glosario de Seguridad de la Información
PPA-018 – Procedimiento de administración de cuentas de usuario
FA-432 – Formato Creación de Código de Usuarios
PPA-727 – Procedimiento de Control de Cambios en Recursos de IT
PNA-744 – Política de Informática
PIA-018 - Especificaciones de seguridad
GNA-1651 – Política de Protección de Datos Personales
PNA-1863 – Requisitos de Seguridad Para Proyectos de Sistemas de Información
GPA-1978 – Procedimiento de Clasificación de la Información
PPA-1999 – Procedimiento de Gestión y Remediación de Vulnerabilidades Informáticas.
GPA-1664 – Plan de Respuesta a Incidentes Informáticos
GMA-2099 – Manual de Seguridad de la Información y Ciberseguridad
PPA-2112 – Seguridad de la información en la relación con proveedores y contratistas
PMA-2030 – Manual de Controles Criptográficos

7. CONTROL DE CAMBIOS

Cambios de la versión 12 – Abril 2025

- Se hacen cambios en el numeral de actualización de la política 5.2
- Se actualiza la estructura de gobierno numeral 5.6
- Se realizan cambios en responsabilidades de algunos de los roles descritos en el numeral 5.6

- Se ajusta subtítulo y se adiciona lineamiento en el numeral 5.7.16
- Se crea el anexo para el comité de seguridad de la información y ciberseguridad

Solicitud No. 21408

Cambios de la versión 11 – Diciembre 2022

- Se actualizan códigos de documentos de referencia vigentes.
- Se modifica el numeral de CUMPLIMIENTO DE REGULACIONES, referenciando la Política de Cumplimiento Normativo.
- Se aclara el alcance de revisión de acceso a tercero a aplicaciones críticas y/o administración privilegiada.

Solicitud No. 17969

Cambios de la versión 10 – Julio 2022

- Se realiza ajuste en el numeral 5.7 ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN adicionando a la Gerente General de Enlace como miembro principal del comité de seguridad de la información
- Se corrige el código y nombre del procedimiento SEGURIDAD DE LA INFORMACIÓN EN LA RELACION CON PROVEEDORES Y CONTRATISTAS PPA-112.

Solicitud No. 17338