

POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN

Todos los derechos reservados. Ninguna reproducción, copia o transmisión digital de esta publicación puede ser hecha sin un permiso escrito.

Ningún párrafo de esta publicación puede ser reproducido, copiado o transmitido digitalmente sin un consentimiento escrito o de acuerdo con las leyes que regulan los derechos de autor o copyright en Colombia, las cuales son: Artículo 61 de la Constitución Política de Colombia; Decisión Andina 351 de 1993; Código Civil, Artículo 671; Ley 23 de 1982; Ley 44 de 1993; Ley 599 de 2000 (Código Penal Colombiano), Título VIII; Ley 603 de 2000; Decreto 1360 de 1989; Decreto 460 de 1995; Decreto 162 de 1996.

TABLA DE CONTENIDO

1. Objeto	3
2. Alcance.....	3
3. Definiciones	3
4. Condiciones generales.....	3
4.1. Cumplimiento de la política	4
4.2. Principios	4
5. Contenido	5
5.1. Responsabilidades.....	5
5.2. Organización de seguridad de la información	6
5.2.1. Descripción de roles y responsabilidades.....	6
5.3. Capacitación y creación de cultura de seguridad de la información.	15
5.4. Seguridad en el personal.....	16
5.5. Propiedad intelectual	17
5.6. Cumplimiento de regulaciones externas	18
5.7. Administración del riesgo en seguridad de la información	18
5.8. Control de los eventos de seguridad de la información	18
5.9. Administración de alertas	19
5.10. Clasificación y manejo de la información	20
5.11. Continuidad del negocio.....	22
5.12. Protección de código malicioso.....	22
5.13. Seguridad física.....	24
5.14. Seguridad de la información en los procesos de administración de sistemas	26
5.15. Identificación y autenticación individual.....	27

	POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN	
Versión: 6	Código: GNA-1656	Estado: Vigente
Elaboró: Ever Capdevila Pacheco	Revisó: Adriana Esmeral Berrío	Aprobó: Ximena Correa Agudelo
Cargo: Profesional	Cargo: Coordinador	Cargo: Gerente

5.16.	Control y administración del acceso a la información	30
5.17.	Terceros que acceden información	32
5.18.	Seguridad en las redes.....	33
5.19.	Escritorio limpio y pantalla limpia	36
5.20.	Dispositivos móviles	36
5.21.	Uso adecuado de internet	38
6.	Documentos de referencia y anexos	38
7.	Control de cambios	39

	POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN	
Versión: 6	Código: GNA-1656	Estado: Vigente
Elaboró: Ever Capdevila Pacheco	Revisó: Adriana Esmeral Berrío	Aprobó: Ximena Correa Agudelo
Cargo: Profesional	Cargo: Coordinador	Cargo: Gerente

1. OBJETO

Establecer los lineamientos relacionados con el manejo seguro de la información, de forma que ésta sea accedida sólo por aquellos que tienen una necesidad legítima para la realización de sus funciones del negocio (**Confidencialidad**), que esté protegida contra modificaciones no planeadas, realizadas con o sin intención (**Integridad**), que esté disponible cuando sea requerida (**Disponibilidad**).

2. ALCANCE

Esta política es corporativa, por lo cual aplica a todo el personal de Promigas y empresas vinculadas; y a terceros quienes tienen acceso de forma interna o externa a la información, sin importar su ubicación.

Para aquellos casos en los que no es posible aplicarla, total o parcialmente, deben reportarse tan pronto se conozcan cualquier impedimento, a la vicepresidencia correspondiente y al profesional de Seguridad Información o al Coordinador de Riesgos de Promigas.

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

Este documento recopila los principios y normas internas que constituyen los fundamentos principales de la Política de Seguridad de la Información para las compañías, y son la base para la implementación de los procedimientos.

La implementación de nuevos procesos de negocios que generen información física o electrónica, sistemas de información, debe cumplir con las directrices definidas en esta política y con lo establecido en la Política de Informática **PNA-744**, o documento

	POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN	
Versión: 6	Código: GNA-1656	Estado: Vigente
Elaboró: Ever Capdevila Pacheco	Revisó: Adriana Esmeral Berrío	Aprobó: Ximena Correa Agudelo
Cargo: Profesional	Cargo: Coordinador	Cargo: Gerente

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 lo establecido en la ley 1581 y su decreto reglamentario según lo definido en la Política de Protección de Datos Personales **GNA-1651**, o documento equivalente para cada compañía.

Esta política será revisada anualmente o antes si se identifican circunstancias que ameriten su modificación, para garantizar que se mantenga adecuado, suficiente y eficaz.

4.1. CUMPLIMIENTO DE LA POLÍTICA

El cumplimiento de los principios, directrices, normas, procedimientos y demás documentos es obligatorio y cualquier excepción debe ser documentada como un riesgo en el que incurre la compañía y debe ser formalmente aceptada por el Líder del proceso.

Es obligación de los usuarios, sin excepción alguna, conocer, respetar, y hacer cumplir esta Política de Seguridad de la Información.

4.2. 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, 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.

	POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN	
Versión: 6	Código: GNA-1656	Estado: Vigente
Elaboró: Ever Capdevila Pacheco	Revisó: Adriana Esmeral Berrío	Aprobó: Ximena Correa Agudelo
Cargo: Profesional	Cargo: Coordinador	Cargo: Gerente

5. CONTENIDO

5.1. RESPONSABILIDADES

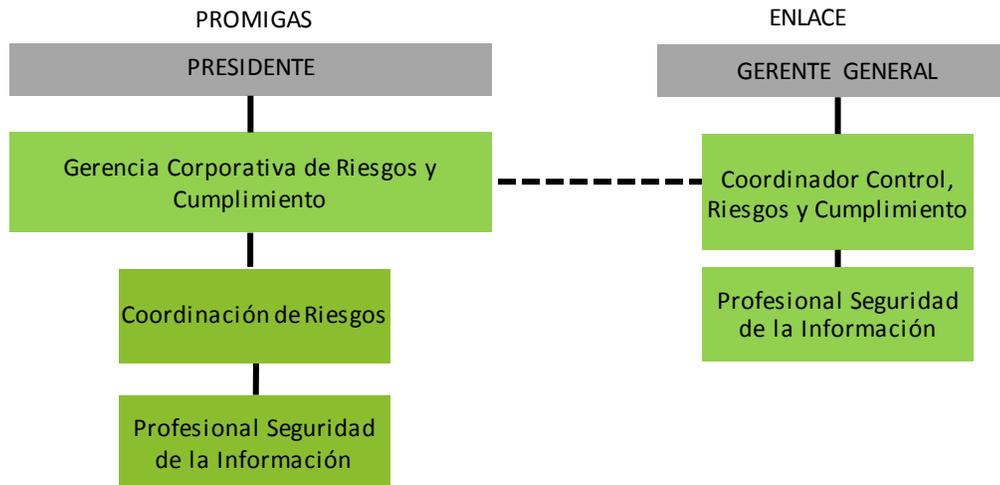
Primera línea de defensa: Conformada por las gerencias, líderes de procesos y gerentes de proyectos de la Compañía. Son los propietarios de los riesgos, incluyendo los de seguridad de la información, y quienes los gestionan. Responsables de mantener un control interno efectivo, ejecutar procedimientos de control sobre los riesgos e implementar las acciones correctivas necesarias.

Segunda línea de defensa: Conformada por los equipos responsables de liderar el proceso de gestión de riesgos en la Organización, incluyendo los de seguridad de la información, de facilitar y monitorear la implementación de prácticas efectivas de gestión de riesgos, así como también asistir a la primera línea de defensa en la definición y monitoreo de los controles necesarios para la gestión efectiva de riesgos.

Tercera línea de defensa: Conformada por los equipos de Auditoría Interna, quienes son los responsables de evaluar, de forma independiente y objetiva, la gestión de riesgos en la Organización, reportando los resultados al Comité. Su evaluación proporciona seguridad razonable sobre la eficacia del gobierno, la gestión de riesgos y del control interno, incluyendo la forma en que la primera y segunda línea de defensa logran los objetivos de gestión de riesgos y control. 5.1.1 ESTRUCTURA Y GOBIERNO DE SEGURIDAD DE LA INFORMACIÓN.

Organigrama 1. Estructura y Gobierno de Seguridad de la Información.

	POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN	
Versión: 6	Código: GNA-1656	Estado: Vigente
Elaboró: Ever Capdevila Pacheco	Revisó: Adriana Esmeral Berrío	Aprobó: Ximena Correa Agudelo
Cargo: Profesional	Cargo: Coordinador	Cargo: Gerente



5.2. ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN

A continuación, se definen los roles y responsabilidades a desarrollar por cada uno de los funcionarios que componen la organización de seguridad de la información, de manera que contribuyan a la implementación y operación de la Política de Seguridad de la Información definido para la compañía.

5.2.1. Descripción de roles y responsabilidades

5.2.1.1. Comité de Gestión Corporativa / Comité de Enlace

Responsabilidad: Mantener la calidad del proceso de seguridad de la información, con base en lo definido en esta Política, tomando las acciones preventivas, correctivas y de mejora necesarias para garantizar su correcta implementación en las compañías. Este comité se reunirá periódicamente para el desarrollo de las actividades citadas a continuación.

Actividades asociadas al Rol:

- Fomentar el desarrollo de la Organización de Seguridad de la Información.
- Velar porque se realice seguimiento y se cumplan los lineamientos definidos de Seguridad de la Información.
- Velar porque el Profesional Seguridad de la información ejecute y controle la política de Seguridad de la Información.

	POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN	
Versión: 6	Código: GNA-1656	Estado: Vigente
Elaboró: Ever Capdevila Pacheco	Revisó: Adriana Esmeral Berrío	Aprobó: Ximena Correa Agudelo
Cargo: Profesional	Cargo: Coordinador	Cargo: Gerente

Integrantes Comité de Gestión Corporativa de Promigas:

- Vicepresidente Financiero y Administrativo
- Vicepresidente de Operaciones de Transporte
- Vicepresidente de Asuntos Corporativos
- Vicepresidente de Distribución
- Vicepresidente de Negocios de Transporte
- Gerente de Recursos Humanos
- Gerente de Planeación Financiera y Estratégica
- Gerente de Medio Ambiente
- Gerente Comunicaciones
- Gerente de Mantenimiento
- Gerente Administrativo
- Gerente Corporativa de Riesgos y Cumplimiento
- Coordinador de Estrategia y Procesos (Coordinadora del Comité)

Integrantes Comité de Enlace:

- Gerente General
- Gerente Administrativo y Compras
- Gerente Financiero
- Gerente de Tecnología
- Coordinadora de Recursos Humanos
- Coordinadora de Control, Riesgos y Cumplimiento (Coordinadora del Comité)

5.2.1.2. Comité de Seguridad de la Información

Responsabilidad: Aplicar las normas, procedimientos y estándares definidos en la presente Política, apoyar los proyectos y actividades definidas por el Comité de Gestión Corporativa / Comité de Enlace en lo referente a seguridad de la información.

Actividades asociadas al Rol:

- 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.

	POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN	
Versión: 6	Código: GNA-1656	Estado: Vigente
Elaboró: Ever Capdevila Pacheco	Revisó: Adriana Esmeral Berrío	Aprobó: Ximena Correa Agudelo
Cargo: Profesional	Cargo: Coordinador	Cargo: Gerente

- Revisar y determinar las acciones a tomar ante los incidentes de seguridad de la información e informática detectados o reportados.
- Verificar el nivel de seguridad de la información por medio del análisis de los indicadores de gestión, para así tomar acciones correctivas o de mejora en caso de que se requiera.
- Velar por la ejecución de los Proyectos de Seguridad de la Información e informática periódicamente y tomar las acciones correctivas respecto a aquellos que lo requieran.
- Verificar la efectividad de los Proyectos de Seguridad de la Información.
- Velar porque las actividades cumplan con la política, procedimientos y estándares de Seguridad de la Información e informática.
- Escalar al Comité de Gestión Corporativa / Comité de Enlace los temas relevantes de seguridad de la Información e informática tratados en el Comité de Seguridad de la Información.

Integrantes Comité de Seguridad de la Información

Promigas

Principales:

- Gerente Administrativo
- Gerente Corporativa de Riesgos y Cumplimiento
- Coordinadora de Riesgos
- Coordinadora de Informática
- Profesional Seguridad de la Información (Coordinador del Comité)
- Profesional de Informática

Invitados:

- Directora de Seguridad TI – Grupo Aval
- Especialista de Seguridad TI – Grupo Aval
- Oficial de Seguridad de la Información – Corficolombiana
- Profesional de Seguridad de la Información - Enlace

Integrantes Comité de Seguridad de la Información

Enlace

Principales:

- Gerente de Tecnología
- Coordinadora de Control, Riesgos y Cumplimiento

	POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN	
Versión: 6	Código: GNA-1656	Estado: Vigente
Elaboró: Ever Capdevila Pacheco	Revisó: Adriana Esmeral Berrío	Aprobó: Ximena Correa Agudelo
Cargo: Profesional	Cargo: Coordinador	Cargo: Gerente

- Coordinador de Infraestructura
- Profesional Senior de Infraestructura
- Profesional Senior de Seguridad
- Profesional Seguridad de la Información (Coordinador del Comité)

Invitados:

- Coordinadora de Riesgos - Promigas
- Profesional de Seguridad de la Información - Promigas

Nota:
El comité podrá contar con otros invitados según los temas a tratar.

5.2.1.3. Coordinadora de Riesgos Promigas / Coordinadora de Control, Riesgos y Cumplimiento Enlace

Responsabilidad: Velar por la implementación, mantenimiento y correcto funcionamiento de la Política de Seguridad de la Información y de los procedimientos establecidos; en los activos de la información de la Compañía y bajo las directrices del Comité de Gestión Corporativa/ Comité de Enlace.

Actividades asociadas al Rol:

- Liderar la definición del plan estratégico de seguridad de la información.
- Coordinar con las áreas las actividades y proyectos encaminados al fortalecimiento del programa de gestión de seguridad de la información.
- Asegurar la apropiación de los recursos requeridos para la implementación y operación del sistema de gestión de seguridad de la información.
- Velar por la actualización de los documentos de seguridad de la información.

5.2.1.4. Coordinadora de Informática Promigas / Coordinador de Infraestructura Enlace

Responsabilidad: Velar por la implementación, mantenimiento y correcto funcionamiento de la Política de Seguridad de la Información y de los procedimientos establecidos, en los activos informáticos de la compañía, según los requerimientos de las áreas del negocio y bajo las directrices del Comité de Seguridad de la Información.

	POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN	
Versión: 6	Código: GNA-1656	Estado: Vigente
Elaboró: Ever Capdevila Pacheco	Revisó: Adriana Esmeral Berrío	Aprobó: Ximena Correa Agudelo
Cargo: Profesional	Cargo: Coordinador	Cargo: Gerente

Actividades asociadas al Rol:

- Definir el plan estratégico de seguridad informática de la compañía.
- 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 de Informática.
- Definir e implementar arquitecturas de seguridad informática definidas.
- Realizar un diagnóstico periódico de la seguridad informática en la compañía.
- Revisar la seguridad informática de los programas que se van a instalar en la compañía.
- Revisar y asegurar que los dispositivos móviles de los funcionarios o terceros no almacenen o envíen información sensible.
- Revisar los equipos borrados con el fin de validar que no sea posible recuperar información sensible de la compañía.
- Dar mantenimiento a la documentación de seguridad informática.
- Definir los controles necesarios para dar cumplimiento a las regulaciones de seguridad informática.
- Liderar proyectos que mejoren los niveles de seguridad informática, cumplan las regulaciones y mitiguen los riesgos evidenciados.
- Implementar esquemas de seguimiento y supervisión del buen uso de comandos y utilitarios sensitivos que impacten el acceso a la información.
- Participar en la gestión de incidentes de seguridad informática y en la definición de acciones correctivas para evitar la recurrencia de incidentes de seguridad informática.
- Coordinar la ejecución de análisis forense de los incidentes de seguridad informática presentados.
- Definir y verificar la implementación de los estándares de seguridad informática en las plataformas de la compañía.
- Asegurar la correcta configuración de seguridad de las herramientas de seguridad informática.
- Proponer y hacer seguimiento a indicadores de gestión de seguridad informática.
- Revisar los equipos de terceros evitando que estos presenten riesgos para la compañía.

5.2.1.5. Profesional Seguridad de la Información

Responsabilidad: Realizar las actividades requeridas para la implementación, mantenimiento y correcto funcionamiento de la Política de Seguridad de la Información y

	POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN	
Versión: 6	Código: GNA-1656	Estado: Vigente
Elaboró: Ever Capdevila Pacheco	Revisó: Adriana Esmeral Berrío	Aprobó: Ximena Correa Agudelo
Cargo: Profesional	Cargo: Coordinador	Cargo: Gerente

de los procedimientos establecidos; en los activos de la información de la compañía y bajo las directrices del Comité de Gestión Corporativa y/o Comité de Enlace.

Actividades asociadas al Rol:

- Definición del plan estratégico de seguridad de la información de la compañía en función de los objetivos del negocio.
- Participar en proyectos de seguridad de la información y liderar su ejecución al interior de la compañía.
- Proponer mejoras a la Política de Seguridad de la Información.
- Participar en las definiciones de las arquitecturas de seguridad informática.
- Revisar periódicamente la arquitectura de seguridad informática.
- Revisar periódicamente las actividades de usuarios privilegiados de los Recursos Informáticos críticos.
- Evaluar periódicamente los niveles de seguridad comparándolos contra normas de seguridad de la información.
- Definir y verificar los lineamientos y directrices de seguridad de la información a ser incluidas en el DRP.
- Coordinar el Comité Seguridad de la Información.
- Dar mantenimiento a la documentación de seguridad de la información.
- Apoyar a los líderes del proceso en la definición y verificación de los perfiles de usuario de las aplicaciones.
- Apoyar a los Líderes del Proceso en los análisis de riesgos de seguridad de la información y en la definición de los controles para mitigarlos.
- Proponer y ejecutar planes de divulgación y concientización en seguridad de la información e informática.
- Monitorear la ejecución del curso anual en Seguridad de la Información por parte de todos los empleados. Para los empleados nuevos, se realiza un monitoreo mensual a la ejecución del curso virtual de seguridad de la información como parte de su proceso de inducción
- Monitorear y controlar aspectos relacionados con la fuga de información.
- Participar en la gestión de incidentes de seguridad de la información y en la definición de acciones correctivas para evitar la recurrencia de incidentes de seguridad de la información.
- Actualizar inventario de activos de información.
- Coordinar la ejecución de análisis forense de los incidentes de seguridad de la información cuando se requiera.

	POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN	
Versión: 6	Código: GNA-1656	Estado: Vigente
Elaboró: Ever Capdevila Pacheco	Revisó: Adriana Esmeral Berrío	Aprobó: Ximena Correa Agudelo
Cargo: Profesional	Cargo: Coordinador	Cargo: Gerente

- Verificar periódicamente la correcta asignación de los usuarios y perfiles a los sistemas de información de la compañía.
- Proponer y hacer seguimiento a indicadores de gestión de seguridad de la información.
- Verificar la correcta aplicación de los controles de seguridad de acuerdo con la clasificación de la información definida.
- Definir, presentar y velar por la aprobación del presupuesto de Seguridad de la Información

5.2.1.6. Líder del Recurso

Responsabilidad: Velar por el correcto funcionamiento del recurso a su cargo, siguiendo la política de seguridad de la información y dar cumplimiento a las actividades establecidas en este documento.

Actividades asociadas al Rol:

- Autorizar la creación, modificación o retiro de códigos de usuario genéricos o privilegiados en el recurso informático bajo su responsabilidad.
- Autorizar la restauración de la información de una aplicación, de la aplicación como tal o de cualquier objeto ejecutable que forme parte de la aplicación.
- Reportar cualquier incidente o situación sospechosa que pueda perjudicar de forma alguna los principios de integridad, disponibilidad, confidencialidad de la información.
- Procurar que los usuarios del recurso informático reciban el entrenamiento necesario para la utilización de los recursos informáticos que les sean asignados.
- Autorizar la ejecución del procedimiento de control de cambios en las aplicaciones bajo su responsabilidad.
- Revisar y aprobar la matriz de segregación de funciones de la aplicación bajo su responsabilidad, con la periodicidad establecida en la Política.
- Revisar, con la periodicidad definida, los informes de usuarios de la aplicación.

5.2.1.7. Administrador del Recurso Informático

	POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN	
Versión: 6	Código: GNA-1656	Estado: Vigente
Elaboró: Ever Capdevila Pacheco	Revisó: Adriana Esmeral Berrío	Aprobó: Ximena Correa Agudelo
Cargo: Profesional	Cargo: Coordinador	Cargo: Gerente

Responsabilidad: Aplicar y mantener los controles y estándares de seguridad informática en los recursos informáticos bajo su responsabilidad, en forma acorde con la Política de Seguridad de la Información.

Actividades asociadas al Rol:

- Aplicar y mantener los parámetros de seguridad definidos en la Política de Seguridad de la información para el recurso bajo su responsabilidad.
- Identificar los riesgos de seguridad en el recurso que administra y gestionar la implementación de controles mitigatorios.
- Gestionar la actualización de la documentación de los estándares de la aplicación o plataforma tecnológica que administre.
- Justificar y documentar formalmente las excepciones a las normas y estándares establecidos.
- Administrar los perfiles, grupos y códigos de usuario en la aplicación o plataforma tecnológica bajo su responsabilidad, de acuerdo con las autorizaciones recibidas de parte de los jefes correspondientes.
- Configurar los eventos de seguridad a registrarse.
- Reportar cualquier incidente o situación sospechosa que pueda perjudicar de forma alguna los principios de integridad, disponibilidad, confidencialidad de la información.
- Participar en el diseño de un plan de acción para resolver incidentes en la seguridad y restaurar los sistemas a la situación normal.
- Informar al Coordinador de Informática, y para enlace al Coordinador de Infraestructura y al Profesional de Seguridad de la Información los incidentes de violación a la seguridad establecida.
- Revisar y hacer seguimiento regular a los informes de incidencias sobre seguridad informática generados por el sistema, analizando las posibles incidencias ocurridas.
- Realizar los informes periódicos de revisión de usuarios inactivos, permisos de usuarios y matriz de segregación de funciones.
- Mantener actualizado el listado de usuarios con privilegios especiales en la aplicación.
- Mantener actualizado el listado de interfaces de la aplicación.
- Validar y aprobar los cambios en la aplicación antes de que sean implementados en ambiente productivo.

5.2.1.8. Líder del Proceso

	POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN	
Versión: 6	Código: GNA-1656	Estado: Vigente
Elaboró: Ever Capdevila Pacheco	Revisó: Adriana Esmeral Berrío	Aprobó: Ximena Correa Agudelo
Cargo: Profesional	Cargo: Coordinador	Cargo: Gerente

Responsabilidad: El Líder del Proceso debe identificar claramente el valor de la información bajo su responsabilidad, 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.

Actividades asociadas al Rol:

- Identificar e inventariar los activos críticos de información a su cargo y mantenerlos actualizados con los requerimientos de seguridad de información.
- Clasificar los activos de información de acuerdo con su criticidad e impacto en el negocio, conforme a la Política de Seguridad de la Información, que define la clasificación de la información en la compañía.
- Clasificar la información con base en su valor, sensibilidad, riesgo de pérdida o compromiso y/o requerimientos legales de retención; y deben realizar el Análisis de Riesgos de seguridad de la información de la que son responsables, para implementar controles óptimos para resguardarlos.
- Identificar, definir y evaluar los riesgos a que pudiera estar expuesta la información a su cargo.
- Definir los controles a implementar para cada riesgo identificado siguiendo los lineamientos de la política de seguridad de la información.
- Definir y ejecutar los planes de acción para mitigar los riesgos de seguridad de la información a su cargo con apoyo del Profesional de Seguridad de la Información.
- Definir los requerimientos de Seguridad de la Información de su área, teniendo en cuenta los criterios de confidencialidad, integridad y disponibilidad.
- Definir los requerimientos de seguridad de la información de acuerdo con las necesidades del negocio.
- Mantener un nivel adecuado de conocimiento y conciencia en cuanto a la Seguridad de la Información en su área de negocio.
- Garantizar que los planes de continuidad incluyan las normas necesarias de Seguridad de la Información.
- Autorizar al Administrador de Recursos Informáticos la aplicación de los controles de seguridad a los recursos informáticos.

5.2.1.9. Usuario Final

	POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN	
Versión: 6	Código: GNA-1656	Estado: Vigente
Elaboró: Ever Capdevila Pacheco	Revisó: Adriana Esmeral Berrío	Aprobó: Ximena Correa Agudelo
Cargo: Profesional	Cargo: Coordinador	Cargo: Gerente

Responsabilidad: Todos los usuarios de la compañía son responsables de poner en práctica los programas y planes liderados por Seguridad de la Información e informática, que garanticen la protección de la información de la empresa.

Actividades asociadas al Rol:

- Dar cumplimiento a las normas establecidas en la Política de Seguridad de la Información.
- Identificar riesgos en los recursos sobre los cuales tiene acceso y generar sugerencias para mejorar las condiciones de seguridad implementadas.
- Reportar a la Coordinación de Informática y para enlace al Coordinador de Infraestructura y al Profesional de Seguridad de la Información cualquier incidente o situación sospechosa que considere puede afectar la seguridad de los equipos de cómputo o de la información.
- Tratar la información del negocio de acuerdo con el nivel de confidencialidad definido.
- Establecer claves seguras para el acceso a los recursos informáticos.

5.2.1.10. Terceros

Responsabilidad: Cumplir con las cláusulas de seguridad de información definidas en los contratos y/o acuerdos firmados por la compañía.

Actividades asociadas al Rol:

- Tramitar los permisos necesarios con el jefe de la dependencia para acceder, copiar o transmitir información de la compañía.
- Mantener e implementar los controles necesarios para proteger la integridad, confidencialidad, disponibilidad de la información.
- Proteger la información de la compañía.
- Brindar la información que sea necesaria para apoyar las labores de investigación de incidentes de seguridad de información en la compañía.

5.3. CAPACITACIÓN Y CREACIÓN DE CULTURA DE SEGURIDAD DE LA INFORMACION.

- Todos los funcionarios que ingresen a trabajar a Promigas o empresas vinculadas recibirán en su proceso de inducción, la capacitación virtual sobre seguridad de la información.

	POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN	
Versión: 6	Código: GNA-1656	Estado: Vigente
Elaboró: Ever Capdevila Pacheco	Revisó: Adriana Esmeral Berrío	Aprobó: Ximena Correa Agudelo
Cargo: Profesional	Cargo: Coordinador	Cargo: Gerente

- Todos los funcionarios anualmente recibirán una capacitación virtual sobre los aspectos claves de la política.
- La estructura de la Organización de Seguridad de la Información y las responsabilidades de sus miembros serán divulgadas periódicamente.
- Adicionalmente, se podrán realizar campañas de sensibilización y concientización del sistema de gestión de seguridad de la información, jornada de seguridad, artículos, entre otros.
- Se realizarán evaluaciones de los resultados de la inducción a fin de medir su efectividad y obtener información que permita establecer ajustes y correctivos en su diseño y ejecución.

5.4. SEGURIDAD EN EL PERSONAL

- La administración de la seguridad es responsabilidad de la compañía y no debe ser ejecutada por personal ajeno a la misma o terceras personas, sin las definiciones y directrices de seguridad de la información, las cuales deben estar alineadas al cumplimiento de todos los elementos de la Política de Seguridad de la Información.
- En todos los proyectos se debe incluir un componente de seguridad de la información, donde se identifiquen los requerimientos de confidencialidad, integridad, disponibilidad de la Organización.
- La Gerencia de Recursos Humanos, Dirección de Gestión Humana y/o Coordinación de Recursos Humanos, según corresponda, deberá realizar las verificaciones necesarias, para confirmar la veracidad de la información suministrada por el candidato, aspirante a una posición laboral en la compañía, antes de su vinculación definitiva.
- Al momento en que ingresan a la compañía, los usuarios deberán comprometerse formalmente a garantizar la confidencialidad de la información, a través de la firma de un documento que entrega la Gerencia de Recursos Humanos, Dirección de Gestión Humana y/o Coordinación de Recursos Humanos, según corresponda. Este compromiso de confidencialidad es de obligatorio cumplimiento y el no aplicarlo tendrá implicaciones disciplinarias.

	POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN	
Versión: 6	Código: GNA-1656	Estado: Vigente
Elaboró: Ever Capdevila Pacheco	Revisó: Adriana Esmeral Berrío	Aprobó: Ximena Correa Agudelo
Cargo: Profesional	Cargo: Coordinador	Cargo: Gerente

- El jefe de la dependencia deberá monitorear y reportar, de manera inmediata, la desvinculación, licencia, vacaciones o cambio de posición laboral, de los funcionarios y contratistas a la Gerencia de Recursos Humanos, Dirección de Gestión Humana y/o Coordinación de Recursos Humanos, según corresponda.
- La Gerencia de Recursos Humanos, Dirección de Gestión Humana y/o Coordinación de Recursos Humanos, enviará correo electrónico notificando la desvinculación de los funcionarios a todas las dependencias para comenzar con el respectivo procedimiento de paz y salvo.
- La Gerencia de Recursos Humanos, Dirección de Gestión Humana y/o Coordinación de Recursos Humanos, debe aplicar el proceso disciplinario, definido y aprobado por la Alta Dirección, cuando se identifiquen incumplimientos de la política de seguridad de la información, acuerdos de confidencialidad, así como cualquier otra violación de seguridad que ponga en riesgo la preservación de la confidencialidad, integridad y disponibilidad de la información.
- La compañía incluirá cláusulas de seguridad de la información en los contratos firmados con usuarios externos, relacionadas con los riesgos de pérdida de confidencialidad, integridad y disponibilidad de la información.
- La alta dirección es responsable de establecer, asignar, comunicar y formalizar a los responsables de los Activos de la información para lograr su reconocimiento a nivel institucional.

5.5. PROPIEDAD INTELECTUAL

- Todo software propiedad de la compañía debe ser identificable como tal a través de la interfaz de usuario, el manual de usuario, guía de instalación y el código fuente, e indicar el estado de protección.
- La utilización de información de la empresa para publicación en medio masivos debe ser autorizada por el responsable de la estrategia de comunicación.
- La utilización de información técnica de la empresa para publicación en literatura científica o técnica debe ser autorizada por el responsable de la estrategia de propiedad intelectual.

	POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN	
Versión: 6	Código: GNA-1656	Estado: Vigente
Elaboró: Ever Capdevila Pacheco	Revisó: Adriana Esmeral Berrío	Aprobó: Ximena Correa Agudelo
Cargo: Profesional	Cargo: Coordinador	Cargo: Gerente

- Se prohíbe el almacenamiento digital en Activos de la empresa de obras comerciales (libros, música, películas, software) de los cuales no se hayan obtenido los derechos de uso correspondientes.

5.6. CUMPLIMIENTO DE REGULACIONES EXTERNAS

- El software que reside en los Recursos Informáticos sólo podrá ser el autorizado por la Coordinación de Informática y/o Coordinación de Infraestructura en Enlace.
- La compañía deberá cumplir con las regulaciones de Seguridad de la Información vigentes en el país y con regulaciones internacionales que se le obliguen a adoptar.

5.7. ADMINISTRACIÓN DEL RIESGO EN SEGURIDAD DE LA INFORMACIÓN

- Se realiza periódicamente un Análisis de Riesgos que permita identificar los Recursos de Información críticos y orientar los esfuerzos para proteger dichos recursos.
- Todo riesgo de seguridad de la información identificado por un usuario debe ser oportunamente reportado al Profesional de Seguridad de la Información, a su jefe inmediato, a la Coordinación de Riesgos y para enlace a la Coordinación de Control, Riesgos y Cumplimiento.

5.8. CONTROL DE LOS EVENTOS DE SEGURIDAD DE LA INFORMACIÓN

- Los Recursos informáticos deben incluir registros de auditoría que involucren cualquier evento susceptible de verificación posterior e incluyan el código de usuario que lo generó.
- La Coordinación de Informática, y/o Coordinación de Infraestructura en Enlace, deberá retener los registros que contienen eventos relevantes de Seguridad de la Información por un periodo mínimo de 1 año. Durante este período, deberán protegerse los registros en archivos históricos de forma tal que no puedan modificarse y sólo puedan ser leídos por personas autorizadas.

	POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN	
Versión: 6	Código: GNA-1656	Estado: Vigente
Elaboró: Ever Capdevila Pacheco	Revisó: Adriana Esmeral Berrío	Aprobó: Ximena Correa Agudelo
Cargo: Profesional	Cargo: Coordinador	Cargo: Gerente

- La información de auditoría de los Recursos Informáticos deberá estar disponible para su uso del Profesional de Seguridad de la Información y los funcionarios de la Coordinación de Informática y/o Coordinación de Infraestructura en Enlace.
- El Profesional de Seguridad de la Información revisará de manera periódica las actividades de usuarios privilegiados de los Recursos Informáticos críticos.
- La Coordinación de Informática y/o Coordinación de Infraestructura en Enlace, garantizará que la fecha y la hora en todos los Recursos Informáticos estarán sincronizados de acuerdo con un estándar, para asegurar que los registros reflejan el tiempo exacto de ocurrencia. En el caso de que se trate de Recursos Informáticos ubicados en el exterior, se deben tener en cuenta las diferencias horarias.

5.9. ADMINISTRACION DE ALERTAS

- La Coordinación de Informática, y/o Coordinación de Infraestructura en Enlace, garantizará que todos los Recursos Informáticos críticos para el negocio estén incluidos en el monitoreo de eventos que comprometan su integridad, confidencialidad y/o disponibilidad.
- El Profesional de Seguridad de la Información define la generación y registro de alertas que permitan documentar en forma completa el evento con un nivel de detalle suficiente que facilite su detección, entendimiento, priorización, seguimiento y resolución.
- La Coordinación de Informática, y/o Coordinación de Infraestructura en Enlace, garantizará el monitoreo de alertas que faciliten su detección, notificación y seguimiento.
- La Coordinación de Informática, y/o Coordinación de Infraestructura en Enlace, utilizará herramientas que permiten la extracción y el análisis de los registros de alertas para el desarrollo de una gestión eficiente de verificación, control y seguimiento. Se utilizarán herramientas que faciliten la extracción, análisis y consolidación de alertas en Logs de auditoría y que permitan generar informes estadísticos que faciliten la identificación y seguimiento a posibles violaciones de seguridad.

	POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN	
Versión: 6	Código: GNA-1656	Estado: Vigente
Elaboró: Ever Capdevila Pacheco	Revisó: Adriana Esmeral Berrío	Aprobó: Ximena Correa Agudelo
Cargo: Profesional	Cargo: Coordinador	Cargo: Gerente

- Todos los funcionarios son responsables por reportar en forma inmediata cualquier condición anormal o vulnerabilidad que detecte en el uso los Recursos Informáticos.
- La información específica sobre las vulnerabilidades o condiciones anormales de seguridad de la información tiene carácter restringido y solo debe darse a conocer a personas autorizadas y que tengan una necesidad demostrada de saberlo.
- La compañía tiene un Procedimiento de Gestión de Incidentes de Seguridad **GPA-1664** formal de reporte de eventos o incidentes de seguridad que le permita a los usuarios, terceros y entidades, informar acerca de éstos cuando se presenten o se tenga sospecha de su ocurrencia. Las directrices establecidas deben incluir los mecanismos para responder a un Incidente de seguridad, la activación de los planes de continuidad de negocio (en caso de que aplique) y la recolección y preservación de la evidencia.
- Todo evento o incidente de seguridad debe ser tratado de principio a fin mediante un procedimiento de tratamiento de Incidentes que garanticen el análisis, investigación, documentación, solución completa y seguimiento a cualquier Incidente de seguridad. El Profesional de Seguridad de la Información evalúa los eventos de seguridad de la información, para determinar si se debe tratar como un Incidente.

5.10. CLASIFICACIÓN Y MANEJO 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, así:
 - **Restringida:** Información que es extremadamente crítica para la compañía, con alto valor para la Empresa y de manejo exclusivo de unas personas designadas dentro de la Organización.
 - **Interna:** Información sensitiva dentro, usada para propósitos del negocio por grupos específicos de Colaboradores.
 - **Pública:** Información que puede ser utilizada dentro o fuera de la Institución.

	POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN	
Versión: 6	Código: GNA-1656	Estado: Vigente
Elaboró: Ever Capdevila Pacheco	Revisó: Adriana Esmeral Berrío	Aprobó: Ximena Correa Agudelo
Cargo: Profesional	Cargo: Coordinador	Cargo: Gerente

- Toda información Restringida y almacenada en cualquier medio (físico, magnético, portable o impreso), debe ser rotulada. En el caso que la información contenga piezas con distintas categorías, esta debe rotularse con la clasificación más alta de cualquier elemento de información contenida.
- Si un recurso informático contiene información con varias categorías de clasificación, los controles usados para la protección deben reflejar la mayor de las categorías que contenga.
- Todos los usuarios deben conocer la Clasificación de la Información que utilizan para el desarrollo de sus actividades.
- La Clasificación de la Información de los clientes y accionista es Restringida o Interna, según aplique, y por ningún motivo puede volverse Pública.
- La información Restringida que se encuentre en las PC's debe ser adecuadamente protegida.
- El intercambio con entes externos de información Restringida o de Uso Interno debe hacerse únicamente con la autorización del jefe de la dependencia y aplicando los controles necesarios tales como la existencia de un acuerdo previo de términos contractuales garantizando la Confidencialidad e Integridad y controles de cifrado y certificados digitales durante el intercambio de la misma. El intercambio de información con Terceros, Entes de Control, Entidad o empresas relacionadas se debe realizar sólo si es requerido por razones de negocio.
- La información Restringida almacenada electrónicamente debe ser adecuadamente protegida. Se debe evaluar respecto al riesgo al que está expuesta, la implementación de controles tales como ser cifrada y firmada electrónicamente cuando se vaya a respaldar, guardar y transmitir.
- Cuando la información Restringida o Interna por razones de negocio deba ser desechada, se debe destruir de manera que no se pueda recuperar por ningún medio.
- Cuando un recurso informático va a estar fuera de servicio o desechado, la información almacenada en él debe ser destruida conforme a los métodos aprobados por la compañía.

	POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN	
Versión: 6	Código: GNA-1656	Estado: Vigente
Elaboró: Ever Capdevila Pacheco	Revisó: Adriana Esmeral Berrío	Aprobó: Ximena Correa Agudelo
Cargo: Profesional	Cargo: Coordinador	Cargo: Gerente

5.11. CONTINUIDAD DEL NEGOCIO

- Los planes de continuidad del negocio deberán mantener los niveles de seguridad establecidos en la Política de Seguridad de la Información, para los servicios habilitados durante el evento de contingencia. Se deberá definir una estrategia permanente de recuperación para la operatividad de los Recursos Informáticos críticos, así como desarrollar, documentar, probar y mantener los planes de recuperación que conduzcan a su restauración.
- La Coordinación de Informática, y/o Coordinación de Infraestructura en Enlace, garantizará la existencia de los usuarios en contingencia para ser utilizados en el momento en que se presente la contingencia.
- La Coordinación de Informática, y/o Coordinación de Infraestructura en Enlace, garantizarán pruebas periódicas de los medios que contienen copias de respaldo de Información restringida que incluyan la restauración y verificación de la información.
- La Coordinación de Informática, y/o Coordinación de Infraestructura en Enlace, deberá elaborar un plan de recuperación ante desastres, para el centro de datos y un conjunto de procedimientos de contingencia, recuperación y retorno a la normalidad para cada uno de los servicios, sistemas operativos y recurso informático existente.
- La Coordinación de Informática, y/o Coordinación de Infraestructura en Enlace, y el Profesional de Seguridad de la Información, deben participar activamente en las pruebas de recuperación ante desastres planificadas y efectuadas, notificando los resultados obtenidos a la Alta Dirección. Los requerimientos de seguridad de la información se encuentran definidos en el **Anexo 1** – Requerimientos de Seguridad en Continuidad del Negocio.

5.12. PROTECCION DE CODIGO MALICIOSO

- La Coordinación de Informática, y/o Coordinación de Infraestructura en Enlace, es responsable de establecer mecanismos, estándares y/o manuales de prevención, detección y corrección de Código Malicioso. Llámese Código Malicioso a todo tipo de software (incluyendo scripts y macros) diseñado para interrumpir las operaciones,

	POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN	
Versión: 6	Código: GNA-1656	Estado: Vigente
Elaboró: Ever Capdevila Pacheco	Revisó: Adriana Esmeral Berrío	Aprobó: Ximena Correa Agudelo
Cargo: Profesional	Cargo: Coordinador	Cargo: Gerente

reunir información sin autorización, acceder sin autorización a los recursos del sistema, y posiblemente otra conducta abusiva o perjudicial sobre el sistema.

- Es responsabilidad del administrador de la consola de antivirus conservar toda la documentación relacionada con la configuración de las políticas, cambios de versiones y las excepciones que se encuentren debidamente
- La Coordinación de Informática, y/o Coordinación de Infraestructura en Enlace, debe garantizar que los equipos de cómputo cuenten con las últimas definiciones y actualizaciones de antivirus y parches de seguridad aprobados.
- El agente de antivirus debe estar activo de forma permanente.
- Los usuarios no están autorizados a instalar software que interfiera con el agente antivirus, bien degradando su eficacia o impidiendo en modo alguno su correcto funcionamiento.
- El antivirus deberá estar configurado para recibir actualizaciones con una periodicidad suficiente, así como actualizaciones de emergencia, cuando sea necesario.
- El agente antivirus deberá monitorear y analizará los mensajes de correo y sus adjuntos.
- El agente de antivirus debe tener la capacidad de analizar el contenido de los medios extraíbles que se conecten a las estaciones de trabajo al momento de ser conectados.
- Se debe efectuar como mínimo revisiones o escaneos semanales del software y datos contenidos en los diferentes componentes tecnológicos que sean críticos para la operación con el fin de verificar y controlar la presencia de programas, archivos u otro tipo de Código Malicioso que pueda afectar el rendimiento y las operaciones soportadas por estos componentes.
- Cualquier alerta, Evento o situación asociada con infecciones de Código Malicioso que sea evidenciada debe ser reportada por quien lo detectó como Incidente de seguridad de la información.

	POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN	
Versión: 6	Código: GNA-1656	Estado: Vigente
Elaboró: Ever Capdevila Pacheco	Revisó: Adriana Esmeral Berrío	Aprobó: Ximena Correa Agudelo
Cargo: Profesional	Cargo: Coordinador	Cargo: Gerente

- Todo equipo de cómputo que se identifique con Código Malicioso debe ser inmediatamente evaluado y se deben tomar las respectivas medidas. En el caso que un software de Código Malicioso pueda llegar a generar un evento de mayor magnitud como la propagación del mismo hacia otros componentes o el detrimento de las redes de datos, el equipo de cómputo debe ser desconectado de la red en forma inmediata, y notificación al área afectada y al Profesional de Seguridad de la Información.

5.13. SEGURIDAD FISICA

- Las áreas físicas de la compañía se clasifican considerando la criticidad de la información que resguarden. Adicionalmente se debe desarrollar un plan de seguridad física por cada área clasificada como crítica.
- Deben existir controles estrictos para la autorización y el registro del personal que ingresa a las áreas donde se encuentren los Recursos Informáticos que contienen Activos Críticos de Información y a las áreas que trabajan con información clasificada como Restringida. El acceso a las áreas donde residen los componentes de la red de comunicación y de Recursos Informáticos que soportan actividades críticas, debe ser estrictamente controlado y restringido. El acceso debe estar permitido únicamente a personal formalmente autorizado.
- Los únicos usuarios autorizados para acceder en forma permanente al centro de cómputo son aquellos que, en virtud de sus actividades y responsabilidades, deban hacerlo. Las demás personas deberán ser previamente autorizadas y registrar tanto su ingreso como su salida.
- La información clasificada como Restringida deberá preservar las características de seguridad cuando es almacenada físicamente y por ningún motivo debe ser desatendida. La persona que genera información, con este tipo de clasificación, en un medio de almacenamiento portable es responsable por el buen uso que se haga de la misma y por el cumplimiento de las directrices que se emitan para la protección de la información. Los discos duros de los equipos portátiles donde se almacenan los datos deben ser cifrados con el fin de protegerla.
- Los medios de almacenamiento que contienen copias de respaldo de información deberán protegerse en concordancia con la Clasificación de la Información que almacenan.

	POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN	
Versión: 6	Código: GNA-1656	Estado: Vigente
Elaboró: Ever Capdevila Pacheco	Revisó: Adriana Esmeral Berrío	Aprobó: Ximena Correa Agudelo
Cargo: Profesional	Cargo: Coordinador	Cargo: Gerente

- Las áreas donde se encuentran Recursos Informáticos que contienen Activos de Información Crítica deberán contar con equipos de seguridad ambiental, procedimientos formales para su uso y controles periódicos de verificación de su estado.
- Los operadores deberán recibir capacitación en el uso de los equipos de seguridad ambiental para control de situaciones de emergencia y este conocimiento debe ser reforzado periódicamente.
- Las áreas de procesamiento de Información Restringida, y las indispensables para la operación del negocio, deberán contar con circuitos alternos y equipo de respaldo para suministro de energía con los procedimientos y la capacitación del personal para su correcto uso.
- Se deberán establecer mecanismos y responsabilidades frente a la administración centralizada de las llaves físicas que permiten el ingreso a las áreas de acceso restringido, a los muebles donde se guardan componentes críticos de red y las áreas que almacenan Activos Críticos de Información.
- Se establecen controles específicos y de obligatorio cumplimiento para el acceso de visitantes a áreas de acceso restringido. Únicamente el personal de la compañía, formalmente autorizado, puede acceder a las áreas restringidas en función de las actividades que desarrolla. En el caso que funcionarios de otras áreas y/o de entes externos requieran ingresar a estas áreas, deben obtener autorización del Responsable del Área Crítica y seguir los procedimientos establecidos.
- Los registros de acceso y alertas de intento de violación a las áreas protegidas deben ser revisados periódicamente por el responsable del área. Las bitácoras de visitas y los reportes de alertas de intento de acceso no autorizado a las áreas de acceso restringido deben ser revisados de manera exhaustiva por el Responsable del área y los permisos registrados deben ser validados.
- Se establecen y se ejecutan los mantenimientos preventivos y correctivos de acuerdo a lo establecido por los fabricantes y además se deberá llevar los registros que cubra todos los Recursos Informáticos.

	POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN	
Versión: 6	Código: GNA-1656	Estado: Vigente
Elaboró: Ever Capdevila Pacheco	Revisó: Adriana Esmeral Berrío	Aprobó: Ximena Correa Agudelo
Cargo: Profesional	Cargo: Coordinador	Cargo: Gerente

- Todos los cambios estructurales dentro de los lugares destinados al procesamiento de datos y/o almacenamiento de Recursos Informáticos críticos deben ser programados y desarrollados de acuerdo con un plan, observando las medidas de seguridad necesarias para la protección de los equipos.
- Está prohibido consumir alimentos en las áreas de acceso restringido que contienen Recursos Informáticos críticos.

5.14. SEGURIDAD DE LA INFORMACIÓN EN LOS PROCESOS DE ADMINISTRACIÓN DE SISTEMAS

- 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 Estándares de Seguridad de Recursos Informáticos **PPA-786**, o documento equivalente para las demás empresas vinculadas. 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 compañía implementará un proceso de gestión de las vulnerabilidades técnicas de su plataforma tecnológica que incluya los responsables en su gestión, las acciones a implementar y el plazo para la mitigación.
- Las adquisiciones y desarrollos de mantenimiento de software realizado por personal interno o por terceros deben cumplir con el Procedimiento de Adquisición e Implantación de Soluciones Informáticas **PPA-761** y el Procedimiento de Control de Cambios en Recursos de IT **PPA-727** que incluye los requerimientos de seguridad de la información, o documento equivalente para las empresas.
- Los requerimientos de seguridad de la información deben ser cumplidos durante todo el ciclo de desarrollo y mantenimiento de software y éstos deben ser integrados desde

	POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN	
Versión: 6	Código: GNA-1656	Estado: Vigente
Elaboró: Ever Capdevila Pacheco	Revisó: Adriana Esmeral Berrío	Aprobó: Ximena Correa Agudelo
Cargo: Profesional	Cargo: Coordinador	Cargo: Gerente

el principio como parte de la solución y deben ser verificados previos a su puesta en producción.

- La puesta en producción de nuevos desarrollos o modificación de aplicativos es permitida únicamente si estos cumplen con lo establecido en el Procedimiento de Control de Cambios en Recursos de IT **PPA-727**, o documento equivalente para las demás empresas vinculadas. La implementación de nuevos aplicativos que no contemplen los mecanismos mínimos de seguridad establecido en el Procedimiento de Adquisición e Implantación de Soluciones Informáticas **PPA-761**, o documento equivalente para las empresas vinculadas.
- La compañía garantiza ambientes separados de desarrollo, pruebas y producción cuando se requieran realizar cambios en los Recursos Informáticos. Para lo cual mantiene controles físicos y de acceso lógico para asegurar dicha separación.
- Los aplicativos de la compañía y sus modificaciones deberán cumplir con el proceso de revisión por el administrador de la aplicación en el ambiente de pruebas, antes de ser liberados a producción.
- La información de producción sólo deberá ser utilizada en ambientes de desarrollo o pruebas, con los debidos controles para proteger su confidencialidad.

5.15. IDENTIFICACIÓN Y AUTENTICACIÓN INDIVIDUAL

- Cada funcionario tiene asignado un único código de usuario para obtener acceso a cada una de las plataformas y aplicaciones que utilice.
- Los usuarios de los Recursos Informáticos no deben compartir su código de usuario/contraseña o cualquier mecanismo otorgado para su identificación y autenticación. La responsabilidad que un usuario adquiere al recibir su código de usuario/contraseña o cualquier mecanismo de identificación y autenticación se extiende a todo tipo de interacción que ese identificador tenga con el sistema.
- Para el acceso a cualquier Recurso Informático mediante la red, pública o privada, se requiere un proceso de identificación y autenticación del funcionario o del programa al que se accede; este proceso será parte del sistema de identificación y autenticación.

	POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN	
Versión: 6	Código: GNA-1656	Estado: Vigente
Elaboró: Ever Capdevila Pacheco	Revisó: Adriana Esmeral Berrío	Aprobó: Ximena Correa Agudelo
Cargo: Profesional	Cargo: Coordinador	Cargo: Gerente

- Todos los funcionarios deberán acceder a través de la VPN a los Recursos Informáticos cuando se encuentren fuera de la red corporativa.
- Todos los Recursos Informáticos deben disponer de los mecanismos que soliciten la identificación y autenticación al usuario o a los programas que pretendan accederlos.
- Toda la creación, eliminación y actividades de los códigos de usuarios, deben mantener la información histórica de los Logs.
- La desactivación de un código de usuario debe realizarse previa solicitud de recursos humanos una vez ha finalizado la vinculación laboral.
- La asignación de privilegios de acceso a la información debe ser autorizada mediante un proceso formal del jefe de la dependencia. En general los usuarios con privilegios especiales deben usar métodos de acceso y comunicación seguros y sus acciones deben ser monitoreadas de manera periódica.
- A todos los códigos de usuario que vienen por defecto con los sistemas operativos, bases de datos y productos de las diferentes plataformas se les debe restringir el acceso siempre que sea posible o cuando no exista restricción técnica para tal fin.
- Todas las contraseñas deberán ser creadas de acuerdo con el documento Estándares de Seguridad de Recursos Informáticos **PPA-786**, o documento equivalente para las demás empresas vinculadas. Se puede tener el apoyo de herramientas automáticas que aseguren el cumplimiento del estándar de creación de contraseñas.
- Las contraseñas o cualquier otro método de autenticación son clasificados como información Restringida y esta condición se debe mantener desde su creación hasta su eliminación. En particular la contraseña no debe escribirse o almacenarse en medios que puedan ser leídos por otras personas. Por su carácter de Restringida es, adicionalmente, personal e intransferible.
- La asignación de contraseñas deberá ser controlada por un proceso de administración formal que permita:
 - Obtener el compromiso escrito de los usuarios de mantener la confidencialidad de las contraseñas.

	POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN	
Versión: 6	Código: GNA-1656	Estado: Vigente
Elaboró: Ever Capdevila Pacheco	Revisó: Adriana Esmeral Berrío	Aprobó: Ximena Correa Agudelo
Cargo: Profesional	Cargo: Coordinador	Cargo: Gerente

- Asegurar que los usuarios acaten los estándares y recomendaciones para la elección y el cambio de contraseñas.
 - Notificar de manera segura las contraseñas temporales/iniciales a los usuarios.
 - Confirmar la recepción de las contraseñas por parte de los usuarios
- Están prohibidos la suplantación, el Enmascaramiento o la firma por otros usuarios para el acceso a cualquier recurso informático. Los usuarios deben usar siempre su código de usuario para acceder a los recursos informáticos, incluso si deben hacerlo desde una estación diferente a la asignada.
 - Las contraseñas usadas para acceder a los Recursos Informáticos deberán ser cambiadas periódicamente. La contraseña debe tener una vigencia mínima de tiempo luego del cual el usuario puede realizar un cambio de contraseña, la cual vencerá automáticamente después de transcurrida la vigencia máxima establecida. Un usuario con contraseña vencida requiere ingresar una nueva contraseña para acceder a los Recursos Informáticos. El usuario debe ser informado previamente al vencimiento de su contraseña. Se debe llevar un registro histórico de las últimas contraseñas para evitar que las mismas sean repetidas después de un cierto número de cambios.
 - El cambio de contraseña debe ser solicitado en forma automática cuando un usuario acceda a los Recursos Informáticos por primera vez, cuando la vigencia de la contraseña haya expirado o cuando la contraseña haya sido reinicializada. Este procedimiento también estará disponible para que pueda ser realizado manualmente por el usuario cuando lo estime conveniente.
 - Se deshabilitará el acceso de los usuarios que se ausenten por novedades de nómina (licencia, vacaciones, incapacidades, entre otras) por un período mayor a 5 días hábiles.
 - Las contraseñas son bloqueadas después de un número definido de intentos fallidos definido en el Estándar de Seguridad de Recursos Informáticos **PPA-786**, o documento equivalente para las empresas vinculadas.

	POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN	
Versión: 6	Código: GNA-1656	Estado: Vigente
Elaboró: Ever Capdevila Pacheco	Revisó: Adriana Esmeral Berrío	Aprobó: Ximena Correa Agudelo
Cargo: Profesional	Cargo: Coordinador	Cargo: Gerente

- La reactivación del acceso a los usuarios de cualquier plataforma deberá ser autorizada según el nivel establecido en el procedimiento **PPA-212-S2**, o documento equivalente para las empresas vinculadas.

5.16. CONTROL Y ADMINISTRACIÓN DEL ACCESO A LA INFORMACIÓN

- Los accesos a la información, por parte de los usuarios, deben ser definidos y autorizados por el jefe de la dependencia y deben estar basados en requerimientos específicos del negocio.
- Con el objeto de prevenir el acceso no autorizado a la información contenida en los Recursos Informáticos, se deberá establecer controles de acceso lógico que permitan el acceso únicamente a los usuarios autorizados. Los Recursos Informáticos deben:
 - Controlar los accesos de usuarios a los datos conforme a los lineamientos de control de acceso definidas por la compañía.
 - Proveer la protección del acceso no autorizado a cualquiera de los utilitarios del software operativo o de soporte de los aplicativos que sea capaz de modificar los parámetros del sistema o de la aplicación.
 - Evitar comprometer la seguridad de otros Recursos Informáticos que sean compartidos con otras aplicaciones.
- Los permisos de acceso a los aplicativos deben ser garantizados a grupos de usuarios y no a individuos. Se deberán otorgar permisos de acceso a los Recursos Informáticos en función de grupos. Estos grupos deberán ser conformados por individuos cuyo rol, responsabilidad y actividades sean equivalentes. Cada grupo debe ser asociado a un perfil de acceso autorizado por el jefe de la dependencia y los usuarios a quienes sea asignado un mismo perfil contarán con los mismos privilegios.
- Los jefes de la dependencia realizan la solicitud de creación/modificación de usuarios a través del formato **FA-432**, o documento equivalente para Enlace y las demás empresas vinculadas; y los administradores de recursos asignan los permisos de acuerdo con esta solicitud. Cuando un empleado se retire o cambie de rol/cargo o un usuario externo que termine las labores, se deben eliminar o reasignar sus privilegios de acceso a los Recursos Informáticos.

	POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN	
Versión: 6	Código: GNA-1656	Estado: Vigente
Elaboró: Ever Capdevila Pacheco	Revisó: Adriana Esmeral Berrío	Aprobó: Ximena Correa Agudelo
Cargo: Profesional	Cargo: Coordinador	Cargo: Gerente

- Los privilegios de los usuarios de los Recursos Informáticos deberán ser manejados y controlados centralizadamente, de acuerdo con los lineamientos de esta Política.
- El jefe de la dependencia deberá realizar una comparación anual entre los requerimientos de acceso de los usuarios a los aplicativos y el nivel de acceso con que en realidad cuentan y verificar que los usuarios que efectivamente acceden la información corresponden a los autorizados previamente por él.
- La información Restringida que está en producción no debe ser utilizada en los ambientes de desarrollo o pruebas.
- El único acceso a los datos de producción son los aplicativos. Cualquier otro modo de acceso a los datos, deberá ser plenamente justificado y documentado.
- Los ambientes de desarrollo, pruebas y producción de los recursos informáticos deben estar separados siguiendo al menos los siguientes requisitos:
 - a) Los programas fuente, objeto y los datos de un ambiente son independientes de los de otro ambiente.
 - b) La ejecución de procesos o procedimientos en un ambiente no debe afectar a los otros ambientes.
 - c) El acceso otorgado a un ambiente no permite el acceso a los otros.
- La utilización de Utilitarios Sensitivos deberá ser restringido a Usuarios Privilegiados que por su rol requieran su aplicación. Los Eventos asociados a su uso deben ser incluidos en el Log del sistema para que puedan ser verificados y controlados en forma periódica.
- Por defecto a todos los funcionarios se les desactivará los puertos USB desde la entrega del equipo y sólo aquellos que sean requeridos por necesidad del negocio y/o proceso podrán ser habilitados previa justificación del Gerente de la dependencia y la aprobación del Profesional de Seguridad de la Información
- Todos los funcionarios tienen prohibido el envío de información de la compañía a correos electrónicos personales como Gmail, Hotmail, Yahoo, iCloud, entre otros, y

	POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN	
Versión: 6	Código: GNA-1656	Estado: Vigente
Elaboró: Ever Capdevila Pacheco	Revisó: Adriana Esmeral Berrío	Aprobó: Ximena Correa Agudelo
Cargo: Profesional	Cargo: Coordinador	Cargo: Gerente

sólo serán autorizados aquellos correos que sean requeridos por necesidad del negocio y/o proceso, previa justificación del Gerente de la dependencia y aprobación del Profesional de Seguridad de la Información.

- Para proteger la información almacenada en Carpetas Compartidas creadas en los servidores, el responsable de dicha Información debe definir los usuarios y los permisos de acceso que deben tener (control total, lectura, escritura). Se deberá evitar el uso de carpetas compartidas con permisos a todos los usuarios (“todos”) y que sean creadas directamente en los equipos PC’s.
- El proceso de toma de control remoto de equipos se deberá efectuar únicamente con las herramientas autorizadas y su uso debe ser restringido; el proceso debe ser aprobado previamente por el usuario. Lo anterior aplica tanto para las herramientas utilizadas a nivel interno (Ej. para brindar soporte a usuarios finales), así como también para las herramientas para la toma de control remoto que se requiera por parte de terceros.

5.17. TERCEROS QUE ACCEDEN INFORMACIÓN

- Se deberá incluir cláusulas de seguridad de información en los contratos firmados con entes externos relacionados con los riesgos de pérdida de confidencialidad, integridad y disponibilidad de la información. Los acuerdos o cláusulas de confidencialidad deberán incluir como mínimo lo siguiente (Según aplique):
 - La obligación de proteger la privacidad de la información verbal, escrita, o en cualquier otro medio que se encuentre, restringiendo su uso exclusivamente al personal que tenga absoluta necesidad de conocerla y para los efectos que se determinen en el contrato. De igual forma se deberá garantizar que las personas que tengan acceso a la información restringida conozcan su carácter de confidencialidad y aseguren su tratamiento, y el compromiso de que será utilizada única y exclusivamente para los fines estipulados en el contrato.
 - De acuerdo con el objeto del contrato, se deben definir los niveles de servicio en cuanto a seguridad de la información, para cumplir por parte del tercero.
 - La titularidad de que la información que sea entrega, procesada o resultante de la ejecución del contrato, pertenece a la compañía o de sus clientes o usuarios.

	POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN	
Versión: 6	Código: GNA-1656	Estado: Vigente
Elaboró: Ever Capdevila Pacheco	Revisó: Adriana Esmeral Berrío	Aprobó: Ximena Correa Agudelo
Cargo: Profesional	Cargo: Coordinador	Cargo: Gerente

- Restricciones sobre el software empleado durante la ejecución del contrato, garantizando que dicho software cumple con los requisitos de Derechos de Autor.
- Restricciones sobre el software desarrollado que indiquen los controles a implementar con el fin de prevenir el uso de Código Malicioso.
- Cláusulas contractuales que especifican la propiedad de la información que se transmite por redes públicas.
- El acceso de entes externos a los Activos de Información deberá cumplir con las siguientes condiciones:
 - Solicitud del jefe de la dependencia mediante el Formato Creación de Código de Usuarios **FA -432**, o documento equivalente para Enlace y las empresas vinculadas.
 - Tener asignados identificadores únicos y claramente reconocibles para el acceso a los Recursos Informáticos.
 - Están implementados los procedimientos de supervisión y control de las actividades del tercero.
 - Los Recursos Informáticos empleados por el tercero en el suministro del servicio han sido homologados y aprobados por la compañía.
- El administrador del recurso, en coordinación con el jefe de la dependencia, deberá realizar periódicamente una revisión formal de los derechos de acceso de los usuarios de entes externos que acceden información de la compañía.
- Se deberá evaluar regularmente el cumplimiento de los compromisos de seguridad de la información por parte de terceros y contratistas.

5.18. SEGURIDAD EN LAS REDES

- Se deben definir zonas de red separadas que agrupen lógicamente los recursos informáticos, de acuerdo con la criticidad de los activos de información que se

	POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN	
Versión: 6	Código: GNA-1656	Estado: Vigente
Elaboró: Ever Capdevila Pacheco	Revisó: Adriana Esmeral Berrío	Aprobó: Ximena Correa Agudelo
Cargo: Profesional	Cargo: Coordinador	Cargo: Gerente

manejen en cada segmento. En cada zona se deben implantar controles de acceso consecuentes con la clasificación de la información que allí reside.

- Los Firewall (centralizados o descentralizados) definidos por la compañía son los únicos puntos autorizados para el establecimiento de conexiones de cualquier Recurso Informático de la empresa con redes externas. No se permite, en ninguna circunstancia, establecer conexiones directas hacia redes externas desde los recursos informáticos
- La información técnica de la red de datos (direcciones internas, configuración y diseño de la red) está clasificada como restringida y por lo tanto sólo está disponible para el personal autorizado que tenga necesidad legítima de conocerla y con una previa autorización explícita del responsable de la Información.
- Se debe contar con mecanismos que controlen el enrutamiento en la red. El acceso a los recursos informáticos desde redes externas o internas requiere que se verifique y controle que el acceso sea realizado exclusivamente sobre los recursos informáticos autorizados.
- Los accesos desde puntos remotos o redes externas deben contar con mecanismos de autenticación y control de acceso de la conexión que prevengan posibles accesos no autorizados.
- El acceso remoto a la red de datos corporativa sólo puede ser autorizado por el responsable de la Información, previa evaluación de una razón justificada del negocio. Las actividades realizadas deben quedar registradas en un log de auditoría y los permisos del usuario deben estar restringidos específicamente a la actividad particular a realizar.
- Los equipos desde los que se accede remotamente deben estar aprobados por la compañía, previa validación de que la tecnología y la configuración de los equipos cumplan con los Estándares de Seguridad Informática definidos.
- Deben considerarse controles que limiten el acceso a operaciones específicas, permitiendo el acceso únicamente a la información absolutamente necesaria y controlando el uso de utilitarios en los recursos informáticos. Algunos controles a tener en cuenta son:

	POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN	
Versión: 6	Código: GNA-1656	Estado: Vigente
Elaboró: Ever Capdevila Pacheco	Revisó: Adriana Esmeral Berrío	Aprobó: Ximena Correa Agudelo
Cargo: Profesional	Cargo: Coordinador	Cargo: Gerente

- a) Obligar el paso de toda comunicación remota a través de los componentes de seguridad (firewalls, analizador de contenido) para restringir el uso de comandos sensitivos.
 - b) Incorporar mecanismos de autenticación de la conexión que prevengan accesos no autorizados.
 - c) Registrar en el log de auditoría las actividades realizadas mediante esta conexión.
- El acceso desde la red de datos corporativa a otras redes externas, mediante módems, módems inalámbricos o Access Points no administrados por la compañía, entre otros, sólo debe realizarse por razones estrictas de negocio y desde equipos desconectados de la red corporativa.
 - Para los equipos móviles que almacenen información confidencial de la Compañía se deben definir e implementar la protección física requerida, los controles de acceso, las técnicas de cifrado, las copias de respaldo, la protección contra virus o código malicioso, las reglas para conexión a las redes y las directrices para el uso del equipo móvil en lugares públicos.
 - Se deben considerar en la arquitectura de la red los mecanismos apropiados que minimicen la probabilidad de que la información que fluye en la red pueda ser alterada.
 - Todo usuario debe ser consciente y cumplir las normas de seguridad de la información establecida, cuando hace uso de los servicios de Internet e Intranet, e igualmente debe velar por el cumplimiento de las normas establecidas por las redes remotas a las cuales se conecta. Los usuarios son absolutamente responsables de la utilización que hagan de dichos servicios y por las consecuencias que se deriven de su incorrecta utilización.
 - El Profesional de Seguridad de la Información y la Coordinación de Informática, y/o Coordinación de Infraestructura en Enlace, son los autorizados para la divulgación al interior de la empresa, de mensajes de advertencias de seguridad de la Información e Informática.

	POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN	
Versión: 6	Código: GNA-1656	Estado: Vigente
Elaboró: Ever Capdevila Pacheco	Revisó: Adriana Esmeral Berrío	Aprobó: Ximena Correa Agudelo
Cargo: Profesional	Cargo: Coordinador	Cargo: Gerente

- Todo correo recibido con alertas sobre un supuesto virus o la existencia de código dañino dentro en algún recurso informático debe ser verificado con el Líder de TI y Profesional de Seguridad de la Información.

5.19. ESCRITORIO LIMPIO Y PANTALLA LIMPIA

- Toda la información clasificada como “Restringida” debe conservarse en lugares seguros cuando no se esté utilizando (cajas fuertes, archivadores, etc.). En los escritorios de los PC’s y servidores no debe permanecer información “Restringida” para evitar su acceso no autorizado.
- Con el fin de proteger la información el usuario deberá bloquear la sesión de trabajo cuando se ausente de su puesto de trabajo y requiera dejar su computador en posición de encendido.
- Toda información impresa y/o en medios magnéticos que no esté siendo utilizada deberá ser asegurada en forma adecuada, usando para esto archivadores, cajas fuertes o muebles destinados para su almacenamiento.
- Todo funcionario que tenga acceso a información Restringida en medios físicos deberá prevenir la divulgación no autorizada de la misma a personas que trabajen en ambientes o módulos de trabajo cercano o ajeno a la compañía.
- Es responsabilidad de los funcionarios retirar de forma inmediata cualquier tipo de documento enviado a las impresoras dispuestas para tal fin.
- Todo documento que contenga información clasificada como Restringida no podrá ser reciclado; deberá ser destruido utilizando medios que impidan la reconstrucción de dicha información.

5.20. DISPOSITIVOS MOVILES

- La Coordinación de Informática, y/o Coordinación de Infraestructura en Enlace, debe evaluar las opciones de protección de los dispositivos móviles de la Compañía y personales, que hagan uso de los servicios provistos por la empresa.

	POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN	
Versión: 6	Código: GNA-1656	Estado: Vigente
Elaboró: Ever Capdevila Pacheco	Revisó: Adriana Esmeral Berrío	Aprobó: Ximena Correa Agudelo
Cargo: Profesional	Cargo: Coordinador	Cargo: Gerente

- La Coordinación de Informática, y/o Coordinación de Infraestructura en Enlace, deberá establecer las configuraciones aceptables, para los dispositivos móviles o personales, que hagan uso de los servicios provistos por la compañía.
- La Coordinación de Informática, y/o Coordinación de Infraestructura en Enlace, deberá establecer un método de bloqueo (por ejemplo, contraseñas, biométricos, patrones, etc.) para los dispositivos móviles de la compañía, que serán entregados a los usuarios. Se debe configurar estos dispositivos para que pasado un tiempo de inactividad pasen automáticamente a modo de suspensión y, en consecuencia, se active el bloqueo de la pantalla el cual requerirá el método de desbloqueo configurado.
- La Coordinación de Informática, y/o Coordinación de Infraestructura en Enlace, deberá activar la opción de cifrado de la memoria de almacenamiento de los dispositivos móviles de la compañía, haciendo imposible la copia o extracción de datos, si no se conoce el método de desbloqueo.
- La Coordinación de Informática, y/o Coordinación de Infraestructura en Enlace, deberá configurar la opción de borrado remoto de información, en los dispositivos móviles de la compañía, con el fin de eliminar los datos de dichos dispositivos y restaurarlos a los valores de fábrica, de forma remota, evitando así divulgación no autorizada de información en caso de pérdida o hurto.
- Los funcionarios deben evitar conectar los dispositivos móviles de la compañía asignados, por puerto USB, a cualquier computador público, de hoteles o cafés internet, entre otros.
- Los funcionarios deben evitar hacer uso de redes inalámbricas de uso público, así como deben desactivar las redes inalámbricas como WIFI, Bluetooth, o infrarrojos en los dispositivos móviles de la compañía asignados.
- Los funcionarios no deben modificar las configuraciones de seguridad de los dispositivos móviles de la compañía bajo su responsabilidad, ni desinstalar el software provisto con ellos al momento de su entrega.
- Cada vez que el sistema de sus dispositivos móviles de la compañía notifique de una actualización disponible, los funcionarios deberán aceptarla y aplicar la nueva versión.

	POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN	
Versión: 6	Código: GNA-1656	Estado: Vigente
Elaboró: Ever Capdevila Pacheco	Revisó: Adriana Esmeral Berrío	Aprobó: Ximena Correa Agudelo
Cargo: Profesional	Cargo: Coordinador	Cargo: Gerente

5.21. USO ADECUADO DE INTERNET

- La Coordinación de Informática, y/o Coordinación de Infraestructura en Enlace, debe definir e implementar controles, para evitar la descarga de software no autorizado y/o código malicioso, proveniente de Internet y evitar el acceso a sitios catalogados como restringidos o no gratos para la compañía.
- No se autoriza la instalación de software espía o similares en los equipos.
- No está permitida la descarga y/o instalación de herramientas que permitan vulnerar algún tipo de sistema (Hacking Tools).
- El acceso a Internet debe ser moderado y no debe afectar sus responsabilidades laborales, se asume que el funcionario es responsable y autónomo de administrar su tiempo.
- Ningún funcionario debe acceder a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página web que vaya en contra de la ética moral, las leyes vigentes.
- Todos los funcionarios tienen prohibido el acceso y el uso de servicios interactivos comunitarios o mensajería instantánea o almacenamiento en la nube, como Facebook, Instagram, Twitter, WhatsApp Web, Hotmail, Gmail, Yahoo, Outlook, Dropbox, Google Drive, OneDrive Personal, paginas catalogadas como entretenimiento, y otras similares. En caso de requerir el acceso debe ser previamente justificada por el Gerente de la dependencia y aprobada por el Profesional de Seguridad de la Información.
- Los funcionarios no deben descargar, usar, intercambiar y/o instalar juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de los autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica y sistemas de información de la compañía.

6. DOCUMENTOS DE REFERENCIA Y ANEXOS

	POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN	
Versión: 6	Código: GNA-1656	Estado: Vigente
Elaboró: Ever Capdevila Pacheco	Revisó: Adriana Esmeral Berrío	Aprobó: Ximena Correa Agudelo
Cargo: Profesional	Cargo: Coordinador	Cargo: Gerente

Se enuncian los documentos de Promigas relacionados con esta Política:

Anexo 1 – Requerimientos de Seguridad de la Información en Continuidad del Negocio

PIA – 1661 – Glosario de Seguridad de la Información

PPA-786 – Estándar de Seguridad de Recursos Informáticos

PPA-761 - Procedimiento de Adquisición e Implantaciones de Soluciones Informáticas

PPA-212-S2 – Procedimiento de Administración de Código de Usuarios y Claves de Acceso

FA -432 – Formato Creación de Código de Usuarios

PPA-727-Procedimiento de Control de Cambios en Recursos de IT

PNA-744- Política de Informática

GNA-1651 - Política de Protección de Datos Personales

PNA-1863 - Requisitos de Seguridad Para Proyectos de Sistemas de Información

7. CONTROL DE CAMBIOS

Cambios de la versión 5 – Junio 2019

Se realizaron modificación a los siguientes lineamientos:

- Es responsabilidad del administrador de la consola de antivirus conservar toda la documentación relacionada con la configuración de las políticas, cambios de versiones y las excepciones que se encuentren debidamente aprobadas.
- Todos los funcionarios deberán acceder a través de la VPN a los Recursos Informáticos cuando se encuentren fuera de la red corporativa.
- Se deshabilitará el acceso de los usuarios que se ausenten por novedades de nómina (licencia, vacaciones, incapacidades, entre otras) por un período mayo a 5 días hábiles.
- Por defecto a todos los funcionarios se les desactivará los puertos USB desde la entrega del equipo y sólo aquellos que sean requeridos por necesidad del negocio y/o proceso podrán ser habilitados previa justificación del Gerente de la dependencia y aprobación del Profesional de Seguridad de la Información.
- Todos los funcionarios tienen prohibido el envío de información de la compañía a correos electrónicos personales como Gmail, Hotmail, Yahoo, iCloud, entre otros, y sólo serán autorizados aquellos correos que sean requeridos por necesidad del negocio y/o proceso, previa justificación del Gerente de la dependencia y aprobación del Profesional de Seguridad de la Información.
- Todos los funcionarios tienen prohibido el acceso y el uso de servicios interactivos comunitarios o mensajería instantánea o almacenamiento en la nube, como Facebook, Instagram, Twitter, WhatsApp Web, Hotmail, Gmail, Yahoo, Outlook, Dropbox, Google Drive, OneDrive Personal, paginas catalogadas como entretenimiento, y otras similares. En caso de requerir el acceso debe ser previamente justificada por el

	POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN	
Versión: 6	Código: GNA-1656	Estado: Vigente
Elaboró: Ever Capdevila Pacheco	Revisó: Adriana Esmeral Berrío	Aprobó: Ximena Correa Agudelo
Cargo: Profesional	Cargo: Coordinador	Cargo: Gerente

Gerente de la dependencia y aprobada por el Profesional de Seguridad de la Información.

Solicitud No. 11993

Cambios de la versión 4 – Abril 2019

- Se incluyó en las funciones del Profesional de Seguridad de la Información, el monitoreo a los cursos de seguridad de la Información para los empleados.
- Se incluyeron los Requisitos de Seguridad Para Proyectos de Sistemas de Información.

No. Solicitud: 11701

Cambios de la versión 3 – Diciembre 2018

- Se incluye en el alcance a ENLACE SERVICIOS COMPARTIDOS y a las demás empresas vinculadas.
- Se incluyeron los cargos equivalentes para ENLACE SERVICIOS COMPARTIDOS.
- **No. Solicitud: 10885**