TABLA DE CONTENIDO

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

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.

4.1. ACTUALIZACION

La gerencia corporativa de riesgo y cumplimiento es responsable de modificar o actualizar las directrices señaladas en este documento. El comité de seguridad de la información podrá revisar y emitir conceptos sobre las propuestas de ajustes o cambios en la política de seguridad de la información.

Para efectos de asegurar su vigencia, suficiencia y nivel de eficacia, este documento se debe mantener actualizado, por lo cual se define que se debe revisar en su totalidad por el Profesional de Seguridad de la Información de Promigas anualmente o antes si se identifican circunstancias que ameriten su modificación.

4.2. 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.

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.

4.3. 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.

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.

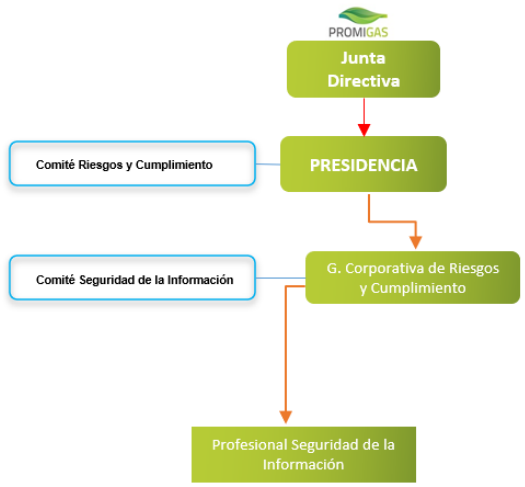

Imagen1: Estructura y Gobierno de Seguridad de la Información.

5.2. ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN

Para dar cumplimiento al objetivo de la Política Corporativa de Seguridad de la Información, 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.

5.2.1. Descripción de roles y responsabilidades

5.2.1.1. Comité de Riesgos y Cumplimiento

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.

Integrantes Comité de Riesgos y Cumplimiento:

- Presidente
- Vicepresidente Financiero y Administrativo
- Vicepresidente de Operaciones de Transporte
- Vicepresidente de Asuntos Corporativos
- Vicepresidente de Negocios Distribución
- Vicepresidente de Negocios de Transporte
- Gerente Corporativa de Riesgos y Cumplimiento
- Coordinador de Riesgo
- Coordinador de Cumplimiento
- Profesional Seguridad de la Información

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 Riesgos y Cumplimiento 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.

- 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 Riesgos y Cumplimiento 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
Principales

- Gerente Corporativa de Riesgos y Cumplimiento
- Gerente de Tecnología
- Coordinador de Infraestructura
- Profesionales 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

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

5.2.1.3. Gerente Corporativa de Riesgo y Cumplimiento

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 Riesgos y Cumplimiento.

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. Coordinador de Infraestructura

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

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 Corporativa de Seguridad de la Información.
- Implementar y mantener arquitecturas de seguridad informática establecidas.
- 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.
- Asegurar la implementación de medidas de seguridad informática requeridas para mantener un adecuado uso de la información corporativa a través de dispositivos móviles.
- Dar mantenimiento a la documentación de seguridad informática.
- Definir y mantener 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.
- 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.

5.2.1.5. Profesional Seguridad de la Información

Responsabilidad: Realizarlas actividades requeridas para 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 y/o Comité de Enlace.

Actividades asociadas al Rol:

- Definir el plan estratégico de seguridad de la información de la compañía en función de los objetivos del negocio.
- Participar en proyectos del negocio que puedan representar impactos en seguridad de la información y velar por que se mantenga el ambiente de control sobre estos al interior de la compañía.
- Proponer mejoras a la Política Corporativa 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 Lideres 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.
- 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. Profesional de Informática/Profesional Senior Seguridad TI

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:

- 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.
- Garantizar la configuración de los registros o logs de seguridad en las diferentes aplicaciones del negocio, en las cuales se involucren activos de información de clasificación restringida.
- Reportar cualquier incidente o situación sospechosa que pueda perjudicar de forma alguna los principios de integridad, disponibilidad, confidencialidad de la información.
- Participar en los planes de respuesta a incidentes informáticos de acuerdo con su impacto.
- Revisar y hacer seguimiento regular a los informes de eventos sobre seguridad informática generados por los sistemas informáticos, analizando las posibles incidencias ocurridas.
- Realizar los informes periódicos de revisión de usuarios inactivos, permisos de usuarios y conflicto 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.
- Gestionar los cambios en las aplicaciones o sistemas de información antes de que sean implementados en ambiente productivo.
- Autorizar la creación, modificación o retiro de códigos de usuario genéricos o privilegiados en el recurso informático bajo su responsabilidad.
- Procurar que los usuarios del recurso informático reciban el entrenamiento necesario para la utilización de los recursos informáticos que les sean asignados.

5.2.1.7. Líder del Proceso

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.

5.2.1.8. Usuario Final

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.

5.2.1.9. 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 las empresas vinculadas recibirán en su proceso de inducción, la capacitación virtual sobre seguridad de la información

- 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 Corporativa de Seguridad de la Información.

- La Gerencia de Recursos Humanos, o según corresponda en las compañías vinculadas, 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, o según corresponda en las compañías vinculadas. Este compromiso de confidencialidad es de obligatorio cumplimiento y el no aplicarlo tendrá implicaciones disciplinarias.

- 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, o según corresponda en las compañías vinculadas.

- La Gerencia de Recursos Humanos, o según corresponda en las compañías vinculadas, 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, o según corresponda en las compañías vinculadas, 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, académica o técnica debe ser autorizada por el responsable de la estrategia de propiedad intelectual.
- 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

- 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.

- La Compañía, implementará procedimientos y establecerá controles para asegurar el cumplimiento de las normas y políticas de seguridad internas, requisitos estatutarios, reglamentarios y contractuales pertinentes para cada sistema de información. Todas las

áreas que dentro de sus procesos deban cumplir con reglamentación aplicable, deben disponer de procedimientos para asegurar el cumplimiento legal.

5.7. ADMINISTRACIÓN DEL RIESGO EN SEGURIDAD DE LA INFORMACIÓN

- El objetivo de esta política es fijar los criterios básicos necesarios para la adecuada gestión de los riesgos asociados a la seguridad de la información con alcance a todos los activos de información de la compañía. La compañía reconoce la importancia de preservar los activos de información, por lo que asigna alta prioridad a la gestión de riesgo a través de la identificación, evaluación y tratamiento de los riesgos relativos a la seguridad de la información, por lo anterior es política de la entidad:

    - Establecer, formalizar y poner en práctica metodologías para la gestión del riesgo.
    - Considerar e identificar las amenazas internas y externas, las vulnerabilidades y los
      posibles impactos razonablemente previsibles que puedan afectar a la compañía.
    - Definir planes de tratamiento y controles sobre los riesgos residuales que permitan reducir los niveles de exposición al riesgo.
    - Definir en forma explícita el nivel de aceptación del riesgo por parte de la dirección de la compañía.
    - Mantener una medición periódica de los riesgos y el diseño de los controles, los cuales harán del mapa de riesgo operativo de la entidad.
    - Realizar evaluaciones periódicas de riesgo en seguridad de la información.
    - Mantener informadas a las partes involucradas sobre el estado del riesgo.

- Todo riesgo de seguridad de la información identificado por un usuario debe ser oportunamente reportado a su jefe inmediato, al Profesional de Seguridad de la Información y a la Gerencia Corporativa de Riesgo 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.

- Los responsables en la Gerencia de TI, deberán retener los registros que contienen eventos relevantes de Seguridad de la Información por un periodo mínimo de 1 año. Durante el cual, deberán protegerse los registros en archivos históricos de forma tal que no puedan modificarse y sólo puedan ser leídos por personas autorizadas.

- Los registros de auditoría de los Recursos Informáticos deberán estar disponibles para su uso por parte de la segunda y tercera línea de defensa.

- El Profesional de Seguridad de la Información revisará de manera periódica a través de los habilitadores tecnológicos disponibles, las actividades de usuarios privilegiados de los Recursos Informáticos críticos.

- La Gerencia de TI, 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 Infraestructura, 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 Infraestructura, garantizará la implementación, mantenimiento y soporte de las soluciones de seguridad que permitan gestionar el monitoreo de alertas para la detección, notificación y seguimiento de posibles incidentes.

- El Profesional de Seguridad de la Información gestionará los controles implementados para mitigar el riesgo de fuga información y monitoreo de alertas de las soluciones de seguridad para detección, notificación y seguimiento de posibles incidentes.

- La Coordinación de Infraestructura, utilizará soluciones de seguridad informática y procedimientos que permitan la extracción, consolidación, análisis y seguimiento de eventos de seguridad y logs de auditoria en los sistemas informáticos con el fin de lograr una gestión eficiente que faciliten la identificación de posibles violaciones de seguridad.

- Todos los funcionarios son responsables por reportar en forma inmediata a través de los canales habilitados relacionados en el Plan de Respuesta a Incidentes Informáticos GPA-1664 cualquier condición anormal o vulnerabilidad que detecte en el uso de los Recursos Informáticos.

- La información específica de las vulnerabilidades técnicas sobre la infraestructura tecnológica de Promigas y sus vinculadas tiene carácter restringido y solo debe darse a conocer a personas autorizadas y que tengan una necesidad de acceso justificada.

- 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.

- La compañía tiene un Plan de Respuesta a Incidentes Informáticos **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.

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 Promigas, con alto valor para la Empresa y de manejo exclusivo de unas personas designadas dentro de la organización. Se incluye información financiera del negocio, los planes comerciales, la información

sensible de los clientes de la Entidad, los datos críticos similares por ejemplo los datos relacionados con fusiones o adquisiciones inminentes, estrategias de inversión e información similar. La información clasificada como Restringida tiene muy limitados el uso y la distribución y debe protegerse en todo momento. Requiere un alto nivel de protección y seguridad. En esta clasificación se incluyen los activos de información que tienen una valoración alta con respecto a su confidencialidad, integridad y disponibilidad.

- **Interna**: Información sensitiva dentro, usada para propósitos del negocio por grupos específicos de Colaboradores.

- **Publica:** Información que puede ser utilizada dentro o fuera de la Institución.

- La compañía cuenta con el procedimiento **GPA-1978** – Clasificación de la Información mediante el cual se definen los lineamientos que se deben considerar para la adecuada categorización y tratamiento de la información corporativa.

- 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 encentre 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 (Coordinador, Jefe,

Director, Gerente) y aplicando los controles necesarios tales como la existencia de un acuerdo previo de términos contractuales garantizando la Confidencialidad e Integridad, usando los mecanismos y herramientas corporativas, con 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.

- Cuando se haya dado la autorización por el responsable de la información, la Gerencia de TI debe ejecutar la eliminación segura de la información, a través de los métodos que ésta misma defina en la plataforma tecnológica de acuerdo con la necesidad y teniendo en cuenta el medio en que reposa; para cumplir con este requerimiento se pueden utilizar cualquiera de los siguientes métodos según sea conveniente:

    - **Desmagnetización**: La desmagnetización consiste en la exposición de los soportes de almacenamiento a un potente campo magnético, proceso que elimina los datos almacenados en el dispositivo. Este método es válido para la destrucción de datos de los dispositivos magnéticos.

    - **Destrucción Física**: El objetivo de la destrucción física es la inutilización del soporte que almacena la información en el dispositivo para evitar la recuperación posterior de los datos que almacena.

        - ✓ Desintegración, pulverización, fusión e incineración: son métodos diseñados para destruir por completo los medios de almacenamiento. Estos métodos suelen llevarse a cabo en una destructora de metal o en una planta de incineración autorizada, con las capacidades específicas para

realizar estas actividades de manera eficaz, segura y sin peligro.

- ✓ Trituración: las trituradoras de papel se pueden utilizar para destruir los medios de almacenamiento flexibles. El tamaño del fragmento de la basura debe ser lo suficientemente pequeño para que haya una seguridad razonable en proporción a la confidencialidad de los datos que no pueden ser reconstruidos. Los medios ópticos de almacenamiento (CD, DVD, otros), deben ser destruidos por pulverización, trituración de corte transversal o incineración.

- **Sobreescritura**: La sobreescritura consiste en la escritura de un patrón de datos sobre los datos contenidos en los dispositivos de almacenamiento. Para asegurar la completa destrucción de los datos se debe escribir la totalidad de la superficie de almacenamiento, para dispositivos electrónicos se debe utilizar un software que efectué borrado a bajo nivel, guardando los registros como evidencia de la destrucción de la información.

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 Gerencia de TI garantizará la existencia de los usuarios en contingencia para ser utilizados en el momento en que se presente la contingencia.

- La Gerencia de TI, garantizarán pruebas periódicas de los medios que contienen copias de respaldo de Información restringida que incluyan la restauración y verificación de la información.

- Es responsabilidad de la Gerencia de TI 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 Gerencia de TI con el acompañamiento del 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 requisitos de seguridad de la información en Continuidad del Negocio que se encuentran definidos son:

  - **De cumplimiento General**

    - ✓ El acceso a los aplicativos debe mantenerse de acuerdo con los perfiles definidos en las matrices de acceso. No obstante, si por indisponibilidad de personal clave en un escenario de continuidad se requieren hacer cambios en los perfiles de acceso, pueden existir modificaciones previa autorización del jefe inmediato, líder aprobador por proceso y Seguridad de la Información
    - ✓ Durante la ejecución del PCN, debe permanecer lo definido en el Procedimiento Administración de Códigos de Usuarios y Claves de Acceso - PPA-212-S2
    - ✓ Los equipos de suministro de energía y de comunicación deben estar en un sitio con acceso restringido. Los accesos deben ser realizados únicamente por los funcionarios de tecnología. Para control del acceso a estos sitios, se deberá contar con una planilla de control de acceso o adquirir un CCTV para disponer de las grabaciones.
    - ✓ El ingreso de los funcionarios debe ser autorizado y controlado de acuerdo con lo establecido en los procedimientos. Funcionarios no autorizados no deben ingresar a las instalaciones.

  - **De cumplimiento por parte de Tecnología**

    - ✓ Los usuarios que se configuren en los equipos que se utilicen durante la ejecución del PCN, deben ser los mismos que se encuentran configurados en la operación normal.
    - ✓ Las contraseñas de acceso deben mantener las políticas de contraseñas definidas en el Estándar de Seguridad de Recursos Informáticos – PPA-786
    - ✓ Los equipos que se utilicen durante la ejecución del PCN deben tener el sistema operativo con soporte disponible por fabricante.

- ✓ Los componentes de infraestructura de red y de tecnología deben tener implementados los estándares de seguridad; dichos estándares, deben estar validados.
- ✓ Se debe realizar el escaneo de vulnerabilidades de la infraestructura tecnológica, con la misma periodicidad deifinida para la operación normal
- ✓ Las restricciones para el acceso a Internet deben permanecer para el PCN de acuerdo con el filtro de contenido implementado, según las categorías de navegación definidos para la operación normal.
- ✓ Los siguientes controles implementados en la operación normal deben permanecer durante la ejecución del PCN:
  - Antivirus - Antimalware
  - Filtrado de contenido
  - VPN
- ✓ Las comunicaciones entre las redes desde y hacia el exterior, deben estar controladas por un Firewall durante la ejecución del PCN.
- ✓ Los equipos y usuarios con permiso de acceso por VPN deben ser los autorizados o definidos como críticos en contingencia. Y en caso de requerirse nuevas conexiones, estas deberán ser autorizadas de acuerdo con el procedimiento establecido.
- ✓ Los equipos configurados para el PCN, deben tener por defecto bloqueados los puertos de salida. Las áreas deben definir la necesidad de disponer del servicio de los Puertos USB y Unidades de CD/DVD, para los equipos asignados a los funcionarios; esto será validado por Seguridad de la Información.
- ✓ Se deberá realizar backups de las actividades ejecutadas sobre las bases de datos y aplicativos durante la ejecución del PCN; el backup deberá ser cifrado y permanecer en custodia en un sitio externo diferente a las instalaciones de la compañía.

- **De cumplimiento por parte de Usuarios Finales**

- ✓ De acuerdo con lo establecido en las Política de Seguridad de la Información GNA-1656, los usuarios no pueden compartir credenciales de acceso a sistemas.
- ✓ El acceso a los portales debe ser realizado por el titular, teniendo en cuenta que los Tokens como las contraseñas, son personales e intransferibles.

5.12. PROTECCION DE CODIGO MALICIOSO

- La Gerencia de TI, 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, 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 aprobadas.

- La Gerencia de TI, 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.

- 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 de este 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 de acuerdo con el Plan de Respuesta a Incidentes Informáticos **GPA-1664.**

- La Gerencia de TI deberá proveer la disponibilidad de la infraestructura de la compañía, por los menos una vez al año para desplegar un análisis de vulnerabilidades que permita estados resultantes de las vulnerabilidades encontradas.

- La Gerencia de TI debe garantizar que se incluyan en el análisis los equipos o dispositivos que expongan algún servicio hacia internet. En caso de que se realicen cambios importantes en la plataforma tecnológica (Equipos activos, servicios, servidores), que pudieran afectar la seguridad informática, deberán considerarse realizar pruebas adicionales.

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.

- Todo equipo de cómputo de usuario final, ya sea de escritorio o portátil, mediante el cual se realice algún tipo de tratamiento (acceso, almacenamiento, modificación, etc.) de información clasificada como restringida debe contar con los requisitos de seguridad (controles) señalados en Anexo 1 - Estándares para el tratamiento de la información.

- Los medios de almacenamiento que contienen copias de respaldo de información deberán protegerse en concordancia con la Clasificación de la Información que almacenan.

- 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 con lo establecido por los fabricantes y además se deberá llevar los registros que cubra todos los Recursos Informáticos.

- 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 cuenta con un proceso de gestión de las vulnerabilidades técnicas a través del procedimiento **PPA-1999** Procedimiento de Gestión y Remediación de Vulnerabilidades Informáticas, lo cual incluye responsables de su gestión, las acciones a implementar y tiempos 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.

- Promigas y sus empresas vinculadas aseguraran que el software adquirido y desarrollado tanto internamente como por terceras partes, cumplirá con los requisitos de seguridad y calidad establecidos por estos. El profesional de Seguridad de la Información generará recomendaciones y requisitos de seguridad en la definición de requerimientos.

- La Gerencia de TI analizará las modificaciones de configuración, cambios evolutivos o de emergencia y mantenimiento sobre los sistemas de información de alta criticidad para el logro de los objetivos del negocio. Conforme al análisis, para los cambios que impliquen la implementación de nuevas funcionalidades en las aplicaciones, cambios para extracción y visualización de información de bases de datos en ambientes

productivos y cambios directos sobre bases de datos, serán escalados al Profesional de Seguridad de la Información para su validación y aprobación.

- 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.

- Los datos de ambientes de producción sólo deberán ser utilizados en ambientes de desarrollo o pruebas, con los debidos controles para proteger su confidencialidad.

5.15. IDENTIFICACIÓN Y AUTENTICACIÓN INDIVIDUAL

- Cada uncionario 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.

- Cada funcionario tiene asignado un único código de usuario para obtener acceso a cada una de las plataformas y aplicaciones que utilice.

- 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.

- 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 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:

- Asegurar que los usuarios acaten los estándares y recomendaciones para la elección y el cambio de contraseñas.
- Obtener el compromiso escrito de los usuarios de mantener la confidencialidad de las 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.

- Para las aplicaciones core del negocio 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, este control no aplica para el correo electrónico.

- 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.

- 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 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.

- Los privilegios de los usuarios de los Recursos Informáticos deberán ser manejados y controlados centralizadamente, de acuerdo con los lineamientos de esta Política.

- La coordinación de infraestructura con apoyo del 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.

- Los datos de producción únicamente deben ser accedidos a través de las aplicaciones de negocio de propósito especifico disponibles. 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 es 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 restringirá el acceso a los puertos USB, Unidad de CD/DVD y SD desde la entrega del equipo para que tengan funcionalidad de solo lectura y sólo aquellos que sean requeridos por necesidad del negocio y/o proceso podrán ser habilitados para escritura previa justificación del Gerente de la dependencia y la aprobación del Profesional de Seguridad de la Información.

- El profesional de seguridad de la información anualmente generará una certificación

con los líderes de procesos sobre las excepciones habilitadas para puertos USB, Unidad de CD/DVD, SD, sitios de internet, entre otros, con el fin de asegurar que los funcionarios no mantengan los permisos más del tiempo requerido.

- Toda solicitud de excepción a puertos USB, Unidad de CD/DVD, SD, sitios de internet, entre otros, deberán contar con las aprobaciones correspondientes, el tiempo requerido de la excepción y la debida justificación del permiso solicitado.

- La información restringida de la compañía debe ser tratada con las medidas de seguridad definidas a nivel corporativo para minimizar al máximo los riesgos que puedan afectar la confidencialidad y privacidad de esta. En el uso de correo electrónico los colaboradores que tienen acceso a información restringida deben contar con la autorización del gerente de dependencia y el profesional de seguridad de la información para su envío por este medio a raíz de una necesidad del negocio y/o proceso.

- 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.

- 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 en 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 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:

  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 Infraestructura, son los autorizados para la divulgación al interior de la empresa, de mensajes de advertencias de seguridad de la Información e Informática. 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 Y PANTALLA LIMPIOS

- 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 Infraestructura, 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.

- La Coordinación de Infraestructura, deberá establecer las configuraciones aceptables, para los dispositivos móviles o personales, que hagan uso de los servicios provistos por la compañía.

- La Coordinación de Infraestructura, 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 Infraestructura, 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 Infraestructura, 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.

5.21. USO ADECUADO DE INTERNET

- La Coordinación de Infraestructura, 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.

5.22. CONEXIONES Y TRABAJO REMOTO

- La compañía dispondrá de medidas preventivas para el uso de conexiones remotas con el objetivo de proteger la información que es accedida desde lugares donde se realiza trabajo remoto.

- El Profesional de Seguridad de la Información, debe analizar y monitorear los métodos de conexión remota a la plataforma tecnológica de la compañía.

- Es responsabilidad de la Coordinación de Infraestructura implementar y mantener los métodos y controles de seguridad para el adecuado establecimiento de conexiones remotas autorizadas hacia la plataforma tecnológica de la compañía.

- Se deben restringir las conexiones remotas solo a los recursos de la plataforma tecnológica necesarios; únicamente se debe permitir su acceso a personal autorizado y por periodos de tiempo definidos, teniendo en cuenta las labores a desempeñar.

- Los accesos remotos se deben configurar considerando siempre: conexiones cifradas para mantener confidencialidad, disponibilidad y tiempos de sesión, autenticación a nivel de usuario e integridad de los datos durante la comunicación. Para este propósito, el mecanismo autorizado son conexiones de tipo VPN (Virtual Private Network).

- Cuando se requieran conexiones externas, previamente autorizadas, por parte de proveedores o socios de negocio, La Gerencia de TI debe garantizar el uso de mecanismos de autenticación para controlar el acceso remoto a través de VPN configurada y asignada en el firewall. Las cuentas utilizadas por proveedores para el acceso remoto solo estarán habilitadas durante el tiempo requerido para realizar las labores específicas de acuerdo con la necesidad, y luego serán desactivadas.

- La Gerencia de TI debe verificar la efectividad de los controles aplicados sobre las conexiones remotas a los recursos de la plataforma tecnológica de Promigas y empresas vinculadas de manera permanente.

- Las solicitudes de acceso remoto a equipos de cómputo en la red corporativa deben ser realizadas mediante el formato FA-432 para Promigas y documento o formato equivalente en empresas vinculadas y deben contar con el aval del líder del área al cual pertenece el funcionario solicitante del acceso, adicionalmente, los funcionarios deben acatar las condiciones de uso establecidas para dichas conexiones.

- Posterior al tiempo de duración del acceso remoto, el acceso será revocado hasta que se haga una nueva solicitud. La revocación exige la creación de nuevas credenciales de acceso para el usuario solicitante.
- El funcionario solicitante de la conexión remota es responsable del uso indebido o no autorizado que se haga con el acceso remoto que le ha sido designado, incluyendo el que realicen otros usuarios con acceso al equipo de cómputo desde el cual se hace el acceso remoto.

5.23. DOCUMENTOS DE REFERENCIA Y ANEXOS

Se enuncian los documentos de Promigas relacionados con esta Política:

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
GPA-1978 – Procedimiento de Clasificación de la Información
PPA-1999 – Procedimiento de Gestión y Remediación de Vulnerabilidades Informáticas.

6. CONTROL DE CAMBIOS

Cambios de la versión 7 – Agosto 2021

Se realizaron modificaciones menores de forma y se asocia el ANEXO 1 - ESTÁNDARES PARA EL TRATAMIENTO DE LA INFORMACIÓN.

Solicitud No. 16120

Cambios de la versión 6 – diciembre 2020

Se realizaron modificaciones y se incluyen los siguientes nuevos lineamientos:

- Se adiciona el capítulo de actualización en la política donde se define la responsabilidad de actualización y modificación sobre las directrices de la política y el tiempo en que se deben ejecutar estas actividades.
- Se actualiza el capítulo 5.1 y 5.2 de responsabilidades y organización de la seguridad de la información.
- Se actualiza la definición de la categoría Restringido y se alinea con los establecidos en el procedimiento de Clasificación de la Información.
- Se definen nuevos lineamientos en el capítulo 5.14 y 5.16
- Se adiciona el capítulo 5.22 conexiones y trabajo remoto.
- Se actualizan las áreas de reporte de TI teniendo en cuenta los nuevos cambios estructurales.

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 mayor 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 Gerente

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

Solicitud No. 11993