

	POLITICA PARA LA SEGURIDAD DE LA INFORMACION	Cód: DG03-PR05-GG
		Versión: 02
		Julio de 2019

GAS CAQUETA S.A E.S.P, se compromete a velar por el cumplimiento de los requisitos legales, por medio de la aplicación estrategias de control con el fin de identificar, valorar y tratar los riesgos de la seguridad de la información, estableciendo las acciones necesarias para garantizar la confidencialidad, integridad, disponibilidad de la información y mejora continua del sistema de gestión de la seguridad de la información.

Para garantizar su cumplimiento se enmarcan las siguientes normas:

NORMAS DE CONTROL DE ACCESO A SISTEMAS Y APLICATIVOS

- La Gerencia o la Oficina de sistemas como propietarias de los sistemas de información y aplicativos que apoyan los procesos y áreas que lideran, velarán por la asignación, modificación y revocación de privilegios de accesos a sus sistemas o aplicativos de manera controlada. La Dirección de Sistemas, como responsable de la administración de dichos sistemas de información y aplicativos, propenderá para que estos sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico. Así mismo, velará porque los desarrolladores, tanto internos como externos, acojan buenas prácticas de desarrollo en los productos generados para controlar el acceso lógico y evitar accesos no autorizados a los sistemas administrados.
- El Departamento de Sistemas debe establecer ambientes separados a nivel físico y lógico para desarrollo, pruebas y producción, contando cada uno con su plataforma, servidores, aplicaciones, dispositivos y versiones independientes de los otros ambientes, evitando que las actividades de desarrollo y pruebas puedan poner en riesgo la integridad de la información de producción.
- El Departamento de Sistemas debe asegurar, mediante los controles necesarios, que los usuarios utilicen diferentes perfiles para los ambientes de desarrollo, pruebas y producción, y así mismo que los menús muestren los mensajes de identificación apropiados para reducir los riesgos de error.
- El Departamento de Sistemas debe establecer el procedimiento y los controles de acceso a los ambientes de producción de los sistemas de información; así mismo, debe asegurarse que los desarrolladores internos o externos, posean acceso limitado y controlado a los datos y archivos que se encuentren en los ambientes de producción.
- El Departamento de Sistemas debe proporcionar repositorios de archivos fuente de los sistemas de información; estos deben contar con acceso controlado y restricción de privilegios, además de un registro de acceso a dichos archivos.
- Los desarrolladores deben asegurar que los sistemas de información construidos requieran autenticación para todos los recursos y páginas, excepto aquellas específicamente clasificadas como públicas.
- Los desarrolladores deben certificar la confiabilidad de los controles de autenticación, utilizando implementaciones centralizadas para dichos controles.
- Los desarrolladores deben certificar que no se almacenen contraseñas, cadenas de conexión u otra información sensible en texto claro y que se implementen controles de integridad de dichas contraseñas.
- Los desarrolladores deben establecer los controles de autenticación de tal manera que cuando fallen, lo hagan de una forma segura, evitando indicar específicamente cual fue la falla durante el proceso de autenticación y, en su lugar, generando mensajes generales de falla.

	POLITICA PARA LA SEGURIDAD DE LA INFORMACION	Cód: DG03-PR05-GG
		Versión: 02
		Julio de 2019

- Los desarrolladores deben asegurar que no se despliegan en la pantalla las contraseñas ingresadas, así como deben deshabilitar la funcionalidad de recordar campos de contraseñas.
- Los desarrolladores deben certificar que se inhabilitan las cuentas luego de un número establecido de intentos fallidos de ingreso a los sistemas desarrollados.
- Los desarrolladores deben asegurar que si se utiliza la reasignación de contraseñas, únicamente se envíe un enlace o contraseñas temporales a cuentas de correo electrónico previamente registradas en los aplicativos, los cuales deben tener un periodo de validez establecido; se deben forzar el cambio de las contraseñas temporales después de su utilización.
- Los desarrolladores deben certificar que el último acceso (fallido o exitoso) sea reportado al usuario en su siguiente acceso exitoso a los sistemas de información.

NORMAS DE AREAS SEGURAS

- Las solicitudes de acceso al centro de cómputo o a los centros de cableado deben ser aprobadas por funcionarios de la Dirección de Sistemas autorizados; no obstante, los visitantes siempre deberán estar acompañados de un funcionario de dicha dirección durante su visita al centro de cómputo o los centros de cableado.
- El Departamento de Sistemas autoriza el ingreso de los visitantes al centro de cómputo y a los centros de cableado que están bajo su custodia, luego del registro en la bitácora ubicada en la entrada de las instalaciones de la empresa.
- El Departamento de Sistemas debe discontinuar o modificar de manera inmediata los privilegios de acceso físico al centro de cómputo y los centros de cableado que están bajo su custodia, en los eventos de desvinculación o cambio en las labores de un funcionario autorizado.
- El Departamento de Sistemas debe proveer las condiciones físicas y medioambientales necesarias para certificar la protección y correcta operación de los recursos de la plataforma tecnológica ubicados en el centro de cómputo; deben existir sistemas de control ambiental de temperatura y humedad, sistemas de detección y extinción de incendios, sistemas de descarga eléctrica, sistemas de vigilancia y monitoreo y alarmas en caso de detectarse condiciones ambientales inapropiadas. Estos sistemas se deben monitorear de manera permanente.
- Los ingresos y egresos de personal a las instalaciones de la Entidad deben ser registrados; por consiguiente, los funcionarios y personal provisto por terceras partes deben cumplir completamente con los controles físicos implantados.
- Los funcionarios deben portar el carné que los identifica como tales en un lugar visible mientras se encuentren en las instalaciones de la Empresa; en caso de pérdida del carné o tarjeta de acceso a las instalaciones, deben reportarlo a la mayor brevedad posible.
- Los funcionarios de la Empresa y el personal provisto por terceras partes no deben intentar ingresar a áreas a las cuales no tengan autorización.

	POLITICA PARA LA SEGURIDAD DE LA INFORMACION	Cód: DG03-PR05-GG
		Versión: 02
		Julio de 2019

NORMAS DE SEGURIDAD PARA LOS EQUIPOS INSTITUCIONALES

- El Departamento de Sistemas debe proveer los mecanismos y estrategias necesarios para proteger la confidencialidad, integridad y disponibilidad de los recursos tecnológicos, dentro y fuera de las instalaciones de la empresa.
- El Departamento de Sistemas debe garantizar los mantenimientos preventivos y correctivos de los recursos de la plataforma tecnológica de la Entidad.
- El Departamento de Sistemas debe generar estándares de configuración segura para los equipos de cómputo de los funcionarios de la Entidad y configurar dichos equipos acogiéndose los estándares generados.
- El Departamento de Sistemas debe establecer las condiciones que deben cumplir los equipos de cómputo de personal provisto por terceros, que requieran conectarse a la red de datos de la Entidad y verificar el cumplimiento de dichas condiciones antes de conceder a estos equipos acceso a los servicios de red.
- El Departamento de Sistemas debe aislar los equipos de áreas sensibles, para proteger su acceso de los demás funcionarios de la red de la empresa.
- El Departamento de Sistemas debe generar y aplicar lineamientos para la disposición segura de los equipos de cómputo de los funcionarios de la Entidad, ya sea cuando son dados de baja o cambian de usuario.
- La Dirección de Sistemas es la única área autorizada para realizar movimientos y asignaciones de recursos tecnológicos; por consiguiente, se encuentra prohibida la disposición que pueda hacer cualquier funcionario de los recursos tecnológicos de la Entidad.
- Las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos asignados a los funcionarios y personal provisto por terceras partes deben acoger las instrucciones técnicas de proporcione la oficina de Sistemas.
- Cuando se presente una falla o problema de hardware o software en una estación de trabajo u otro recurso tecnológico de propiedad de Empresa, el usuario responsable debe informar a esta oficina, en donde se atenderá con el fin de realizar una asistencia adecuada. El usuario no debe intentar solucionar el problema.
- La instalación, reparación o retiro de cualquier componente de hardware o software de las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos de la Entidad, solo puede ser realizado por los funcionarios de la Oficina de Sistemas, o personal de terceras partes autorizado por dicha dirección.
- Los funcionarios de la entidad y el personal provisto por terceras partes deben bloquear sus estaciones de trabajo en el momento de abandonar su puesto de trabajo.
- Los funcionarios de la empresa y el personal provisto por terceras partes no deben dejar encendidas las estaciones de trabajo u otros recursos tecnológicos en horas no laborables.
- Los equipos de cómputo, bajo ninguna circunstancia, deben ser dejados desatendidos en lugares públicos o a la vista, en el caso de que estén siendo transportados.
- Los equipos de cómputo deben ser transportados con las medidas de seguridad apropiadas, que garanticen su integridad física.
- Los equipos portátiles siempre deben ser llevados como equipaje de mano y se debe tener especial cuidado de no exponerlos a fuertes campos electromagnéticos.

	POLITICA PARA LA SEGURIDAD DE LA INFORMACION	Cód: DG03-PR05-GG
		Versión: 02
		Julio de 2019

- En caso de pérdida o robo de un equipo de cómputo de la Empresa, se debe informar de forma inmediata al líder del proceso para que se inicie el trámite interno y se debe poner la denuncia ante la autoridad competente.
- Los funcionarios de la Entidad y el personal provisto por terceras partes deben asegurar que sus escritorios se encuentran libres de los documentos que son utilizados durante el desarrollo de sus funciones al terminar la jornada laboral y, que estos sean almacenados bajo las protecciones de seguridad necesarias.

NORMAS DE ASIGNACIÓN DE RESPONSABILIDADES OPERATIVAS

- El Departamento de Sistemas debe efectuar, a través de sus funcionarios, la documentación y actualización de los procedimientos relacionados con la operación y administración de la plataforma tecnológica de la Entidad.
- El Departamento de Sistemas debe proporcionar a sus funcionarios manuales de configuración y operación de los sistemas operativos, firmware, servicios de red, bases de datos y sistemas de información que conforman la plataforma tecnológica de la Empresa.
- El Departamento de Sistemas debe proveer los recursos necesarios para la implantación de controles que permitan la separación de ambientes de desarrollo, pruebas y producción, teniendo en cuenta consideraciones como: controles para el intercambio de información entre los ambientes de desarrollo y producción, la inexistencia de compiladores, editores o fuentes en los ambientes de producción y un acceso diferente para cada uno de los ambientes.
- El Departamento de Sistemas, a través de sus funcionarios, debe realizar estudios sobre la demanda y proyecciones de crecimiento de los recursos administrados de manera periódica (anual), con el fin de asegurar el desempeño y capacidad de la plataforma tecnológica.

NORMAS DE PROTECCIÓN FRENTE A SOFTWARE MALICIOSO

- El Departamento de Sistemas debe proveer herramientas tales como antivirus, antimalware, antisipam, antispyware, entre otras, que reduzcan el riesgo de contagio de software malicioso y respalden la seguridad de la información contenida y administrada en la plataforma tecnológica de la Entidad y los servicios que se ejecutan en la misma.
- El Departamento de Sistemas debe asegurar que el software de antivirus, antimalware, antisipam y antispyware cuente con las licencias de uso requeridas, certificando así su autenticidad y la posibilidad de actualización periódica de las últimas bases de datos de firmas del proveedor del servicio.
- El Departamento de Sistemas debe certificar que la información almacenada en la plataforma tecnológica sea escaneada por el software de antivirus, incluyendo la información que se encuentra contenida y es transmitida por el servicio de correo electrónico.
- El Departamento de Sistemas, a través de sus funcionarios, debe asegurarse que los usuarios no puedan realizar cambios en la configuración del software de antivirus, antisipam, antimalware.

	POLITICA PARA LA SEGURIDAD DE LA INFORMACION	Cód: DG03-PR05-GG
		Versión: 02
		Julio de 2019

- El Departamento de Sistemas, a través de sus funcionarios, debe certificar que el software de antivirus, antispyware, antispam, antimalware, posea las últimas actualizaciones y parches de seguridad, para mitigar las vulnerabilidades de la plataforma tecnológica.
- Los usuarios de recursos tecnológicos no deben cambiar o eliminar la configuración del software de antivirus, antispyware, antimalware, antispam definida por la Dirección de Sistemas; por consiguiente, únicamente podrán realizar tareas de escaneo de virus en diferentes medios.
- Los usuarios de recursos tecnológicos deben ejecutar el software de antivirus, antispyware, antispam, antimalware sobre los archivos y/o documentos que son abiertos o ejecutados por primera vez, especialmente los que se encuentran en medios de almacenamiento externos o que provienen del correo electrónico.
- Los usuarios deben asegurarse que los archivos adjuntos de los correos electrónicos descargados de internet o copiados de cualquier medio de almacenamiento, provienen de fuentes conocidas y seguras para evitar el contagio de virus informáticos y/o instalación de software malicioso en los recursos tecnológicos.
- Los usuarios que sospechen o detecten alguna infección por software malicioso deben notificar a la oficina de sistemas, para que a través de ella, la Dirección de Sistemas tome las medidas de control correspondientes.

NORMAS DE COPIAS DE RESPALDO DE LA INFORMACIÓN

- El Departamento de Sistemas, a través de sus funcionarios, debe generar y adoptar los procedimientos para la generación, restauración, almacenamiento y tratamiento para las copias de respaldo de la información, velando por su integridad y disponibilidad.
- El Departamento de Sistemas debe disponer de los recursos necesarios para permitir la identificación de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada.
- El Departamento de Sistemas, a través de sus funcionarios, debe llevar a cabo los procedimientos para realizar pruebas de recuperación a las copias de respaldo, para así comprobar su integridad y posibilidad de uso en caso de ser necesario.
- El Departamento de Sistemas debe definir las condiciones de transporte o transmisión y custodia de las copias de respaldo de la información que son almacenadas externamente.
- El Departamento de Sistemas debe proporcionar apoyo para la definición de las estrategias de generación, retención y rotación de las copias de respaldo de la los activos información de la Entidad.
- Los propietarios de los recursos tecnológicos y sistemas de información deben definir, en conjunto con la Dirección de Sistemas, las estrategias para la generación, retención y rotación de las copias de respaldo de los activos de información.
- Es responsabilidad de los usuarios de la plataforma tecnológica de la empresa, identificar la información crítica que debe ser respaldada y almacenarla de acuerdo con su nivel de clasificación.

NORMAS DE USO DEL CORREO ELECTRÓNICO

- El Departamento de Sistemas debe generar y divulgar un procedimiento para la administración de cuentas de correo electrónico.

	POLITICA PARA LA SEGURIDAD DE LA INFORMACION	Cód: DG03-PR05-GG
		Versión: 02
		Julio de 2019

- El Departamento de Sistemas debe diseñar y divulgar las directrices técnicas para el uso de los servicios de correo electrónico.
- El Departamento de Sistemas debe proveer un ambiente seguro y controlado para el funcionamiento de la plataforma de correo electrónico.
- El Departamento de Sistemas debe establecer procedimientos e implantar controles que permitan detectar y proteger la plataforma de correo electrónico contra código malicioso que pudiera ser transmitido a través de los mensajes.
- La cuenta de correo electrónico asignada es de carácter individual; por consiguiente, ningún funcionario de la Entidad o provisto por un tercero, bajo ninguna circunstancia debe utilizar una cuenta de correo que no sea la suya.
- Los mensajes y la información contenida en los correos electrónicos deben ser relacionados con el desarrollo de las labores y funciones de cada usuario en apoyo al objetivo misional de la Empresa. El correo institucional no debe ser utilizado para actividades personales.
- Los mensajes y la información contenida en los buzones de correo son propiedad de GAS CAQUETA S.A. – E.S.P. y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.
- Los usuarios de correo electrónico institucional tienen prohibido el envío de cadenas de mensajes de cualquier tipo, ya sea comercial, político, religioso, material audiovisual, contenido discriminatorio, pornografía y demás condiciones que degraden la condición humana y resulten ofensivas para los funcionarios de la Entidad y el personal provisto por terceras partes.
- No es permitido el envío de archivos que contengan extensiones ejecutables, bajo ninguna circunstancia.
- Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definidos por la Empresa y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad.

NORMAS DE USO ADECUADO DE INTERNET

- El Departamento de Sistemas debe proporcionar los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación segura del servicio de Internet, bajo las restricciones de los perfiles de acceso establecidos.
- El Departamento de Sistemas debe diseñar e implementar mecanismos que permitan la continuidad o restablecimiento del servicio de Internet en caso de contingencia interna con base en el proveedor del servicio.
- El Departamento de Sistemas debe monitorear continuamente el canal o canales del servicio de Internet.
- El Departamento de Sistemas debe establecer procedimientos e implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de Internet y evitar el acceso a sitios catalogados como restringidos.
- El Departamento de Sistemas debe generar registros de la navegación y los accesos de los usuarios a Internet, así como establecer e implantar procedimientos de monitoreo sobre la utilización del servicio de Internet.
- Los usuarios del servicio de Internet de la Empresa, deben hacer uso del mismo en relación con las actividades laborales que así lo requieran.

	POLITICA PARA LA SEGURIDAD DE LA INFORMACION	Cód: DG03-PR05-GG
		Versión: 02
		Julio de 2019

- Los usuarios del servicio de Internet deben evitar la descarga de software desde internet, así como su instalación en las estaciones de trabajo o dispositivos móviles asignados para el desempeño de sus labores.
- No está permitido el acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas establecidas en este documento.
- Los usuarios del servicio de internet tienen prohibido el acceso y el uso de servicios interactivos o mensajería instantánea como Facebook, Kazaa, MSN, Yahoo, Sype, Net2phome y otros similares, que tengan como objetivo crear comunidades para intercambiar información, o bien para fines diferentes a las actividades propias de la Empresa.
- No está permitido la descarga, uso, intercambio y/o instalación de 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 sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros. La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) utilizando sitios públicos en Internet debe ser autorizada por el jefe respectivo y la Dirección de Sistemas, o a quienes ellos deleguen de forma explícita para esta función, asociando los procedimientos y controles necesarios para el monitoreo y aseguramiento del buen uso del recurso.
- No está permitido el intercambio no autorizado de información de propiedad de la Empresa, de sus clientes y/o de sus funcionarios, con terceros.

DEFINICIONES

- **Activo de información:** cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de negocios de GAS CAQUETA S.A. – E.S.P. y, en consecuencia, debe ser protegido.
- **Acuerdo de Confidencialidad:** es un documento en los que los funcionarios de GAS CAQUETA S.A. – E.S.P. o los provistos por terceras partes manifiestan su voluntad de mantener la confidencialidad de la información de la Entidad, comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan acceso en virtud de la labor que desarrollan dentro de la misma.
- **Análisis de riesgos de seguridad de la información:** proceso sistemático de identificación de fuentes, estimación de impactos y probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.
- **Autenticación:** es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.
- **Capacity Planning:** es el proceso para determinar la capacidad de los recursos de la plataforma tecnológica que necesita la Entidad para satisfacer las necesidades de procesamiento de dichos recursos de forma eficiente y con un rendimiento adecuado.
- **Centros de cableado:** son habitaciones donde se deberán instalar los dispositivos de comunicación y la mayoría de los cables. Al igual que los centros de cómputo, los centros

 <p>SISTEMA DE GESTIÓN DE CALIDAD</p>	POLITICA PARA LA SEGURIDAD DE LA INFORMACION	Cód: DG03-PR05-GG
		Versión: 02
		Julio de 2019

de cableado deben cumplir requisitos de acceso físico, materiales de paredes, pisos y techos, suministro de alimentación eléctrica y condiciones de temperatura y humedad.

- **Centro de cómputo:** es una zona específica para el almacenamiento de múltiples computadores para un fin específico, los cuales se encuentran conectados entre sí a través de una red de datos. El centro de cómputo debe cumplir ciertos estándares con el fin de garantizar los controles de acceso físico, los materiales de paredes, pisos y techos, el suministro de alimentación eléctrica y las condiciones medioambientales adecuadas.
- **Cifrado:** es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad. El cifrado es una técnica muy útil para prevenir la fuga de información, el monitoreo no autorizado e incluso el acceso no autorizado a los repositorios de información.
- **Confidencialidad:** es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados. Control: es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal.
- **Criptografía:** es la disciplina que agrupa a los principios, medios y métodos para la transformación de datos con el fin de ocultar el contenido de su información, establecer su autenticidad, prevenir su modificación no detectada, prevenir su repudio, y/o prevenir su uso no autorizado.
- **Custodio del activo de información:** es la unidad organizacional o proceso, designado por los propietarios, encargado de mantener las medidas de protección establecidas sobre los activos de información confiados.
- **Derechos de Autor:** es un conjunto de normas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores por el solo hecho de la creación de una obra literaria, artística o científica, tanto publicada o que todavía no se haya publicado.
- **Disponibilidad:** es la garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.
- **Estándar:** Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares son diseñados para promover la implementación de las políticas de alto nivel de la entidad antes de crear nuevas políticas.
- **Equipo de cómputo:** dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.
- **Guía:** Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares buenas prácticas. Las guías son esencialmente, recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo.
- **Guías de clasificación de la información:** directrices para catalogar la información de la Entidad y hacer una distinción entre la información que es crítica y aquella que lo es menos o no lo es y, de acuerdo con esto, establecer diferencias entre las medidas de seguridad a aplicar para preservar los criterios de confidencialidad, integridad y disponibilidad de la información
- **Hacking ético:** es el conjunto de actividades para ingresar a las redes de datos y voz de la Entidad con el objeto de lograr un alto grado de penetración en los sistemas, de forma

	POLITICA PARA LA SEGURIDAD DE LA INFORMACION	Cód: DG03-PR05-GG
		Versión: 02
		Julio de 2019

controlada, sin ninguna intención maliciosa, ni delictiva y sin generar daños en los sistemas o redes, con el propósito de mostrar el nivel efectivo de riesgo a lo cual está expuesta la información, y proponer eventuales acciones correctivas para mejorar el nivel de seguridad.

- **Incidente de Seguridad:** es un evento adverso, confirmado o bajo sospecha, que haya vulnerado la seguridad de la información o que intente vulnerarla, sin importar la información afectada, la plataforma tecnológica, la frecuencia, las consecuencias, el número de veces ocurrido o el origen (interno o externo). Integridad: es la protección de la exactitud y estado completo de los activos.
- **Inventario de activos de información:** es una lista ordenada y documentada de los activos de información pertenecientes a la Entidad.
- **Licencia de software:** es un contrato en donde se especifican todas las normas y cláusulas que rigen el uso de un determinado producto de software, teniendo en cuenta aspectos como: alcances de uso, instalación, reproducción y copia de estos productos.
- **Medio removible:** es cualquier componente extraíble de hardware que sea usado para el almacenamiento de información; los medios removibles incluyen cintas, discos duros removibles, CDs, DVDs y unidades de almacenamiento USB, entre otras.
- **Mejor Práctica:** Una regla de seguridad específica o una plataforma que es aceptada, a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de los sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la entidad.
- **Perfiles de usuario:** son grupos que concentran varios usuarios con similares necesidades de información y autorizaciones idénticas sobre los recursos tecnológicos o los sistemas de información a los cuales se les concede acceso de acuerdo con las funciones realizadas. Las modificaciones sobre un perfil de usuario afectan a todos los usuarios cobijados dentro de él.
- **Política:** Declaración de alto nivel que describe la posición de la entidad sobre un tema específico.
- **Procedimiento:** Los procedimientos, definen específicamente como las políticas, estándares, mejores prácticas y guías que serán implementadas en una situación dada. Los procedimientos son independientes de la tecnología o de los procesos y se refieren a las plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada con dicho proceso o sistema específico. Generalmente los procedimientos son desarrollados, implementados y supervisados por el dueño del proceso o del sistema, los procedimientos seguirán las políticas de la entidad, los estándares, las mejores prácticas y las guías tan cerca como les sea posible, y a la vez se ajustaran a los requerimientos procedimentales o técnicos establecidos dentro de la dependencia donde ellos se aplican.
- **Propiedad intelectual:** es el reconocimiento de un derecho particular en favor de un autor u otros titulares de derechos, sobre las obras del intelecto humano. Este reconocimiento es aplicable a cualquier propiedad que se considere de naturaleza intelectual y merecedora de protección, incluyendo las invenciones científicas y tecnológicas, las producciones literarias o artísticas, las marcas y los identificadores, los dibujos y modelos industriales y las indicaciones geográficas.

	POLITICA PARA LA SEGURIDAD DE LA INFORMACION	Cód: DG03-PR05-GG
		Versión: 02
		Julio de 2019

- **Propietario de la información:** es la unidad organizacional o proceso donde se crean los activos de información. Recursos tecnológicos: son aquellos componentes de hardware y software tales como: servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo al interior de GAS CAQUETA S.A. – E.S.P.
- **Registros de Auditoría:** son archivos donde son registrados los eventos que se han identificado en los sistemas de información, recursos tecnológicos y redes de datos de GAS CAQUETA S.A. – E.S.P. Dichos eventos pueden ser, entre otros, identificación de usuarios, eventos y acciones ejecutadas, terminales o ubicaciones, intentos de acceso exitosos y fallidos, cambios a la configuración, uso de utilidades y fallas de los sistemas.
- **Responsable por el activo de información:** es la persona o grupo de personas, designadas por los propietarios, encargados de velar por la confidencialidad, la integridad y disponibilidad de los activos de información y decidir la forma de usar, identificar, clasificar y proteger dichos activos a su cargo.
- **SGSI:** Sistema de Gestión de Seguridad de la Información.
- **Sistema de información:** es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas. Un sistema de información es todo componente de software ya sea de origen interno, es decir desarrollado por de GAS CAQUETA S.A. – E.S.P. o de origen externo ya sea adquirido por la entidad como un producto estándar de mercado o desarrollado para las necesidades de ésta.
- **Sistemas de control ambiental:** son sistemas que utilizan la climatización, un proceso de tratamiento del aire que permite modificar ciertas características del mismo, fundamentalmente humedad y temperatura y, de manera adicional, también permite controlar su pureza y su movimiento.
- **Software malicioso:** es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse o dañar los recursos tecnológicos, sistemas operativos, redes de datos o sistemas de información.
- **Terceros:** todas las personas, jurídicas o naturales, como proveedores, contratistas o consultores, que provean servicios o productos a la entidad.
- **Vulnerabilidades:** son las debilidades, hoyos de seguridad o flaquezas inherentes a los activos de información que pueden ser explotadas por factores externos y no controlables por la Entidad (amenazas), las cuales se constituyen en fuentes de riesgo.

ISMAEL SILVA ALVAREZ
Gerente