1. OBJETIVO GENERAL

Establecer los lineamientos que permitan proteger la información de EFIGAS S.A E.S.P. a través de acciones de aseguramiento de la información teniendo en cuenta los requisitos legales, operativos, tecnológicos, de seguridad y de la entidad alineados con el contexto de direccionamiento estratégico, requisitos del negocio, gestión del riesgo y del control interno con el fin de preservar el cumplimiento de la confidencialidad, integridad, disponibilidad, autenticidad y legalidad de la información.

2. ALCANCE

Aplica a todos los activos de información físicos y digitales, a los empleados que cualquiera sea su vinculación o situación contractual en la organización, a las dependencias que componen la organización y a los procesos internos o externos vinculados a través de contratos o acuerdos con terceros.

3. REQUISITOS LEGALES Y/O REGLAMENTARIOS

La **Política de gestión, seguridad y privacidad de la Información** de EFIGAS pretende instituir y afianzar la cultura de confidencialidad, integridad y disponibilidad de la información, incluidos datos personales; Implementando buenas prácticas de seguridad de la información que hacen parte de la NTC ISO 27001:2013 así como el marco de trabajo de ciberseguridad NIST 800-53 REV4:2013. Lo anterior, considerando la prevalencia de las leyes y normas legales aplicables vigentes y estándares de industria.

Las violaciones a esta política serán analizadas por el comité de seguridad de la información, teniendo en cuenta los requisitos legales y/o reglamentarios aplicables a la organización enmarcados en la PL-GI-80 PROTECCIÓN DE DATOS PERSONALES, PL-TH-112 CÓDIGO DE CONDUCTA y [PL-LG-19] REGLAMENTO DE PROPIEDAD INTELECTUAL, con el objetivo de aplicar medidas correctivas (se pueden considerar desde acciones administrativas, de orden disciplinario o penal de acuerdo a si las circunstancias lo ameritan) y mitigar posibles afectaciones contra la seguridad de la información y datos personales de EFIGAS.

4. TERMINOS Y DEFINICIONES

Información: Interpretación al conjunto de datos almacenados en medios electrónicos, físicos o en el conocimiento de las personas.

Confidencialidad: Asegurar que la información sea accesible sólo para los usuarios autorizados.

Integridad: Proteger la exactitud de la información en su procesamiento, transmisión y almacenamiento.

Disponibilidad: Asegurar que los usuarios autorizados tengan acceso a la información y cuando estos sean requeridos.

Activo de Información: Todos aquellos datos generados, procesados, recopilados y custodiados por EFIGAS.

5. POLÍTICA DE SEGURIDAD

La alta dirección de EFIGAS S.A E.SP, entendiendo la importancia de una gestión adecuada y segura de los activos de información y protección de datos personales, se compromete con la implementación de un SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION (SGSI) estableciendo procesos y procedimientos que generen confianza en el ejercicio de sus deberes con sus interesados, esto enmarcado en el estricto cumplimiento de las leyes en conformidad con la misión y visión estratégica de la organización y el cumplimiento de los estándares de control interno establecidos.

La Alta Dirección de EFIGAS aprueba esta política, como muestra de su compromiso y apoyo hacia la gestión, privacidad y seguridad de la información que se lleva a cabo en la organización, mediante el SGSI.

La Alta Dirección de EFIGAS debe pretender por:

1- La revisión y aprobación de la **Política de gestión, seguridad y privacidad de la Información** para la organización.

2- La promoción activa de una cultura de seguridad de la información en los empleados, proveedores, contratistas, accionistas, junta directiva y partes interesadas, que tengan acceso a los sistemas de información, datos, repositorios e instalaciones físicas de EFIGAS.

3- Facilitar la divulgación de esta política a empleados, proveedores, contratistas, accionistas, junta directiva y partes interesadas de la organización.

4- El aseguramiento de los recursos adecuados para implementar y mantener la **Política de gestión, seguridad y privacidad de la Información**.

5- La verificación del cumplimiento de las políticas aquí mencionadas.

6- Objeto de revisión y mejoramiento permanente, acorde con los requisitos de seguridad de esta organización y dinámica de los objetivos estratégicos de la misma.

6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

El Comité de Seguridad de la Información y la Alta Dirección velarán por revisar y proponer las políticas y funciones generales de la seguridad de la información, el seguimiento y mejora del SGSI. Es responsabilidad de ambos definir e incorporar buenas prácticas de seguridad a los procesos empresariales y las estrategias de capacitación y sensibilización en materia de seguridad de la información al interior de la organización.

El área de TI velará por el cumplimiento de las funciones relativas a la seguridad de los sistemas de información de la entidad, lo cual incluye la operación del SGSI, supervisión del cumplimiento y proponer mejoras de aspectos inherentes a los temas tratados en la presente política. El nivel de supervisión que pueda realizar cada grupo responsable de seguridad está relacionado con el talento humano que lo conforma y en todo caso deberá ser aprobado por el Comité de Seguridad de la Información.

El jefe de TI asignará al responsable de notificar a todo el personal que se vincula contractualmente con la organización de las obligaciones respecto del cumplimiento de la Política de gestión, seguridad y privacidad de la Información y de todos los estándares, procesos, procedimientos, prácticas y guías que surjan del SGSI. De igual forma, el área de TI será responsable de notificar la presente política y los cambios que en ella se produzcan, así como las tareas de capacitación continua en materia de seguridad de la información según los lineamientos dictados por el Comité.

Responsabilidades del personal

Para poder hacer uso de las plataformas tecnológicas de información y comunicación de EFIGAS, todo el personal de EFIGAS independientemente cual sea su situación contractual, la dependencia o sus funciones debe comprender, adoptar y aceptar la presente política, la cual contiene los términos y condiciones que regulan el uso de recursos de TI y perfiles que autorizan el uso de la información que converja a la organización.

La “Información Confidencial” a que se hace referencia en la presente política se define en el PL-TH-112 CÓDIGO DE CONDUCTA y su clasificación en el PL-GI-80 PROTECCIÓN DE DATOS PERSONALES.

El área de TI, tendrá un cuestionario para verificar el entendimiento de esta política, el cual debe de tener una calificación mínima de un 70% y así proceder a asignar los usuarios de los sistemas de información.

Las áreas de Recursos Humanos, Comunicaciones y TI**,** se encargarán de generar, actualizar, mantener y ejecutar un plan de capacitación en seguridad de la información que propenda por el crecimiento continuo de la conciencia individual y colectiva en temas de seguridad de la información.

Todos los usuarios externos o personal de empresas externas deberán de adoptar y firmar un acuerdo de confidencialidad y estar autorizados por un funcionario de EFIGAS quien será el responsable del control, vigilancia y uso adecuado de la información y los recursos de TI cuando aplique y deberá suscribir pólizas de riesgo cibernético de acuerdo con el documento DA-LG-12 MATRIZ PARA LA SOLICITUD DE PÓLIZAS Y GARANTÍAS

El área de TI será el encargado de gestionar el proceso de mejora continua del SGSI con el fin de mejorar la seguridad de la información dentro de sus pilares fundamentales de confidencialidad, integridad y disponibilidad. Así mismo, será responsabilidad de todos los empleados de la organización velar por que se cumplan los lineamientos establecidos en esta política.

El contacto con las autoridades y grupos de interés se realizará siguiendo los lineamientos respecto a vocería contenido en el documento MA-AG-72 MANUAL PARA LA GETIÓN DE RIESGOS Y CRISIS REPUTACIONAL.

7. SEGUIRIDAD DE LOS RECURSOS HUMANOS

Todos los colaboradores antes, durante y después de la relación laboral son responsables de promover la seguridad de los activos de información y datos personales con el fin de mitigar riesgos y asegurar el cumplimiento de los requisitos legales, estatuarios y contractuales sobre los activos de información y su seguridad cuando participan en los procesos organizaciones y siguiendo los lineamientos del PL-TH-7 REGLAMENTO INTERNO DE TRABAJO.

De igual forma, la vinculación laboral con terceros se supervisará por los administradores de contratos en busca del cumplimiento de lo descrito en esta política y de lo establecido en las cláusulas contractuales y de confidencialidad.

8. GESTION DE ACTIVOS

Los propietarios de los activos de información son los responsables de identificar e inventariar los activos de información que poseen (procesan o producen), establecer los criterios de clasificación, valoración, ubicación y acceso con el fin de gestionarlos de forma segura de acuerdo con las necesidades del negocio y/o requerimientos de ley, adoptando los controles necesarios para la protección basados en la disponibilidad, integridad y confidencialidad de los datos y siguiendo los lineamiento de la PL-GI-80 PROTECCIÓN DE DATOS PERSONALES.

9. CONTROL DE ACCESO

La información de EFIGAS se gestionará solo por personal autorizado, limitando el acceso a los sistemas de información mediante el proceso PR-GI-33 PROCEDIMIENTO DE REVISIÓN DE PERMISOS Y SEGREGACIÓN DE FUNCIONES EN LOS SISTEMAS DE INFORMACIÓN. El derecho concedido mediante el anterior proceso es intransferible y por tanto prohibido delegar este derecho a otra persona.

La gestión de usuarios para los sistemas de información de EFIGAS se realiza alineado al documento PR-GI-35 PROCEDIMIENTO PARA LA ADMINISTRACION DE USUARIOS así como a la guía DA-GI-61 ADMINISTRACIÓN DE CONTRASEÑAS.

10. CRIPTOGRAFIA

EFIGAS, a través del área de TI, implementará controles criptográficos en los computadores y servidores para preservar los atributos de confidencialidad, autenticidad y/o integridad de la información almacenada en estos.

De igual forma, proporcionará a los empleados herramientas de cifrado que aseguren la información al ser compartida a terceros a través de los diferentes canales digitales aprobados por EFIGAS. Es de responsabilidad del empleado verificar la clasificación los activos de información que requieren el uso de las herramientas criptográficas alineados al documento PL-GI-80 PROTECCIÓN DE DATOS PERSONALES.

11. SEGURIDAD FISICA Y AMBIENTAL

El control de accesos no autorizados a las instalaciones de EFIGAS, se realizará según lineamientos del documento PL-GL-39 POLÍTICA DE DISPOSICIONES DE SEGURIDAD, en el cual el acceso a los centros de datos informáticos requerirá el uso de una tarjeta de proximidad para habilitar el acceso, previa autorización del área de TI.

Los niveles de seguridad para la protección física de los data center serán propuestos por el área de TI y el área responsable de la seguridad física, y aprobadas por la alta dirección una vez analizado los niveles impacto y probabilidad de perdida de integridad, confidencialidad y disponibilidad sobre los activos de información de EFIGAS.

Los lineamientos para un escritorio limpio y despejado se realizará por medio del documento PL-GL-39 POLÍTICA DE DISPOSICIONES DE SEGURIDAD y apoyado con campañas realizadas desde el área de Seguridad y Salud en el trabajo.

Todo empleado propenderá tener en su equipo de cómputo un escritorio limpio y será responsable de custodiar los acticos físicos, contraseñas, documentos o cualquier otra información importante para la compañía.

12. SEGURIDAD DE LAS OPERACIONES

La documentación, actualización, publicación y socialización de los procedimientos de operaciones informáticas corresponde al área de TI, así como evaluar, monitorear y adoptar controles que minimicen los riesgos en materia de seguridad de la información y aseguren la disponibilidad de los servicios tecnológicos alineados en la guía GA-GI-119 PLAN DE RECUPERACIÓN ANTE DESASTRES y GU-GI-47 GUÍA COPIAS DE SEGUIRDAD.

De igual forma, el área de TI medirá el impacto de los cambios solicitados a los sistemas de información (incluidas las solicitudes de auditorías las cuales estarán alineadas al PR-GI-85 PROCEDIMIENTO PARA LA GESTIÓN DE AUDITORÍAS EN LOS SISTEMAS DE INFORMACIÓN) y/o infraestructura crítica mediante aprobación del comité de cambios descrito en la guía GU-GI-25 GUÍA DE CONTROL DE CAMBIOS teniendo presente que estos deben implementarse desde los ambientes DEV/QA a producción y para los sistemas informáticos que lo permitan, la implementación de marcos de trabajo de integración y despliegue continuo y seguro.

Las operaciones informáticas deberán estar alineadas a la estrategia organizacional de crecimiento de los recursos administrativos y operativos con el fin de asegurar el correcto desempeño y adecuada capacidad de la plataforma tecnológica.

13. SEGURIDAD EN LAS COMUNICACIONES

La gestión segura de las comunicaciones requiere implementar mecanismos de control que permitan mantener la disponibilidad de las redes de datos, sistemas de comunicaciones y servicios informáticos.

Corresponde al área de TI proponer e implementar las herramientas tecnológicas que permitan controlar y gestionar las comunicaciones y el intercambio de información a través de las redes de datos privadas y públicas de la organización.

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

EFIGAS, a través del área de TI, promoverá la seguridad de la información y datos personales durante todo el ciclo de vida de los sistemas de información mediante controles, estrategias, marcos de trabajo seguro y aplicando el procedimiento de PR-GI-50 PROCEDIMIENTO PARA LA ADMINISTRACIÓN DE SOFTWARE; sea que la gestión la realice directamente la organización y/o se contrate con un tercero.

El responsable de los activos de información, presentes o futuros, deberá informar al área de TI los parámetros de seguridad que se deben incorporar a los diferentes sistemas de información propios o de terceros para ser gestionados y así garantizar continuamente la confidencialidad, integridad y disponibilidad de dichos activos.

Es indispensable que toda adquisición, desarrollo y/o mantenimiento de un sistema de información incluidas las redes, incorpore como requisito la seguridad de los activos de información y protección de datos personales en cualquier de los momentos del proyecto, independiente de que este se ejecute directamente por EFIGAS y/o se contrate con un tercero.

El área de TI, validará las vulnerabilidades reportadas por los test de seguridad realizados por la organización y/o terceros a los sistemas de información en desarrollo, implementación y/o en producción y solicitará la corrección de los mismo con la finalidad de aprobar el despliegue o la gestión de cambios de los sistemas de información.

15. RELACIONES CON PROVEEDORES

Corresponde a EFIGAS establecer las condiciones y controles en materia de seguridad de la información para la prestación de servicios y responsabilidades por terceros, debido a podrían acceder y/o tratar activos de información o infraestructura tecnológica durante las relaciones precontractuales, contractuales y post-contractuales, que podrían afectar los principios de confidencialidad, integridad y disponibilidad de la información.

Se generarán acuerdos de confidencialidad teniendo en cuenta la clasificación del activo de información realizada por los administradores de contratos; así mismo, dichos administradores de contratos informarán a los terceros las disposiciones en materia de seguridad de la información teniendo en cuenta que su cumplimiento es obligatorio.

16. GESTION DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN

Se deberá establecer controles en materia de seguridad de la información y datos personales con el fin de detectar, prevenir, informar y gestionar los incidentes de seguridad y privacidad de la información, así como, reportar ante la SIC aquellos incidentes que hayan comprometido cualquier tipo de dato persona siguiendo los lineamientos del documento IN-GI-98 INSTRUCTIVO PARA REPORTAR INCIDENTES DE SEGURIDAD DE DATOS PERSONALES A LA SIC.

Es obligación de todo empleado EFIGAS, cualquiera sea su vinculación, situación contractual, dependencias adscrito o externo vinculados a través de contratos o acuerdos con terceros, informar oportunamente sobre actividad sospechosa que pueda comprometer la seguridad de los activos de información, incluidos datos personales.

EFIGAS, a través del área de TI, liderará la adopción de controles, procedimientos y responsabilidades en la detección, evaluación, prevención y gestión de los incidentes de seguridad de la información para garantizar la continuidad de los servicios. De igual forma, gestionará el conocimiento a partir de los incidentes, documentará lecciones

aprendidas y retroalimentación para adoptar controles que contribuyan y fortalezcan las competencias para responder a incidentes de seguridad de la información.

17. GESTIÓN DE LA CONTINUIDAD TECNOLÓGICA

Corresponde al área de TI desarrollar e implementar planes de contingencia que permitan contrarrestar las interrupciones de sus procesos críticos y asegurar que los procesos del negocio se pueden restaurar en los plazos requeridos, manteniendo las consideraciones en seguridad de la información y ciberseguridad.

Los planes de contingencia deberán estar alineados a los documentos PR-AG-83 PROCEDIMIENTO PARA LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO y MA-AG-72 MANUAL PARA LA GESTIÓN DE RIESGO Y CRISIS REPUTACIONAL.

18. CUMPLIMIENTO

Es deber de EFIGAS en materia de seguridad de la información, protección de datos personales, propiedad intelectual entre otros, monitorear y evaluar de forma periódica el cumplimiento de la normatividad legal, así como el cumplimiento de las obligaciones contractuales con terceros, proveedores que participen en la ejecución de la actividad empresarial, según el documento GU-LG-01 GUÍA PARA LA GESTIÓN DE LA NORMATIVIDAD APLICABLE A LA ORGANZACIÓN

19. CONTROLES DE SEGURIDAD DE LA INFORMACIÓN:

1- RESPONSABILIDAD POR LOS ACTIVOS

- Cualquier equipo de cómputo que sufra daños será valorado por el área de T.I, si el reporte indica que es descuido o abandono por parte del funcionario, este reporte será enviado a su jefe, a Gestión Humana y a la subgerencia que este dependa.
- Los equipos portátiles y equipos de cómputo de oficinas de servicio al cliente siempre deben estar protegidos con guayas.
- Se debe bloquear la sesión de usuario en los equipos de cómputo cada vez que el usuario se ausente de su puesto de trabajo.
- Los equipos de cómputo de los funcionarios de la organización deben ser apagados después de finalizada la jornada laboral, se concederán excepciones en casos de procesos extra-jornada laboral.
- Velar por el buen uso de los activos asignados por la organización.
- Todos los equipos de cómputo deberán cumplir con lo estipulado en el documento [GU-GI-48] GUIA PARA LA ADMINISTRACION DE EQUIPOS respecto inventario y seguimiento y control de activos fijos.

No está permitido:

- Manipular o abrir los equipos de cómputo para realizar limpiezas sin la autorización del área de TI.
- Realizar mantenimiento a los equipos por personal ajeno al área de TI sin su consentimiento.
- Hacer reparaciones o hacer cambio de partes a los equipos de cómputo por medio de personal ajeno al área de TI.
- Consumir bebidas y o alimentos encima o cerca de los equipos de cómputo
- Modificar, cambiar o sustraer partes de los equipos de cómputo
- Descargar, usar, intercambiar y/o instalar software/material comercial no licenciado o pirata, o software que atente contra la disponibilidad y/o confidencialidad de la información de EFIGAS S.A E.S.P.
- El ingreso y uso de portátiles personales sin registrarlos al ingresar a las instalaciones de la organización.

2- USO DE MEDIOS EXTRAIBLES Y ALMACENAMIENTO EN LA NUBE

No está permitido:

- El uso de medios extraíbles o externos como: memorias USB, unidades de DVD, discos duros, unidades de CD, memorias SD y microSD y cualquier otro medio extraíble que pueda extraer o guardar información de la organización, a excepción de los cargos y/o personas que autorice el comité de seguridad de la información el cual deberá quedar soportado con el formato o documento establecido.
- Utilizar medios de almacenamiento en la nube diferentes al OneDrive Corporativo. De existir una excepción, ésta deberá estar autorizada por el jefe de área y por el comité de seguridad de la información.

3- ACCESO A REDES Y RECURSOS DE RED

- El acceso de usuarios no registrados solo debe de ser permitido a la red de INVITADOS. El acceso y uso a cualquier otro tipo de recurso de información de TI, no es permitido a usuarios invitados o no registrados.
  Cualquier funcionario de Efigas puede dar la autorización para que un externo se conecte a la red wifi de invitados, y lo hace solicitando el caso a la mesa de ayuda para la asignación de contraseña de wifi.

No está permitido:

- Intentar instalar u operar puntos de acceso inalámbricos (Access point) o switchs, y/o conectarlos a la red cableada de la organización sin autorización del área de infraestructura TI.

- Conectar equipos de cómputo y dispositivos móviles personales a la red corporativa de EFIGAS S.A. E.S.P, de ser el caso de una excepción se debe crear una carta de aceptación de riesgos firmada por la subgerencia o dirección, y autorizada por el comité de seguridad de la información. El área de TI puede obviar la exigencia de estas autorizaciones en caso de Desastre o Fuerza Mayor Garantizando la seguridad de los recursos informáticos de la compañía.
- Ingresar equipos de cómputo de terceros a la red de EFIGAS S.A. E.S.P. sin la revisión y debida autorización del área de infraestructura de T.I.
- Intentar cualquier tipo de ataque o intrusión contra los sistemas informáticos de Efigas, sin la autorización de TI.

4- ADMINISTRACION DE USUARIOS

- El empleado deberá abstenerse de compartir sus claves de acceso a los diferentes sistemas de información, ya que estas son personales e intransferibles, el préstamo de credenciales de acceso a cualquier sistema de información solo está autorizado en los casos de incapacidades o ausentismos menores <= a 7 días calendario, para lo cual deberá anexarse un memorando autorizado por el Subgerente de área y jefe del Área, este memorando se archivará en la hoja de vida del empleado que se ausenta. Cualquier novedad en cuanto a fechas de salida e ingresos del personal, será el Coordinador de Nómina y SAP quien lo reporte al área de TI, en caso de una excepción, se deberá tener una carta de aceptación de riesgos firmada por la subgerencia o director y aprobada por el comité de seguridad de la información.
- Las cuentas de servicio de los diferentes sistemas de información deberán ser documentadas y aprobadas por las coordinaciones y la jefatura de T.I

No está permitido:

- Acceder a recursos de red suplantando o usando credenciales de acceso de otros usuarios.
- Crear cuentas genéricas en los sistemas de información, en caso de una excepción el subgerente o director firmará una carta de aceptación de riesgo y será autorizada por el comité de seguridad de la información.
- Configurar usuarios administradores de funcionarios de EFIGAS S.A E.S.P en equipos de cómputo, servidores, dispositivos de red o de seguridad, en caso de una excepción deberá ser autorizado por el comité de seguridad de la información.
- Eliminar usuarios de los sistemas de información.

5- SEGURIDAD FISICA Y DEL ENTORNO:

No está permitido:

- El ingreso a los data center de EFIGAS S.A E.S.P, a excepción del personal que la coordinación de infraestructura de T.I y la jefatura de T.I autorice.
- Dejar residuos plásticos, de cartón o de rápida combustión en los data center
- Manipular los dispositivos de control de acceso
- El ingreso del personal a las instalaciones sin el registro en recepción y el acompañamiento de personal de EFIGAS S.A E.S.P
- El ingreso a las áreas de archivo de EFIGAS S.A E.S.P, a excepción del personal que la coordinación de servicios administrativos autorice.
- Consumir productos alimenticios en los data center y áreas de archivo.
- Fumar en los data center y áreas de archivo
- Tomar fotos de la infraestructura tecnológica de los data center sin previa autorización de la coordinación de infraestructura de T.I o la jefatura de T.I
- Tomar fotos de las áreas de archivos.
- Generar copiado de documentos a excepción de las áreas o personal que el área de servicios administrativos autorice.

6- COPIAS Y RESPALDO DE LA INFORMACION

No está permitido:

- Generar copias de seguridad de la información de los computadores o sistemas de información de EFIGAS S.A E.S.P., sin autorización del área de TI
  Generar copias de seguridad de la información en programas o dispositivos diferentes a los designados por el área de T.I.

7- CONTROL DE SOFTWARE

No está permitido:

- Descargar, usar, intercambiar y/o instalar software/material comercial no licenciado o pirata, o software que atente contra la disponibilidad y/o confidencialidad de la información de EFIGAS S.A E.S.P.
- Instalar software de espionaje, monitoreo de tráfico o programas maliciosos en la organización.
- Lanzar cualquier tipo de virus, gusano o programa de computador cuya intención sea hostil o destructiva.
- Instalar o ejecutar cualquier tipo de software o programa que permita el acceso remoto sin la autorización de TI.
  Detener u omitir las actualizaciones o parches de seguridad de los sistemas de información o equipos de la organización.

8- GESTIÓN DE LA SEGURIDAD DE LAS REDES

No está permitido:

- Crear rutas, puertos, protocolos o servicios de comunicación sin la debida autorización de TI.
- Las políticas de firewall no deben tener excepciones de tráfico sin restricción de puertos, protocolos o servicios de comunicación.
  Publicar servicios hacia Internet sin la autorización de TI

9- USO DEL CORREO ELECTRÓNICO INSTITUCIONAL

No está permitido:

- Enviar cualquier comunicación electrónica fraudulenta.
- Usar las comunicaciones electrónicas para violar los derechos de propiedad de los autores.
- Enviar 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 o amenazantes para los empleados, terceros, accionistas o partes interesadas de la organización.
- Revelar información confidencial o privada sin el permiso explícito del secretario general y jurídico de la organización.
- Utilizar el correo electrónico corporativo para registrarse en blogs, foros, redes sociales u otro tipo de sitios web que no tenga vínculos con la organización.
- Utilizar la misma contraseña de su correo corporativo en blogs, foros, redes sociales u otro tipo de sitios web.
- Configurar el correo electrónico corporativo en dispositivos diferentes a los suministrados por el área de T.I, si requieren alguna excepción, se deberá crear una carta de aceptación de riesgos firmada por el subgerente o directivo y ser autorizado por el comité de seguridad de la información.
- Enviar adjuntos que sean programas ejecutables (.dll, .bat, .exe).
- Enviar correos electrónicos masivos o cadenas de ningún tipo, a excepción del área de comunicaciones, área de tecnología y área de gestión humana.
- Él envió de información de carácter sensible o privada sin la autorización del dueño de la misma.
- Él envió de información de carácter confidencial y estratégica para la organización a correos electrónicos no corporativos (Gmail, Hotmail, Outlook etc.) y sin previa autorización del dueño de la misma.

10- USO ADECUADO DE INTERNET

No está permitido:

- Descargar archivos o software de uso no corporativo o publicar material ilegal, con derechos de propiedad intelectual o material nocivo usando un equipo o las redes de la organización
- El uso de páginas para compartir archivos diferentes a los designados por el área de T.I.
- El acceso a páginas con restricción de navegación según lo establecido por el comité de seguridad de EFIGAS S.A E.S.P
- Hacer uso de proxys en los exploradores web u otro tipo de programa que trate de saltar las restricciones de navegación.
- Intercambiar información confidencial, de manera no autorizada, con terceros.
- Intercambiar información confidencial con terceros sin usar encripción.

11-TRANSFERENCIA DE INFORMACIÓN

No está permitido:

- El uso de los recursos informáticos propiedad de EFIGAS S.A. E.S.P. que tengan como objetivo cualquier tipo de ganancia económica personal para cualquier funcionario o contratista, con excepción de algún uso especial que sea autorizado formalmente por la organización, a través de la Gerencia.
- Tener directorios de Windows compartidos en los computadores (SMB) sin la autorización de TI.
- Alterar o falsificar de manera fraudulenta los registros computarizados, permisos, documentos de identificación u otros documentos de la organización.
- Envió de información sensible de forma física por medio de empresas de mensajería no especializada o no segura.
- Envió de información sensible de forma digital por medio de mensajería pública y no autorizada sin ningún tipo de cifrado o mecanismo de seguridad.

12- PROCESOS DE DESARROLLO Y SOPORTE DE LOS SISTEMAS DE INFORMACIÓN

No está permitido:

- Almacenar contraseñas, cadenas de conexión u otra información sensible en texto claro
- Realizar pruebas en ambientes de producción
- Desplegar en ambiente productivo cualquier desarrollo o ajuste a los sistemas de información sin la aprobación pertinente definida por el área de TI
- Dejar usuarios de aplicaciones, sistemas de administración, páginas web, bases de datos, sistemas operativos con las contraseñas por defecto y sin complejidad

- Usuarios con accesos ilimitados a información en ambientes de producción y calidad

13-PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES

No está permitido:

- El uso o tratamiento de datos personales sin ningún tipo de autorización de los titulares de los mismos
- Divulgar o usar los datos personales para otros fines diferentes a los autorizados por el titular
- Omitir la inclusión de cláusulas de confidencialidad y de tratamiento de datos en los contratos con terceros con quienes se compartan datos personales de los clientes de la organización

14-DISPOSITIVOS MOVILES

- Todo empleado deberá autorizar y firmar el documento RE-GI-92 AUTORIZACION USO APPS DISPOSITIVOS MOVILES para acceder a herramientas de colaboración en sus dispositivos móviles personales.
- Todo empleado autorizará la instalación de Apps de terceros que buscan proteger, custodiar y restringir el acceso a la información corporativa en los dispositivos móviles personales.
- Todo empleado autorizará la recopilación, procesamiento y compartir información sobre el estado y configuraciones del dispositivo móvil por medio de Apps de terceros que buscan proteger y custodiar la información corporativa en los dispositivos móviles personales.
- Todo empleado deberá tener una medida de protección (PIN, Patrón) para el acceso a las aplicaciones del dispositivo móvil personal o corporativo.
- Los dispositivos móviles personales o corporativos deben contar con la última versión liberada por el fabricante, así como las aplicaciones de colaboración corporativas instaladas en este dispositivo.
- Todo empleado acepta la restricción de acceso a la información corporativa en cualquier momento por parte de EFIGAS, sin previo aviso.
- Todo empleado acepta el borrado remoto de la información corporativa en cualquier momento por parte de EFIGAS, sin previo aviso.
- Todo empleado debe reportar la perdida inmediata por medio de la mesa de ayuda de su dispositivo móvil personal o corporativo.

No está permitido:

- Configurar servicios de colaboración como correo electrónico, servicios de almacenamiento nube, herramientas unificadas de comunicación y colaboración en dispositivos móviles cuyo sistema operativo no sea el original o haya sido rooteado.

- Instalar aplicaciones de colaboración no oficiales para acceder a estos servicios corporativos de EFIGAS

15- ACCESO REMOTO

- Todo empleado deberá activar la herramienta SDP (Software-Defined Perimeter) y tener su dispositivo con el MFA (Doble Factor de Autenticación) para poder acceder a los recursos informáticos de Efigas
- El modelo de Teletrabajo solo será aplicable cuando EFIGAS lo autorice y deberá cumplir con todos los lineamientos de seguridad y de ley.

No está permitido:

- Realizar instalaciones y o configuraciones de aplicaciones de acceso remoto a los servicios informáticos de EFIGAS en dispositivos no autorizados por el área de TI.
- Instalar o configurar aplicaciones de terceros que permitan tomar control remoto de dispositivos propiedad de Efigas.
- El uso de portátiles personales para ejecutar actividades corporativas sin previa autorización del área de TI.