

CONDICIONES DE CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN.

CLÁUSULAS DE SEGURIDAD DE LA INFORMACIÓN PARA CONTRATOS

Para el cumplimiento de los requerimientos de seguridad de la información y Ciberseguridad se tendrán en cuenta las siguientes definiciones:

Seguridad de la Información: Es el conjunto de políticas, estrategias, metodologías, recursos, soluciones informáticas, prácticas y competencias para proteger, asegurar y preservar la confidencialidad, integridad y disponibilidad de la información que se almacene, reproduzca o procese en los sistemas informáticos de la entidad.

Ciberseguridad: Es el desarrollo de capacidades empresariales para defender y anticipar las amenazas cibernéticas con el fin de proteger y asegurar los datos, sistemas y aplicaciones en el ciberespacio que son esenciales para la operación de la entidad.

Evento de Ciberseguridad: Ocurrencia de una situación que podría afectar la protección o el aseguramiento de los datos, sistemas y aplicaciones de la entidad que son esenciales para el negocio.

Incidente de Ciberseguridad: Ocurrencia de una situación que afecta la protección o el aseguramiento de los datos, sistemas y aplicaciones de la entidad que son esenciales para el negocio.

En consecuencia y de acuerdo con el objeto del presente contrato, EL CONTRATISTA se compromete a cumplir con las siguientes:

CLÁUSULAS DE SEGURIDAD Y/O SEGURIDAD CIBERNÉTICA

Sin perjuicio de cualesquiera otros términos y condiciones del Acuerdo, se exige al CONTRATISTA aplicar los siguientes requisitos de seguridad de la información:

Política de Seguridad

El CONTRATISTA deberá contar con una política de seguridad donde se incluyan los lineamientos necesarios para proteger toda la información y/o sistemas relacionados con GASES DE LA GUAJIRA.

Control de activos

El CONTRATISTA deberá mantener un inventario de cada uno de los dispositivos tecnológicos destinados a la prestación del servicio con GASES DE LA GUAJIRA

donde se indique como mínimo su ubicación, custodio, responsable, nombre de equipo, serial, etc.

Adicionalmente, se deberá definir una nomenclatura para nombrar estos equipos de cómputo del CONTRATISTA.

El CONTRATISTA deberá crear los usuarios con derechos limitados de configuración (No administrador) y será el responsable de la instalación, operación y soporte de su infraestructura tecnológica.

Control de acceso lógico

Para garantizar el cumplimiento de los requisitos de GASES DE LA GUAJIRA sobre el control de la seguridad para el acceso, el CONTRATISTA deberá:

1. Proteger la confidencialidad de todos los datos de acceso (Rutas, Direcciones IP, Contraseñas y/o Claves de acceso) asignadas al CONTRATISTA.
2. Contar con una política de contraseñas en virtud de la cual su personal, sin excepción alguna, deberán cambiar las contraseñas inmediatamente después de recibirlas y posteriormente las cambien cada cuarenta y cinco (45) días o con mayor frecuencia.

Responsabilidades del personal

Para garantizar el cumplimiento de los requisitos referentes a la responsabilidad de los empleados, el CONTRATISTA deberá:

- 1.** Certificar que todos los dispositivos utilizados por los empleados del CONTRATISTA o sus subcontratistas que estén conectados al ambiente de procesamiento de GASES DE LA GUAJIRA cumplan y sigan cumpliendo los siguientes requisitos:
 - a. Deben aplicarse y estar al día los paquetes de actualizaciones (*service pack*) más recientes y todos los parches de seguridad aplicables a todos los sistemas operativos y software residentes en los dispositivos.
 - b. EL CONTRATISTA debe asegurar que los computadores utilizados para el procesamiento de datos de GASES DE LA GUAJIRA no cuenten con accesos habilitados a puertos USB.
 - c. Garantizar que los datos de clientes suministrados por GASES DE LA GUAJIRA no serán tratados a través de dispositivos móviles, celulares, tabletas, etc., a menos que en el desarrollo de las actividades propias del contrato se requiera específicamente que los datos de los usuarios sean tratados en dispositivos móviles.

d. Abstenerse de realizar almacenamientos o tratamientos de datos suministrados por GASES DE LA GUAJIRA en sistemas de almacenamiento o transferencia personales tales como OneDrive, Google Drive, Dropbox o WeTransfer; esta evaluación estará a cargo de la persona encargada de Seguridad de la Información en GASES DE LA GUAJIRA.

Endpoint Detection and Response (EDR):

El Contratista y/o proveedor que requiera conexión a los recursos tecnológicos internos de Gases de La Guajira (red, sistemas de información, almacenamientos, repositorios y plataformas de desarrollo, sistemas de impresión y gestión documental, plataformas operativas y funcionales, los demás que apliquen) se comprometerá a implementar y mantener en óptimas condiciones de funcionamiento una plataforma **Endpoint Detection and Response (EDR)** legalmente licenciada y de uso corporativo en todos los dispositivos y sistemas (Computador, Tablet, teléfonos móviles) utilizados en la ejecución de sus labores diarias para este contrato. El EDR debe ser capaz de detectar, prevenir y responder a amenazas cibernéticas de manera proactiva y eficiente.

Entre sus funcionalidades avanzadas este EDR deberá permitir:

- 1.** Control de la superficie de ataque (Protección web, Control y reputación de descargas, control de periféricos y aplicaciones).
- 2.** Supervisiones de instaladores antes que se ejecuten en el dispositivo mediante técnicas next-gen en tiempo real (Deep Learning, aprendizaje automático, agente antiransomware, protección contra ataques sin archivos, Host IPS).
- 3.** Higiene de las operaciones de seguridad TI mediante búsqueda de amenazas guiada (Detección de tráfico malicioso, ejecutables sospechosos, prevención y detección de exploits, prevención de fuga de datos, investigación profunda con análisis de causa raíz, generación de archivos para análisis forense de investigaciones, eliminación de malware y aislamiento automático de Endpoints comprometidos)
- 4.** Funcionalidad de integridad (Listas externas dinámicas e internas de conexiones permitidas y bloqueadas, monitorización de integridad de archivos)

El Contratista deberá proporcionar si es requerido por Gases de La Guajira los informes de monitoreo y respuesta a incidentes, así como tomar medidas inmediatas para remediar cualquier brecha de seguridad detectada y esta ser

reportada en un plazo máximo de 2 horas, este reporte debe ser enviado al correo electrónico ciberseguridad@gasguajira.com

Correo Seguro

El Contratista garantiza que todo el tráfico de correo electrónico que involucre información y datos relacionados con este contrato se enviará y recibirá a través de un sistema de correo seguro. El sistema deberá incluir medidas de protección contra phishing, malware y ataques de ingeniería social.

Adicionalmente, se requiere el cifrado de extremo a extremo para la comunicación de correo electrónico sensible. El CONTRATISTA se compromete a mantener registros de correos electrónicos y proporcionar informes de seguridad relacionados con el correo electrónico según sea necesario.

Borrado Seguro de Dispositivos de Terceros

En el caso de que el Contratista y/o proveedor utilice dispositivos de su propiedad para el procesamiento, almacenamiento o transmisión de datos relacionados con este contrato, se requiere que implemente un proceso de borrado seguro de datos en dichos dispositivos al finalizar su uso.

El proceso de borrado deberá cumplir con las mejores prácticas de seguridad cibernética y garantizar que todos los datos y configuraciones sean eliminados de manera irreversible antes de que los dispositivos sean retirados, dados de baja o reasignados a otros fuera de GASES DE LA GUAJIRA.

Seguridad de los servidores

En caso de que el CONTRATISTA utilice su propia infraestructura de servidores de cualquier tipo para la prestación del servicio contratado, debe asegurar la integridad, confidencialidad y disponibilidad de todos los dispositivos utilizados para procesar la información y datos de GASES DE LA GUAJIRA, y para mitigar la amenaza, riesgo e impacto del uso indebido y abusos externos o internos de las plataformas de servidores, el CONTRATISTA deberá:

1. Proteger el acceso a todos los servidores, como mínimo, mediante una combinación de la identificación (ID) del usuario y la contraseña secreta.
2. Cambiar todas las contraseñas de los servidores que vienen de fábrica antes del comienzo del procesamiento y cambiarlas posteriormente cada cuarenta y cinco (45) días o más frecuentemente.
3. Asegurar que los servidores se encuentren ubicados en zonas físicamente seguras.

4. Reforzar la seguridad de todos los servidores utilizados para procesar, almacenar o transmitir datos e información de GASES DE LA GUAJIRA, debiendo dicho reforzamiento incluir, entre otros, la eliminación de todos los privilegios y servicios salvo aquellos que sean esenciales para la ejecución de las operaciones para las que están instalados dichos servidores.
5. Implementar software estándar de la industria contra programas maliciosos (*malware*) instalado, funcionando, actualizado con el último archivo de firma y debidamente licenciado y al día. El dispositivo debe tener instalado y activo un producto de seguridad tipo cortafuego (*firewall*) personal y estándar de la industria.
6. Registrar toda la actividad de acceso del servidor y almacenar los datos de dicha actividad de una manera apropiada por un período mínimo de doce (12) meses.
7. Revisar periódicamente (al menos una vez al año) todos los controles de seguridad del servidor definidos anteriormente para asegurarse de que todavía estén vigentes.

Desarrollo de Software

En caso de que el alcance del servicio contratado incluya desarrollo de software, EL CONTRATISTA deberá garantizar el cumplimiento de los requisitos de GASES DE LA GUAJIRA y de las mejores prácticas de la industria para los códigos seguros, el CONTRATISTA deberá:

- a) Incorporar el análisis Estático y Dinámico de los códigos de seguridad en el ciclo de vida del desarrollo del software con el fin de mitigar los problemas de seguridad identificados durante el proceso de desarrollo antes de pasarlos al entorno de producción.
- b) Capacitar al recurso humano para la prestación del servicio en prácticas seguras de desarrollo de software y cultura en ciberseguridad.

Seguridad de los archivos de datos y bases de datos

Si el alcance del servicio contratado incluye almacenamiento de información de GASES DE LA GUAJIRA en bases de datos del CONTRATISTA, este deberá asegurar la integridad, confidencialidad y seguridad en general de todas las bases de datos y archivos de datos utilizados para almacenar información y datos de GASES DE LA GUAJIRA, el CONTRATISTA deberá:

1. Almacenar la información "Confidencial" de GASES DE LA GUAJIRA (por ejemplo, contraseñas, datos de los clientes, etc.) en un formato cifrado de conformidad con las mejores prácticas de la industria; y acorde al estándar de criptografía aprobado por GASES DE LA GUAJIRA.

2. Ubicar todos los servidores de bases de datos, servidores de archivos y repositorios que contengan datos de GASES DE LA GUAJIRA en un área físicamente segura.
3. Restringir todo el acceso físico y lógico a las bases de datos, archivos de datos e información y datos almacenados en éstos, así como a cualquier sistema o componente de la red relacionado con el procesamiento de transacciones según un esquema basado solo en la "Necesidad de conocer o usar" del negocio.
4. Proteger todos los accesos a las bases de datos y archivos de datos utilizando, como mínimo, una combinación de la identificación del usuario y la contraseña secreta.
5. Cambiar todas las contraseñas de las bases de datos que vienen de fábrica antes del comienzo del procesamiento y cambiarlas posteriormente cada cuarenta y cinco (45) días.
6. Registrar toda la actividad de acceso a las bases de datos y archivos de datos, y almacenar los datos de dicha actividad de una manera apropiada por un período mínimo de doce (12) meses.
7. Registrar toda la actividad de transacciones y almacenar los datos de dicha actividad de una manera apropiada durante al menos doce (12) meses desde la fecha de cada transacción.
8. Manejar todas las copias de respaldo de todos los registros de las bases de datos y archivos de datos de conformidad con medidas estrictas de seguridad y controles de acceso, ejerciendo controles idénticos o similares a los empleados para las bases de datos y los archivos de datos principales.
9. Una vez finalizado el contrato entre GASES DE LA GUAJIRA Y EL CONTRATISTA, se debe eliminar y destruir de una manera adecuada y segura todas las instancias de cualquier información o datos de GASES DE LA GUAJIRA y material impreso asociado para asegurar que las transacciones y demás datos no puedan ser recuperados por personas no autorizadas.
10. Revisar en forma periódica (al menos una vez al año) todos los controles de seguridad de la base de datos definidos anteriormente para asegurar que continúan vigentes.
11. GASES DE LA GUAJIRA deberá dejar documentada la lista expresa de los datos que está suministrando al Contratista.
12. Los datos que GASES DE LA GUAJIRA suministre al Contratista deberán ser transmitidos mediante canales de comunicación seguros, tales como canales de datos privados o utilizando cifrado cumpliendo los protocolos para tal fin.

Seguridad de la red

Para mitigar la amenaza, riesgo e impacto de intrusiones, abuso o uso indebido del sistema o la red, el CONTRATISTA deberá:

1. Instalar, configurar y activar un sistema integral de protección contra intrusiones (en la red y el host), de conformidad con las mejores prácticas de la

industria, para que en forma continua evite, detecte e informe la ocurrencia de ataques no autorizados a la red y en contra de sus sistemas, incluidos, entre otros, intentos de penetración, ataques por denegación de servicio y sondeos excesivos.

2. Instalar cortafuegos (*firewall*) para redes basados en las mejores prácticas de la industria entre los servidores y las puertas de enlace (*gateways*) a la red pública de modo que excluyan los protocolos de comunicación que no sean necesarios para procesar el tráfico de Internet.
3. Registrar toda la actividad de los cortafuegos y puertas de enlace y almacenar los datos de dicha actividad de una manera apropiada por un período mínimo de dieciocho (18) meses.
4. Proteger los datos contra la divulgación no autorizada durante su tránsito a través de redes públicas a GASES DE LA GUAJIRA, o sus agentes autorizados, o sus clientes, para garantizar la seguridad de los datos que sean propiedad de GASES DE LA GUAJIRA o estén relacionados con GASES DE LA GUAJIRA.
5. Aplicar las técnicas criptográficas, **"Transport Layer Security" (TLS)** asociadas por lo menos a la penúltima versión vigente o superior para la autenticación mutua de certificados (del cliente al servidor o de servidor a servidor), y una longitud mínima de clave de 256 bits o una norma equivalente basada en las mejores prácticas de la industria.

Control de cambios

Si el alcance del servicio contratado incluye desarrollo de software, EL CONTRATISTA deberá garantizar el cumplimiento de los requisitos de GASES DE LA GUAJIRA y de las mejores prácticas de la industria para el control de cambios, EL CONTRATISTA deberá desarrollar, probar y documentar cada cambio de conformidad con la gestión de cambios y las normas, procedimientos y procesos de control, preservando la integridad lógica continua de los datos, programas y rastros de auditoría.

Respaldo y recuperación

Para garantizar el cumplimiento de los requisitos de GASES DE LA GUAJIRA y de las mejores prácticas de la industria para el respaldo y la recuperación, EL CONTRATISTA deberá:

1. Implementar medidas de respaldo adecuadas, incluido el almacenamiento de los archivos de datos de respaldo en lugares seguros fuera del sitio de procesamiento, para permitir la recuperación eficiente del sistema.
2. Facilitar la reanudación de las aplicaciones críticas y actividades de negocios de una manera oportuna después de una emergencia o desastre.
3. Mantener un plan de recuperación de desastres documentado para cada sistema crítico relacionado con GASES DE LA GUAJIRA y para las aplicaciones de negocios, y probarlo anualmente.

Notificación, Alerta y escalamiento de problemas y gestión de incidentes de seguridad

En caso de pérdida, acceso no autorizado, o divulgación no autorizada de la Información Confidencial, Información personal de clientes o colaboradores y otros datos de GASES DE LA GUAJIRA, el proveedor de forma inmediata, después de determinar que ha ocurrido la Violación de la Seguridad de los Datos, deberá:

1. Implementar, mantener y cumplir procedimientos documentados de alerta y escalamiento de problemas, que el Proveedor y GASES DE LA GUAJIRA podrán modificar ocasionalmente de mutuo acuerdo y actuando de forma razonable.
2. Investigará la violación de seguridad de la información y proporcionar a GASES DE LA GUAJIRA la información detallada sobre la violación de seguridad de la información.

De igual forma, notificará a GASES DE LA GUAJIRA de las violaciones de seguridad de los datos al siguiente correo electrónico: ciberseguridad@gasguajira.com.

Auditoría y Cumplimiento

El CONTRATISTA se compromete a someterse a Auditorías de seguridad cibernética periódicas para garantizar el cumplimiento de estas medidas de seguridad. GASES DE LA GUAJIRA podrá realizar auditorías o contratar a terceros para llevar a cabo dicha actividad.

En caso de incumplimiento de cualquiera de las disposiciones de esta cláusula, el CONTRATISTA asumirá la responsabilidad de remediar la situación presentada y cubrir los costos asociados con la recuperación de incidentes de seguridad cibernética.