NORMA DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

CONTENIDO

GASES DEL CARIBE, en su compromiso con la protección de la información que gestiona considera de importancia vital establecer los parámetros que deben seguirse en materia de Adquisición, Desarrollo, Implementación y Mantenimiento de Sistemas de Información que soportan la operación de esta organización.

1. CONSIDERANDOS

a) Que son considerados, de forma general, Sistemas de Información, entre otros, los sistemas operativos; infraestructura; software de aplicaciones o programas de ordenador; servicios informáticos y demás servicios soportados en Tecnologías de Información y Comunicaciones que apoyen la operación de esta organización, cualquiera que sea su forma de contratación o derecho que autorice su uso legítimo.
b) Que, para la estructuración de cualquier adquisición, desarrollo, implementación y/o mantenimiento de un Sistema de Información en esta organización deben identificarse y acordarse los requisitos de seguridad, antes de cualquier invitación a contratar, cualquiera que sea la modalidad de proceso a seguir.
c) Que la seguridad es un presupuesto de todo proyecto soportado en Tecnologías de Información y Comunicaciones en esta organización, el cual en ninguna circunstancia puede ser omitido o eludido, en la medida que no es aceptable ninguna propuesta comercial y/o técnica por parte de terceros proveedores que excluya o limite los requisitos de seguridad que deben ser incorporados en todo Sistema de Información, conforme las necesidades de la organización y riesgos de seguridad que se adviertan.
d) Que es imperativo durante todo el ciclo de vida de un proyecto soportado en Tecnologías de Información y Comunicaciones que los requisitos y controles de seguridad estén de forma clara detallados, justificados, aprobados y documentados; los cuales habrán de constituirse en entregables y/o en criterios de aceptación de los mismos, según sea el caso.
e) Que para efectos de precisión cuando se habla de todo el ciclo de vida del proyecto referido a un producto (bien y/o servicio) soportado en Tecnologías de Información y Comunicaciones en GASES DEL CARIBE se entiende que este inicia desde la fase de planeación del proyecto hasta su puesta en producción y estabilización.
f) Que todo proceso de invitación a contratar debe incluir sin excepciones, los requisitos de seguridad que de forma general se identifiquen, los cuales se solicitará sean complementados de forma detallada por los terceros proveedores interesados en un acápite especial de la propuesta; aspectos que serán considerados al momento de seleccionar el proveedor del proyecto soportado en Tecnologías de Información y Comunicaciones.
g) Que corresponde a la Dirección Digital de esta organización impartir las aprobaciones a los requisitos de seguridad que se definan en cada proyecto soportado en Tecnologías de la Información y Comunicaciones, cualquiera que sea el ciclo de vida del mismo.

2. OBJETO

Esta norma que desarrolla la Política de Seguridad de la Información de GASES DEL CARIBE regula lo relacionado con la Adquisición, Desarrollo, Implementación y Mantenimiento de los sistemas de información que soportan la operación de esta organización, sea que estos sistemas de información sean nuevos o estén sometidos a procesos de mejora continua.

3. DESTINATARIOS

Son destinatarios de esta norma los colaboradores de todo nivel quienes tengan responsabilidad sobre la definición de los requisitos funcionales y no funcionales para el desarrollo y adquisición de sistemas de información para la organización.

4. SISTEMAS DE INFORMACION

Se entiende como sistema de información para efectos de esta norma el conjunto de recursos de información e informáticos organizados para la recolección, procesamiento, mantenimiento, uso, distribución, difusión o la disposición de la información. Hacen parte de los sistemas de información la infraestructura dispuesta por esta organización, de forma directa o por parte de un terceto, para que los usuarios desempeñen sus funciones la cual está compuesta entre otras por el hardware, software, servicios de información y redes, certificados digitales, claves privadas, nombres de usuario y contraseñas, entre otros recursos informáticos.

5. REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACION

Todo Sistema de Información, nuevo o en operación, debe garantizar que la seguridad constituya parte integral de este durante todo su ciclo de vida. El acceso de los usuarios a los sistemas y servicios de información dispuestos por esta organización siempre debe realizarse a partir del nombre de usuario y/o de mecanismos de identificación y autenticación personal de cada usuario, creados cumpliendo los parámetros que defina la organización en esta materia.

5.1.PLANEACIÓN DEL PROYECTO DE TECNOLOGÍA

Es obligatorio en esta organización, que los responsables de la preparación de todo proyecto o iniciativa soportada en Tecnologías de la Información y Comunicaciones que tenga como objeto la adquisición, desarrollo, implementación o mantenimiento de un Sistema de Información, identifiquen los requisitos generales de seguridad que son indispensables para proteger la información que será tratada y procesada a través de estos.

En toda invitación que se dirija a eventuales terceros proveedores para participar en la ejecución de un Proyecto basado en Tecnologías de Información y comunicaciones los oferentes deberán cumplir con lo establecido en las políticas de compras y contratación PD-A-09, y asegurar el cumplimiento del Anexo C14 – "Condiciones de ciberseguridad y Seguridad de la Información" documento en el cual se presentan los lineamientos que se deben cumplir según el objeto del contrato o servicio solicitado.

La propuesta de seguridad presentada por el proveedor seleccionado para la ejecución del Proyecto Tecnológico basado en Tecnologías de la Información y Comunicaciones deberá incorporarse en los términos del contrato respectivo; sin perjuicio del detalle de las especificaciones de seguridad que se identifiquen durante en levantamiento de requisitos de seguridad durante el diseño; las cuales en ningún caso podrán ser consideradas fuera del alcance del objeto contractual inicial. La seguridad es un elemento de la esencia de todo sistema de información en esta organización.

5.2.ANÁLISIS Y ESPECIFICACIÓN DE REQUISITOS DE LA SEGURIDAD DE LA INFORMACIÓN PARA LA IMPLEMENTACIÓN DE SISTEMAS DE INFORMACIÓN.

En la ejecución de todo Proyecto soportado en Tecnologías de la Información y Comunicaciones que tenga como objeto la adquisición, desarrollo, implementación y/o mantenimiento de un Sistema de Información en esta organización deberá documentarse en detalle los requisitos mínimos de seguridad de la información que estén presentes. Esto requisitos y los demás que puedan definirse durante el proyecto aplican cuando estos involucren la trasmisión de información sobre redes públicas y/o privadas.

Debe tenerse presente que los requisitos de seguridad que se enuncian y los demás que se adopten propugnan por la seguridad de la información, la preservación de los atributos de la información, la protección contra actividades fraudulentas que den origen a disputas contractuales y/o legales originadas en las transacciones o actividades que se realicen en los sistemas de información.

A continuación, se enuncian los requisitos que se recomienda estén presentes en todo sistema de información, nuevo o actualmente en funcionamiento sujeto a una mejora, que soporte la operación de esta organización, a saber:

- Gestión de accesos y privilegios.
- Gestión de errores de cara al usuario final.
- Gestión de errores de cara al administrador del sistema de información.
- Transporte de Datos.
- Uso de cifrado de datos.
- Calidad de los Datos.
- Gestión del Rendimiento.
- Aseguramiento del Código de Software.
- Ambientes Desarrollo, calidad y Producción.

La organización para cumplir con estos requisitos evaluará aquellos sistemas de misión crítica que deban cumplir con los requisitos de seguridad más robustos, acorde a las necesidades de la organización.

La reducción en los requisitos de ciberseguridad, acorde al tipo de activo de información y su clasificación, que se llegare a adoptar deberá estar justificada, acordada y documentada; la cual requiere de la aprobación de la Dirección Digital.

Si los controles de seguridad básicos o establecidos por defecto en el software objeto de adquisición, implementación o mantenimiento no responden a las necesidades de seguridad de esta organización, de acuerdo con la clasificación de la información existente y su respectiva evaluación en la fase de planeación, estos requisitos de seguridad deberán ser fortalecidos, adicionados y especificados en los términos aquí indicados para la ejecución del respectivo proyecto.

5.3.PROTECCIÓN DE LAS TRANSACCIONES DE LOS SERVICIOS DE APLICACIONES

Respecto de las transacciones que se realicen en los sistemas de información. Los requisitos de seguridad que se definan deberán evitar: trasmisión incompleta de información; enrutamiento errado y/o no autorizado; pérdida de integridad; afectación de la confidencialidad o divulgación no autorizada; duplicación o reproducción de los mensajes no

autorizada; entre otras situaciones que afecten atributos como la integridad, confidencialidad, autenticidad, disponibilidad.

6. PROCESAMIENTO CORRECTO DE APLICACIONES

En la ejecución de todo Proyecto soportado en Tecnologías de la Información y Comunicaciones que tenga como objeto la adquisición, desarrollo, implementación y/o mantenimiento de un Sistema de Información en esta organización debe garantizarse que los requisitos de seguridad de la información definidos en la fase de planeación y análisis de requisitos cumplan las siguientes validaciones y controles.

- Validación de datos de entrada.
- Control de procesamiento interno.
- Integridad del mensaje de datos.
- Validación de los datos de salida.

7. SEGURIDAD EN LOS PROCESOS DE DESARROLLO, IMPLEMENTACION, SOPORTE Y MANTENIMIENTO

La seguridad de la información constituye un requisito indispensable que debe ser considerado no solo en las etapas de planeación y diseño de un sistema de información, sino que debe ser parte fundamental del funcionamiento y mejora a través del mantenimiento preventivo, correctivo y/o evolutivo.

7.1. PARÁMETROS PARA EL DESARROLLO SEGURO

La seguridad de un sistema de información está determinada en gran medida por la calidad del Software, la cual solo se puede verificar y evaluar a la luz del proceso de pruebas. Las pruebas constituyen el conjunto de actividades que permiten determinar en qué medida el software cumple con los requisitos y con las necesidades definidas por esta. El proceso de pruebas pretende que estas permitan identificar de forma temprana los errores y que estos sean corregidos antes de que el software este en producción, evitando los altos costos de solución de tales en etapas posteriores a su puesta en producción.

No es recomendable la puesta en producción de un sistema de información sin haber agotado el proceso de gestión de pruebas definido de forma particular al interior de cada proyecto de tecnología, el cual, en ningún caso, puede ser inferior a los mínimos definidos en este documento y en la Política de Seguridad de la Información de esta organización.

El tipo de pruebas que se recomienda se deben aplicar al software a implementar son las siguientes:

- Pruebas de Especificaciones.
- Pruebas Unitarias s.
- Pruebas de Integración.
- Pruebas de Validación.
- Pruebas de Seguridad.
- Pruebas de Resistencia.
- Pruebas de Rendimiento.

Para la ejecución de estas pruebas es recomendable que al interior del proyecto tecnológico estas se gestionen conforme los siguientes momentos:

- **Fase de Planificación de las Pruebas.** El propósito es elaborar y comunicar a las partes interesadas el plan de pruebas diseñado, el cual contendrá el alcance, la estrategia a usar para las pruebas los recursos involucrados, el entorno en el cual se ejecutarán, definición de métricas y demás requisitos que sean indispensables para asegurar la calidad del software a implementar en esta organización.
- **Fase de Ejecución de las Pruebas**. El propósito es diseñar en detalle las pruebas según su tipo, preparar el ambiente de las pruebas, ejecutar las pruebas, medir las pruebas y documentar las incidencias y resultado de las pruebas.
- **Fase de Monitoreo y Control de Pruebas**. El propósito es asegurar que las pruebas son realizadas de acuerdo con el plan de pruebas y estrategia definida.
- **Fase de Terminación**. El propósito es verificar y validar que las pruebas hayan cumplido los criterios de aceptación definidos de acuerdo con el plan de pruebas con el fin de dar por terminada esta fase.

La organización, según las necesidades operacionales, podrá reducir el formalismo del proceso de pruebas, considerando la urgencia del proyecto, sin que esto implique omitir la necesidad de que el software sea seguro.

7.2. CONTROL DE CAMBIOS EN LOS PROYECTOS

En la ejecución de todo proyecto soportado en Tecnologías de la Información y Comunicaciones en esta organización deberá documentarse, mediante el procedimiento de control de cambios, toda modificación a los requerimiento o requisitos definidos y aprobados en las fases de levantamiento y/o análisis de estos.

En el respectivo contrato se incluirá la previsión contractual que regule el procedimiento de control de cambios a seguirse. Contractualmente los cambios solo serán aprobados por el gerente del proyecto siguiendo el conducto regular establecido al interior de esta organización; por tanto, carecerán de validez contractual y fuerza vinculante los controles de cambio ejecutados sin cumplir el procedimiento definido en el contrato.

7.3. CONTROL DE CAMBIOS EN LOS SISTEMAS

Antes de aprobar un cambio en los sistemas de información que soportan la operación de esta organización, sea en la fase previa o en la fase posterior a su puesta en producción, deberá evaluarse que el mismo no comprometa la seguridad de la información ni el entorno operativo sobre el cual funciona este, ni modifica las condiciones de riesgos de la operación del sistema de información, los usuarios y sus datos.

La evaluación debe incluir un análisis del cambio y del impacto de este sobre los usuarios y los sistemas ya existentes, así como la especificación de los controles de seguridad de la información que deberán ser adoptados en el cambio a introducir. El cambio que se pretenda introducir no puede comprometer los controles de seguridad adoptados previamente tanto a nivel funcional como a nivel de roles de acceso definidos para usuarios y/o personal que den soporte al sistema.

Los controles de cambios que se pretendan introducir a un sistema de información se aconseja que contengan, entre otros aspectos y sin limitarse a estos, la siguiente información y/o evaluaciones:

Un registro de los niveles acordados de autorizaciones

- Certeza de que los cambios son realizados por los usuarios autorizados según su cargo o funciones dentro de la organización
- Revisión de los controles para garantizar que los cambios no comprometen la integridad de la información desde los datos de entrada, procesamiento y salida de datos.
- Identificación de todos los componentes del sistema de información comprometidos en el cambio a realizar. Capacitaciones a los usuarios principales del sistema y acompañamiento en su adaptación de sus procesos en el mismo.
- Resultado de las pruebas realizadas por los usuarios impactados por los cambios a realizar.
- Documentación del cambio realizado y preservación de la documentación previa al cambio a realizar, cuando ello fuere necesario.
- Mantenimiento de la versión del control del cambio para todas las actualizaciones del sistema de información objeto del mismo, así como respecto de las integraciones impactadas.
- Preservación obligatoria de los logs o trazas para auditar los cambios en el sistema de información objeto del cambio.
- Garantía de que la documentación operativa y los procedimientos de usuario se cambian en función de la necesidad con el fin de mantener la idoneidad del sistema de información, siempre que esto fuera indispensable lo cual deberá ser justificado.
- Garantía de que los cambios a implementar se realizan en el momento oportuno y que estos no perturban los procesos de negocios involucrados.

Todo cambio en el sistema de información deberá ser sometido al proceso de prueba que obligatoriamente debe ser pactado a nivel contractual. Esto se aplica igualmente a las actualizaciones de seguridad, paquetes de servicios y otras actualizaciones. Las actualizaciones automáticas deberán ser controladas con el fin de evitar fallas en aquellos sistemas de información que tengan carácter crítico.

La organización, según las necesidades operacionales, podrá reducir el formalismo del proceso de control de cambio en el software y/o proyecto tecnológico, considerando la urgencia del proyecto, sin que esto implique omitir la necesidad de que el software sea seguro

7.4. REVISIÓN TÉCNICA DEL SOFTWARE DESPUÉS DE CAMBIOS EN EL SISTEMA OPERATIVO

Antes de proceder a realizar cambios en los sistemas operativos se debe evaluar el impacto en los sistemas de información críticos que soportan la operación de esta organización. En ejecución del proyecto de cambio del sistema operativo se deben probar las aplicaciones críticas para evaluar si existe compromiso en la seguridad de la información; caso en el cual deberán adoptarse los controles que permitan preservar la seguridad de la información en poder de esta organización.

El proyecto que involucre cambios en el sistema operativo debe comprender los siguientes aspectos:

- Revisar que los procedimientos de integridad y control de los sistemas de información críticos no hayan sido afectados como resultado del cambio.
- Garantizar en los contratos con el proveedor del sistema operativo notificaciones previas sobre los cambios en el sistema operativo que permitan realizar pruebas con el fin de

asegurar, previa la realización del cambio, la preservación de las condiciones de seguridad de la información definidas por esta organización.
- Garantía de que se hacen cambios en los planes de continuidad del negocio.
- Esta organización, a través de la Dirección Digital deberá definir el responsable y asignar las responsabilidades relativas al monitoreo de las vulnerabilidades que se identifiquen en el sistema operativo instalado, así como la identificación de las nuevas versiones de actualizaciones de seguridad o soluciones a las vulnerabilidades comunicadas por el fabricante del sistema operativo. Sea que esto lo realice directamente la organización o lo contrate con terceros.

7.5. RESTRICCIONES EN CAMBIOS A PAQUETES DE SOFTWARE

El software que soporta la operación de esta organización preferiblemente debiera funcionar únicamente sobre el estándar provisto por el fabricante. Cuando se defina la necesidad de realizar cambios o agregar funcionalidades adicionales a las contempladas en el estándar del software deberá propenderse por realizar solo aquellos cambios que sean necesarios y estén justificados, los cuales se deberán controlar de forma diligente.

En aquellos casos en que sea necesario un cambio en el estándar del software deberá evaluarse previamente el compromiso que pueda presentarse respecto de la seguridad de la información y deberá contemplarse en el respectivo proyecto tecnológico los siguientes aspectos:

- Riesgos sobre la integridad de la información y controles que den respuesta a los riesgos que se identifiquen.
- Solicitar la intervención del fabricante cuando el cambio implique una modificación a nivel del código fuente.
- Desarrollar los cambios aplicando las mejores prácticas a nivel de ingeniería de software, conforme las indicaciones del fabricante, con el fin de mitigar el riesgo de afectación en el funcionamiento del software como resultado de estos; como puede ser el desarrollo de cambios como personalizaciones fuera del estándar.
- Tener presente que los cambios realizados podrán ser afectados por las actualizaciones en el paquete de software liberado por el fabricante.

En esta organización deberá regularse en la relación contractual con el fabricante del software y/o terceros proveedores el mantenimiento preventivo y correctivo tanto del estándar del software como de los cambios introducidos al software a nivel de personalizaciones. Todo cambio en el software debe ser probado y documentado en su totalidad, con el fin de aplicarlo nuevamente cuando así fuere necesario, para mejoras futuras del software.

7.6. PRINCIPIOS DE ORGANIZACIÓN DE SISTEMAS DE INFORMACIÓN SEGUROS

La seguridad de los sistemas de información es una actividad de garantía del software que se centra en la identificación y evaluación de los riesgos potenciales que pueden producir un impacto negativo en el software y conducir por tanto a una falla generalizada de este, la cual pueden comprometer la seguridad de la información.

En esta organización la calidad del software debe gestionarse desde tres criterios, a saber: calidad del producto, calidad en el uso y calidad en los datos. Con el ánimo de contribuir a la madurez de los sistemas de información considerando la perspectiva de la seguridad se indican los principios que deben tenerse presentes en los proyectos tecnológicos en materia de pruebas del Software:

i. **Adecuación Funcional**. Se predica de la capacidad del Software para proporcionar las funciones que satisfacen las necesidades, declaradas e implícitas, cuando este se usa en las condiciones especificadas; ello implica completitud, corrección y adecuación funcional.
ii. **Eficiencia en el Desempeño**. Se predica del desempeño del Software para intercambiar información o en relación con la cantidad de recursos utilizados en determinadas condiciones; ello involucra los tiempos de respuesta y procesamiento y el uso racional de los recursos involucrados en el desempeño.
iii. **Compatibilidad**. Se predica de la capacidad del Software para intercambiar información o ejecutar las funciones requeridas en relación con el hardware y/o software; esto comprende la coexistencia e interoperabilidad con otros sistemas de información y el uso de la información intercambiada.
iv. **Capacidad de Uso**. Se predica de la capacidad del producto para ser entendido, aprendido y usado, y para ser amigable con el usuario, en determinadas condiciones. Este principio se refleja en el atributo de ser fácil de entender y operar, fomentar el aprendizaje, prevenir que se incurra en errores, estética de la interfaz y accesibilidad por parte de usuarios con discapacidades.
v. **Fiabilidad**. Se predica de la capacidad del Software o sus componentes para ejecutar las funciones especificadas cuando se usa bajo determinadas circunstancias y períodos. Este principio se materializa en la madurez del sistema, disponibilidad, tolerancia a fallas y capacidad de recuperación después de una falla o interrupción.
vi. **Seguridad**. Se predica de la capacidad del software para proteger la información y los datos, de forma que se impida su lectura o modificación por personas o sistemas no autorizados; lo cual se expresa en garantizar los atributos de confidencialidad, integridad, no repudio, autenticidad y trazabilidad.
vii. **Mantenibilidad.** Se predica de la capacidad de Software para ser modificado bajo criterios de efectividad y eficiencia de acuerdo con las necesidades evolutivas, correctivas y preventivas. Este principio se refleja en la modularidad, reusabilidad y capacidad de ser analizado, modificado y probado.
viii. **Portabilidad**. Se predica de la capacidad del producto o componente de ser transferido de forma efectiva y eficiente a entornos de hardware, software y operatividad diferente al que funciona en ese momento; lo cual se expresa en la posibilidad de adaptarse, instalarse y reemplazar otro sistema de información con el mismo propósito y mismo entorno del actual.

Estos criterios se aconsejan estén incorporados en todo proyecto basado en Tecnologías de la Información y las Comunicaciones que soporte la operación en esta organización, según las necesidades y la respectiva criticidad del sistema de información a implementar.

7.7. AMBIENTE DE DESARROLLO Y CALIDAD EN LOS SISTEMAS DE INFORMACIÓN

En los proyectos de desarrollo y/o en la implementación de software en esta organización deberá acudirse a ambientes diferenciados que garanticen la seguridad de la información y el correcto funcionamiento de los sistemas de información. Para el efecto deberá tenerse presente los requisitos de seguridad dispuesto para el ambiente de producción.

Adicional a lo anterior, en cada proyecto se establecerá la necesidad de crear ambientes de desarrollo y calidad si la organización acorde a sus necesidades lo considera conveniente.

En ningún caso, se procederá a realizar cambios en ambientes productivos, pues tal situación comprometería la seguridad de la información de esta organización.

7.8. PRUEBAS DE LOS SISTEMAS DE INFORMACIÓN

En los proyectos de desarrollo y/o en la implementación de software en esta organización es aconsejable se realicen los siguientes tipos de prueba:

- Unitarias
- Integrales
- Rendimiento
- Seguridad
- Las demás requeridas según las características del proyecto y/o el estado de la técnica.

No se recomienda que un proyecto soportado en Tecnologías de la Información y las Comunicaciones se ejecute al margen de las necesidades de seguridad que deben caracterizar a todo software y/o sistema de información nuevo u objeto de mejora que funcione en esta organización.

7.9. SEGURIDAD DE LOS DATOS DE PRUEBA

En los proyectos soportados en Tecnologías de la Información y las Comunicaciones que se ejecuten en esta organización se debe garantizar la protección de los datos usados en los procesos de prueba.

En los procesos de prueba requeridos en tales proyectos se debe evitar que las pruebas requeridas se realicen usando bases de datos que contengan función personal y/o información estratégica de esta organización.

En caso de establecerse que las pruebas requieren el uso de datos personales reales deberán propenderse por aplicar técnicas de Anonimización de datos que otorguen seguridad a tal información; de no ser factible, el proveedor responsable de las pruebas deberá suscribir un acuerdo de protección de información personal.

Para efectos de dar seguridad a los datos de prueba deberán adoptarse entre otras directrices las siguientes:

- Aplicar los procedimientos de control de acceso durante los procesos de pruebas que se realicen tanto a nivel de sistemas operativos como a software de aplicaciones.
- Autorizar de forma individual cada copia que se realice de las bases de datos que contengan información personal y/o estratégica de la organización.
- Toda información de la organización usada durante el proceso de pruebas debe ser eliminada de este ambiente y deberá obtenerse la certificación del representante legal del proveedor en el sentido de que no conservan copia de tal información; en caso de ser necesario conservar copia de tal información deberá justificarse previamente y tal situación ser aprobada por el.

El proveedor responsable de realizar las pruebas, que acceda a información personal para la ejecución de esta prestación informática, se entenderá para efectos del régimen de datos personales como Encargado del tratamiento; situación que lo hace responsable frente a la organización por cualquier situación que comprometa la seguridad de la información personal tratada durante esta etapa.

7.10. PRUEBAS DE ACEPTACIÓN DE LOS SISTEMAS DE INFORMACIÓN

Las pruebas constituyen un presupuesto fundamental de la calidad de un proyecto soportado en Tecnologías de la Información y las Comunicaciones. Por tanto, en la contratación de tales proyectos debe regularse y controlarse de forma rigurosa la ejecución de las pruebas a realizarse.

Si bien en las pruebas intervienen los usuarios del Software por parte de esta organización, el diseño de las pruebas es una responsabilidad del proveedor tecnológico en su calidad de experto conocedor del software y de las características del mismo. Constituye buena práctica de la ingeniería de software que el equipo del proveedor que diseñe y/o ejecute las pruebas sea diferente de aquel que intervino en el desarrollo del software y/o en la configuración necesaria para la puesta en producción de este.

Respecto del proceso de pruebas deben establecer métricas para evaluar las pruebas, las cuales constituyen criterios de aceptación, sin perjuicio de los demás criterios de aceptación que se pacten acorde a la naturaleza del proyecto tecnológico. El líder de implementación de dicho sistema es el responsable de coordinar la aprobación de las pruebas de seguridad realizadas respecto del software involucrado en el respectivo proyecto tecnológico.

Si el proceso de pruebas respecto del software desarrollado y/o implementado no se ha realizado de manera rigurosa, esta organización debe abstenerse de autorizar la entrada en producción del mismo y exigir al proveedor que cumpla con este requisito de la esencia del contrato.

7.11. SOFTWARE CONTRATADO CON TERCEROS

Todo desarrollo de software a la medida encargado a terceros contratistas debe comprender los requisitos de seguridad definidos durante la ejecución del proyecto contratado, así mismo, el propio desarrollo debe estar caracterizado por buenas prácticas de ingeniería de software, calidad en el desarrollo y seguridad informática.

En el desarrollo de software a la medida debe propenderse porque las pruebas a las que este debe someterse sean realizadas por personas diferentes a quienes intervinieron en la programación del código, pues solo así, puede existir objetividad y lograrse el objetivo de calidad y seguridad en el desarrollo del software.

De acuerdo con las normas legales colombianas en materia de propiedad intelectual toda obra por encargo corresponde a quien la encarga, en este caso a esta organización; razón por la cual en el contrato respectivo debe regularse la propiedad intelectual de GASES DEL CARIBE SA ESP sobre la respectiva creación informática.

7.12. CONTROL DE ACCESO AL CÓDIGO FUENTE DEL SOFTWARE

Respecto al software propietario de los cuales esta organización ejerce los derechos patrimoniales de autor es obligatorio controlar el acceso al código fuente y demás documentación elaborada durante la ejecución del proyecto que dio origen a la creación informática; en tal sentido, el acceso restringido también se predica respecto de los requerimientos técnicos, análisis, diseño, resultados de pruebas, integraciones, manuales, entre otros. El código fuente y sus actualizaciones como parte de un activo de información estratégico para esta organización deberá ser mantenerse seguro y almacenado en bibliotecas

protegidas para evitar riesgos de seguridad de la información, para ello se seguirán las indicaciones de la Dirección Digital.

El código fuente del software propiedad de esta organización, como activos de información, constituye propiedad intelectual de esta organización, razón por la cual deben ser protegidos tanto a nivel contractual, además de las medidas de seguridad físicas, lógicas y administrativas.

El acceso al código fuente del software solo podrá ser realizado por el personal autorizado y para los fines exclusivamente permitidos; en tal sentido, se llevarán registros que permita hacer trazabilidad al personal autorizado y a las actividades realizadas por estos en el código fuente. Todo acceso no autorizado deberá ser informado a la Dirección Digital y ser tratado como incidente de ciberseguridad.

7.13. CONTROL DE LAS CONFIGURACIONES DE LOS SOFTWARE IMPLEMENTADOS EN LA ORGANIZACIÓN

Las configuraciones de los Software implementados en GASES DEL CARIBE, como son los que soportan el proceso administrativo y los propios de cada servicio, entre otros que sostienen la operación de esta organización, deben ser protegidos contra acceso no autorizado y/o fuga de información. Las configuraciones del software incorporan una visión particular de las reglas de negocio que la ley ha delegado en el sector subsidios; por tanto, esa visión particular constituye elementos diferenciadores y competitivos que permiten a la organización participar en el mercado, que a su vez adquieren la entidad de activos de información.

Las configuraciones deben ser protegidas contra acceso no autorizado y/o contra cualquier otra conducta que atente contra la seguridad de la información como puede ser la integridad, la confidencialidad, la autenticidad, la disponibilidad entre otros atributos de la información.

El acceso a las configuraciones del software implementado solo podrá ser realizado por el personal autorizado y para los fines exclusivamente permitidos; en tal sentido, se llevarán registros que permitan hacer trazabilidad al personal autorizado y a las actividades realizadas por estos en el código fuente. Todo acceso no autorizado deberá ser informado a la Dirección Digital ser tratado como incidente de ciberseguridad.

Las configuraciones del software implementados en la organización constituyen activos de información y por tanto son propiedad intelectual de esta organización, razón por la cual merecen ser protegidas tanto a nivel contractual, además de las medidas de seguridad físicas, lógicas y administrativas.

7.14. SOFTWARE LICENCIADO A LA ORGANIZACIÓN

Todo software instalado en la organización debe estar correctamente licenciado por razones de ley y por razones de seguridad de la información. Por tal motivo, en las relaciones contractuales con terceros respecto del licenciamiento de software deben obligatoriamente tenerse presente las siguientes previsiones:

- El otorgamiento del derecho de uso respecto del software y/o cualquier otro derecho patrimonial de autor solo puede ser emitido por el fabricante del software; por tanto, los canales deben aportar la licencia expedida por el fabricante en idioma español cumpliendo con los tramites de ley respecto de las traducciones; la omisión de este requisito

compromete la legalidad del licenciamiento y por tanto la seguridad de la información de la organización.

- Debe exigirse el deber de información y debido asesoramiento a el fabricante o canal que represente al fabricante del software con el fin de que exista certeza en el licenciamiento en cuanto a la cantidad y calidad de las licencias objeto de un licenciamiento. Así mismo, debe exigirse responsabilidad en caso de que el fabricante o canal induzca a un licenciamiento inadecuado que cause perjuicios a esta organización.

En relación con la facultad de auditoria prevista en algunos contratos de licenciamiento de Software, antes de correr cualquier programa informático para verificar la conformidad del licenciamiento existente, deberá informarse a la Dirección Digital Previo a ello, el fabricante deberá suministrar las características del programa informático a ejecutarse, así como los riesgos que puede generar este para la seguridad de la información en la organización, indicando las responsabilidades que asume en caso de causar algún perjuicio a esta organización como resultado de tal acción.

7.15. MANTENIMIENTO, ACTUALIZACIÓN Y SOPORTE

Esta organización, a través del responsable del sistema de información y el líder del l proceso soportado por dicho sistema, definirán la necesidad de suscribir contratos de Mantenimiento (correctivo, preventivo y/o evolutivo); Actualización de versiones y Soporte a estos.

En las relaciones contractuales con los terceros que provean estos servicios informáticos deberá garantizarse la seguridad de la información en esta organización.

7.16. FUGA DE INFORMACIÓN

El principio de confidencialidad como atributo de la información tiene como objetivo que la información, según sus características, sea accesible solo para las personas autorizadas por la organización. En consecuencia, la prevención de la fuga de información constituye un imperativo en la gestión segura de esta, a la cual deben contribuir todos los colaboradores y terceros proveedores que debido a su actividad deban realizar cualquier tratamiento respecto de ella.

Para efectos de prevenir el riesgo de fuga de información esta organización adoptará medidas de seguridad de orden lógico, físico y administrativo, además de las facultades de monitoreo y auditoria que deberá adoptar para lograr el objetivo de confidencialidad sobre la información. Las acciones que podrá adoptar esta organización comprenden, sin limitarse a ellas, las siguientes:

Identificar, proteger y gestionar los activos de información propiedad de esta organización.

Implementar software que prevenga la fuga de información.

Explorar los sistemas de información y de comunicaciones para identificar riesgos de fuga de información.

Monitorear las actividades que colaboradores y/o terceros realizan en los sistemas de información y/o recursos que soportan la operación de esta organización.

Los incidentes de seguridad que comprometan los datos personales que trata esta organización en calidad de responsable deben ser notificados a la Superintendencia de Industria y Comercio, la cual tiene la calidad de autoridad en esta materia.

Los incidentes de seguridad serán gestionados conforme lo definido en la política de seguridad de la información y norma de gestión de incidentes de seguridad adoptadas por la organización.

8. SEGURIDAD DE LOS DATOS DE PRUEBA

En los proyectos soportados en Tecnologías de la Información y las Comunicaciones que se ejecuten en esta organización se debe garantizar la protección de los datos usados en los procesos de prueba.

El proveedor responsable de las pruebas deberá suscribir un acuerdo de protección de información personal. El proveedor responsable de realizar las pruebas, que acceda a información personal para la ejecución de esta prestación informática, se entenderá para efectos del régimen de datos personales como Encargado del tratamiento; situación que lo hace responsable frente a la organización por cualquier situación que comprometa la seguridad de la información personal tratada durante esta etapa.

9. GESTION DE VULNERABILIDADES TECNICAS

La seguridad de los sistemas de información que soportan la operación de la organización exige una estrategia permanente para gestionar las continuas vulnerabilidades a las que se ven expuestos estos, sumado al incremento exponencial de la cibercriminalidad.

Las vulnerabilidades técnicas de todos los componentes de la infraestructura tecnológica deben identificarse y gestionarse, durante todo el ciclo de vida de los servicios. Los esfuerzos de mejora continua deben tender a identificar y resolver las vulnerabilidades en las etapas tempranas del ciclo de vida del servicio, minimizando los recursos de remediación y el posible impacto para los servicios en producción.

Las vulnerabilidades se deben evaluar y priorizar teniendo en cuenta entre otras: la facilidad de explotación, las consecuencias de explotar la vulnerabilidad, y la importancia del componente afectado para la operación de la organización.

La remediación y aplicación de parches y actualizaciones de seguridad deben tender a realizarse de forma automática, mitigando los riesgos asociados, y acorde a los procedimientos establecidos de gestión de cambios.

10. CONTROL

Este documento deberá revisarse de manera periódica con el fin de realizar las actualizaciones que se consideren necesarias cuando surja un cambio importante.

11. USO EXCLUSIVO

12.APROBACION DE ESTA POLITICA

Este documento fue aprobado teniendo en cuenta las actividades descritas en el procedimiento de Normalización y Control de Documentos y Registros PD-A-11 y se encuentra publicado en la Red de Documentos de Gases del Caribe SA ESP