1. OBJETIVO

Establecer las obligaciones mínimas en seguridad de la información y ciberseguridad que debe cumplir los contratistas de Oleoducto de Colombia S.A., en adelante “ODC” o “EL CONTRATANTE”.

2. ALCANCE

Este documento aplica a los contratistas y subcontratistas que desarrollen actividades para ODC.

3. PREMISAS

Las obligaciones contenidas en este documento no eximen al contratista del cumplimiento de la normatividad Colombiana vigente en materia de seguridad de la información y protección de datos.

4. ACTIVIDADES

4.1 CUMPLIMIENTO DE POLÍTICAS DE SEGURIDAD

En línea con las políticas, normas y procedimientos del modelo de seguridad de la información de EL CONTRATANTE, Todos los empleados, colaboradores, dependientes, subcontratistas y en general el personal que designe EL CONTRATISTA para la ejecución del presente contrato, deben dar cumplimiento y acatar las políticas de gestión de seguridad de la información y ciberseguridad que establezca EL CONTRATANTE, así como los documentos relacionados en materia de seguridad de la información y ciberseguridad, los cuales les serán dados a conocer una vez sea suscrito el contrato.

El incumplimiento de las políticas de seguridad de la Información y demás documentos relacionados en materia de seguridad de la información y ciberseguridad, será causal de sanciones que pueden incluir hasta la terminación unilateral del contrato, sin perjuicio de las demás acciones que pueda tomar EL CONTRATANTE, sin que deba reconocer a EL CONTRATANTE el pago de indemnización alguna.

4.2 SEGURIDAD DE LA INFORMACIÓN

EL CONTRATISTA deberá implementar, mantener y hacer cumplir las medidas de seguridad administrativas, técnicas y físicas apropiadas para garantizar la integridad, confidencialidad y disponibilidad de los datos de EL CONTRATANTE y la información personal, proteger contra amenazas anticipadas o riesgos para la seguridad o la integridad de las partes, los datos e información personal, y proteger contra el acceso no autorizado o la utilización de los datos de las partes y la información personal. Estas garantías no podrán ser inferiores a las aceptadas por la industria, incluye un plan de seguridad de la información, los controles de acceso a la información, la protección de los sistemas ejemplo: protección de intrusos y software malicioso), medidas de seguridad física, cifrado de datos, y la formación a conciencia en seguridad de los empleados.

4.3 SOFTWARE

EL CONTRATISTA garantiza que cualquier software que emplee para el desarrollo de este contrato,

es de su exclusiva propiedad o está debidamente licenciado y cumple con la legislación vigente en materia de derechos de autor. Así mismo, se obliga a no utilizar el software de EL CONTRATANTE para fines diferentes de la ejecución del presente contrato, así en algún momento existiera la posibilidad de hacerlo gracias al conocimiento técnico sobre el mismo que haya adquirido en desarrollo de este contrato, ni darlo a conocer a un tercero por ningún motivo. EL CONTRATISTA se abstendrá de reproducir por cualquier medio el software, la documentación o cualquier otra parte, distribuir o comercializarlo, o permitir que personas no autorizadas por EL CONTRATANTE tengan acceso al software o a la documentación relativa a éste, o hagan uso de este. Igualmente, a EL CONTRATISTA le estará prohibido usar el programa de software para fines diferentes a los que EL CONTRATANTE indique, o practicar ingeniería reversa, descifrar o descodificar el programa de software, adoptarlo, modificarlo o en general utilizar el software o realizar cualquier acto que pueda implicar violación de derechos de propiedad intelectual del software de EL CONTRATANTE o de sus contratistas. EL CONTRATISTA no violará ni permitirá que sus empleados o contratistas violen el software suministrado por EL CONTRATANTE.

4.4 PROTECCIÓN CONTRA SOFTWARE MALICIOSO

EL CONTRATISTA debe tomar las siguientes medidas para mitigar los riesgos relacionados con virus informáticos, gusanos, troyanos, keyloggers, botnets, ransomware y otros tipos de software malicioso, comúnmente denominado "malware":

a) Instalar, configurar, activar y mantener actualizado un software antivirus y anti-espías (anti-spyware) basado en las mejores prácticas de la industria, en todos los servidores, dispositivos, computadoras portátiles y estaciones de trabajo que procesen o almacenen las transacciones y cualquier otro dato de EL CONTRATANTE.

b) Configurar dicho software anti-malware para invocarlo automáticamente en el arranque y ejecutarlo interactivamente de forma continua, en todos los dispositivos donde esté instalado.

c) Informar todos los incidentes relacionados con el malware a EL CONTRATANTE con la debida oportunidad.

4.5 GESTION DE ACTUALIZACIONES

EL CONTRATISTA deberá realizar las siguientes actividades tendientes a mitigar los riesgos de vulnerabilidades de seguridad en la infraestructura tecnológica o red de EL CONTRATANTE:

a) Implementar un proceso continuo para investigar en fuentes confiables de advertencias sobre vulnerabilidades de seguridad emergentes.

b) Identificar las vulnerabilidades específicas que puedan impactar los componentes de la infraestructura tecnológica utilizada por EL CONTRATISTA que sea de propiedad o donde se procesa información de EL CONTRATANTE.

c) evaluar la criticidad de las vulnerabilidades y determinar la conveniencia de instalar la correspondiente actualización de seguridad.

d) probar e instalar oportunamente las actualizaciones de seguridad.

4.6 RESPONSABILIDAD AL CONECTAR DISPOSITIVOS A LA RED TECNOLÓGICA DE ODC

Todos los dispositivos utilizados por los empleados de EL CONTRATISTA que se vayan a conectar a la red o infraestructura tecnológica de EL CONTRATANTE, para el cumplimiento del presente Contrato deben cumplir con los siguientes requisitos:

a) Deben estar al día las actualizaciones más recientes y todos los parches de seguridad aplicables a los sistemas operativos y software que se encuentren en los dispositivos.

b) Los dispositivos deben tener instalado el software contra software maliciosos (malware) instalado, funcionando y actualizado.

c) Los dispositivos deben tener instalado y activo un producto de seguridad tipo firewall personal y estándar del mercado.

d) Asegurar que los datos sensibles suministrados por EL CONTRATANTE no serán tratados a través de dispositivos móviles, celulares, tabletas, etc.

4.7 PROTECCIÓN DE SERVIDORES

Con el fin de velar por la integridad, confidencialidad y disponibilidad de la información soportada en los servidores utilizados para procesar dicha información y datos personales de EL CONTRATANTE, EL CONTRATISTA deberá:

a) proteger el acceso a todos los servidores, como mínimo, mediante una combinación de la identificación (ID) del usuario, contraseña y doble factor de autenticación.

b) cambiar todas las contraseñas que vienen por defecto del fabricante en los sistemas operativos y software base, los cuales son de conocimiento público, antes del inicio del procesamiento y cambiarlas posteriormente de forma periódica.

c) los servidores deben estar ubicados en zonas físicamente restringidas, a donde tendrán acceso sólo aquellas personas autorizadas que estrictamente lo requieran para cumplir con sus funciones.

d) fortalecer la seguridad de los servidores (Hardening) utilizados para procesar, almacenar o transmitir información de EL CONTRATANTE, incluyendo entre otros, la eliminación de todos los privilegios y servicios que no son esenciales para la ejecución de las operaciones para las que están instalados dichos servidores.

e) implementar mecanismos de análisis de la seguridad de los servidores para evaluar e informar periódicamente el estado de cada servidor y verificar que las configuraciones, parámetros y opciones están conformes con las líneas base definidas para ese dispositivo y detectar cambios no autorizados.

f) mantener activos los logs de auditoría del servidor y almacenarlos por un período mínimo de dos (2) años.

g) revisar por lo menos una vez al año todos los controles de seguridad del servidor, para asegurarse que siguen operando.

4.8 PROTECCIÓN DE BASES DE DATOS

Con el fin de velar por la integridad, confidencialidad y disponibilidad de las bases de datos y archivos de datos utilizados para almacenar información y datos personales de EL CONTRATANTE, EL CONTRATISTA deberá:

a) almacenar la información sensible de EL CONTRATANTE como contraseñas, datos personales, información de infraestructura crítica, entre otros, en un formato cifrado de conformidad con las buenas prácticas, y acorde al estándar de criptografía aprobado por EL CONTRATANTE.

b) ubicar todos los servidores de bases de datos, servidores de archivos y repositorios que contengan información de EL CONTRATANTE en una nube de alta disponibilidad o en zonas físicamente restringidas, a donde tendrán acceso sólo aquellas personas autorizadas que estrictamente lo requieran para cumplir con sus funciones.

c) restringir todo el acceso a las bases de datos, archivos de datos e información y datos almacenados en éstos, basándose en el principio del “menor privilegio”.

d) proteger todos los accesos a las bases de datos y archivos de datos utilizando al menos la combinación de una identificación del usuario, contraseña y doble factor de autenticación.

e) cambiar todas las contraseñas que vienen por defecto del fabricante en las bases de datos, que son de conocimiento público, antes del inicio del procesamiento y cambiarlas posteriormente de forma periódica.

f) mantener activos los logs de auditoría sobre los acceso a las bases de y almacenarlos por un período mínimo de un (1) año.

g) mantener activos los logs de auditoría que permitan registrar toda la actividad de transacciones y almacenarlos durante un periodo de al menos tres (3) meses desde la fecha de ejecución cada transacción.

h) manejar copias de respaldo requeridas para mantener disponible la información de EL CONTRATANTE durante la ejecución del contrato, estás copias deberán permanecer bajo medidas apropiadas de seguridad física y lógica que garanticen su integridad, confidencialidad y disponibilidad, y deberán ser entregadas a EL CONTRATANTE al finalizar el contrato.

i) implementar mecanismos de análisis de la seguridad de las bases de datos para evaluar e informar periódicamente el estado de cada base de datos y verificar que las configuraciones, parámetros y opciones están conformes con las líneas base definidas para ese estas y detectar cambios no autorizados.

j) eliminar y destruir de una manera segura (borrado seguro certificado) todas las instancias de cualquier información o datos de EL CONTRATANTE y material impreso relacionado, para asegurar que las transacciones y demás datos no puedan ser recuperados por personas no autorizadas.

k) revisar por lo menos una vez al año todos los controles de seguridad de las bases de datos, para asegurarse que siguen operando.

l) Al inicio del contrato se elaborará un inventario de los datos que serán entregados por parte de EL CONTRATANTE a EL CONTRATISTA.

m) Toda información intercambiada entre las partes debe ser transmitida cifrada cumpliendo los protocolos que se definan para tal fin.

4.9 PROTECCIÓN DE LA RED

Con el fin mitigar los riesgos relacionados con intrusiones o uso indebido de la red de EL CONTRATANTE, EL CONTRATISTA deberá:

a) implementar un sistema de protección contra intrusiones (en la red y el host), de conformidad con las buenas prácticas, para que continuamente 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.

b) instalar firewall para redes basados en las buenas prácticas, entre los servidores y los gateways, a la red pública de modo que excluyan los protocolos de comunicación que no sean necesarios para procesar el tráfico de Internet.

c) habilitar los logs de auditoría que permitan registrar la actividad crítica de los firewalls, gateways y dispositivos de red, y almacenarlos por un período de al menos tres (3) meses.

d) proteger la información de EL CONTRATANTE contra la divulgación no autorizada durante su tránsito a través de redes públicas; y e) aplicar las técnicas criptográficas para la transmisión de información, bajo estándares acordes con buenas prácticas.

5. DIAGRAMA DE FLUJO

No Aplica

6. ANEXOS

No Aplica

7. GLOSARIO

Base de Datos: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012).

Ciberseguridad: práctica de proteger sistemas, redes y programas de ataques digitales. Por lo general, estos ciberataques apuntan a acceder, modificar o destruir la información confidencial; Extorsionar a los usuarios o los usuarios o interrumpir la continuidad del negocio.

Contratista: Persona natural o jurídica, consorcio, unión temporal, o cualquier modalidad asociativa permitida por la ley, que ha suscrito un Contrato con ODC para la prestación de servicios, construcción de obras o suministro de bienes, y en general para satisfacer las necesidades corporativas de ODC.

Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables (Ley 1581 de 2012).

Malware: tipo de software diseñado para obtener acceso no autorizado o causar daños en una computadora.

Software: Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora.

8. CONTROL DE ACTUALIZACIONES

VERSIÓN	DESCRIPCIÓN	FECHA
1	Elaboración del documento.	31/07/2023

Original firmado por:
CARLOS ALBERTO SIERRA
Especialista Digital
Oleoducto de Colombia S.A.
Elaboró

Original firmado por:
NICOLAS MANCINI
Presidente (e)
Oleoducto de Colombia S.A.
Revisó y Aprobó