NORMA DE CONTROL DE ACCESO TECNOLÓGICO

CONTENIDO

GASES DEL CARIBE, en su compromiso con la protección de la información que se gestiona en los Servicios que presta, considera de importancia vital establecer los parámetros que deben tenerse presentes a la hora de gestionar el control de acceso a los sistemas y servicios de información que soportan la operación de esta organización.

1. CONSIDERANDOS

a) Que el acceso a los activos de información propiedad de esta organización y/o bajo su custodia debe ser controlados con el fin de evitar el acceso no autorizado a estos, tal como se desprende de la lectura de la norma NTC/ISO 27001/27002, razón por la cual se adopta esta norma.
b) Que a partir de la clasificación de la información adoptada en esta organización los usuarios serán habilitados para acceder solo a los activos de información requeridos para el desempeño de sus funciones; por tanto, el criterio de acceso está fundamentado en el principio del menor privilegio o mínimo necesario como premisa general.
c) Que es imperativo realizar el registro y habilitación de los nuevos usuarios para que estos accedan a los sistemas y servicios de información dispuesto por esta organización, así mismo es necesario suspender y revocar las autorizaciones de acceso cuando un usuario se encuentre en período de vacaciones, licencias, suspensión o desvinculación definitiva. Deberá dejarse registro de los periodos de acceso de los funcionarios autorizados en su momento para fines de evidencia, conforme los criterios que adopte la organización.
d) Que una vez autorizado un usuario para acceder a los sistemas y servicios de información de esta organización este se hace responsable de toda transacción que realice en estos con su nombre de usuario, en virtud de que los sistemas de información disponen de mecanismos que permiten hacer trazabilidad a las acciones realizadas por este durante toda la sesión.
e) Que la asignación de ciertos derechos y/o privilegios de acceso a determinados funcionarios deberán otorgarse en situaciones de carácter excepcional y justificadas que exigen obtener la autorización previa antes de habilitar el acceso.
f) Que el acceso no autorizado o facilitar este a personas no autorizadas, funcionarios o no, constituye un incidente de seguridad, el cual además constituye una violación al régimen contractual que regula la relación entre el usuario autorizado y esta organización.
g) Que esta organización adoptará los controles necesarios para prevenir el acceso no autorizado a los sistemas y servicios de información dispuestos para que los usuarios desempeñen sus funciones.
h) Que esta organización de forma periódica revisará los derechos de acceso y/o privilegios concedidos a los usuarios para acceder a los activos de información dispuestos para que estos desempeñen sus funciones conforme los requerimientos de cada servicio de la organización.
i) Que existen disposiciones de carácter legal y penal que sancionan el acceso no autorizado a sistemas de información, a la información protegida por la propiedad intelectual y a información considerada confidencial como es la personal; situaciones que en caso de presentarse serán objeto de investigación y denuncia por parte de esta organización en cumplimiento de la obligación general que tiene todo ciudadano de poner el conocimiento de las autoridades la sospecha de comisión de una conducta que viole la ley penal.
j) Las áreas responsables coordinarán la habilitación de acceso a los sistemas y servicios de información. Que como fuente de consulta y apoyo para cumplir lo dispuesto en esta norma se tendrá presente las buenas prácticas en la materia.

2. OBJETIVO

Esta norma hace parte de la Política de Seguridad de la Información de GASES DEL CARIBE y regula lo relacionado con el control de acceso a los sistemas y servicios de información que soportan la operación de esta organización.

3. DESTINATARIOS

Son destinatarios de esta norma los colaboradores de todo nivel quienes respecto de los activos de información serán considerados custodios de estos en la medida que acceden y traten activos de información para el desempeño de las funciones contratadas.

Igual serán considerados custodios, aquellos terceros que, en condición de proveedores, accedan y traten activos de información en poder de esta organización; así como aquellos terceros que en virtud de una relación legal estatutaria y/o contractual deban tratar tales activos.

Los custodios tienen la responsabilidad de gestionar de forma segura los activos de información que traten de forma temporal o permanente en virtud de la relación legal y/o contractual existente.

4. SISTEMAS DE INFORMACIÓN

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 indirecta, para que los usuarios desempeñen sus funciones la cual está compuesta entre otras por el hardware, software, servicios de información y redes, nombres de usuario y contraseñas.

5. GESTIÓN DE ACCESO DE USUARIOS

El acceso de los usuarios a los sistemas y servicios de información dispuestos por esta organización siempre debe realizarse a partir del l rol o cargo asignado al usuario y de la contraseña secreta definida por el mismo. Esto, cumpliendo las directrices que esta norman establece.

5.1.CREACIÓN DE ROLES DE USUARIOS

La creación de roles para el acceso a los sistemas y servicios de información digital corresponde al Custodio del Sistema de Información (Dirección Digital, Coordinación SGI y/o Coordinación de Gestión Documental) de esta organización.

Los roles que se creen deben estar asociados necesariamente a los perfiles de acceso a los sistemas y servicios de información dispuestos por esta organización.

5.2.REGISTRO, SUSPENSIÓN Y REVOCACIÓN DE ACCESO A LOS USUARIOS

Todo usuario de los sistemas y servicios de información dispuesto por esta organización solo podrá acceder cuando se haya realizado el proceso de registro y aprobación, conforme el procedimiento que se ejecuta para la creación, administración y eliminación de usuarios adoptado por esta organización. El procedimiento contemplará también lo relativo a los pasos

a seguir para la suspensión temporal y revocación de los de los derechos de acceso, o cualquier otro ajuste que impacte los derechos de acceso.

5.3.ACCESO A LOS SISTEMAS Y SERVICIOS DE INFORMACIÓN

El acceso debe realizarse a través del nombre de usuario único aprobado por esta organización.

De manera excepcional y solo para los casos estrictamente necesarios se podrá acceder a los sistemas y servicios de información de esta organización con cuentas de usuario grupales. En estos casos se deberán adoptar los controles que permitan hacer trazabilidad y tener certeza de las personas que ingresan en un momento determinado y de las transacciones realizadas en los sistemas y servicios de información de esta organización.

El acceso a los sistemas y servicios de información de esta organización realizado por una persona diferente a la autorizada y/o abusando de las autorizaciones otorgadas constituye un incidente de seguridad que puede tener repercusiones jurídicas laborales, penales o civiles y por tanto una violación a la Política de Seguridad de Información.

De los usuarios a los cuales se pretende conceder el acceso a los sistemas de información por medio de la creación de credenciales se llevará un registro histórico por medio de la herramienta definida por la organización en el cual se registra a la fecha de creación, modificación y eliminación del mismo. Este registro se mantendrá por el período que considere necesario la organización y/o por las exigencias de ley, según el caso Este registro tendrá mínimamente la siguiente información: Nombre del usuario, correo asignado, fecha de asignación, modificación o eliminación, según el caso.

5.4.GESTIÓN DE DERECHOS Y/O PRIVILEGIOS

La asignación de derechos y/o privilegios para el acceso a los sistemas y servicios de información debe realizarse de manera restringida y/o temporal, según cada caso. Para la asignación de derechos y/o privilegios deberá seguirse diligenciarse el formato de solicitud de acceso y respectiva autorización dirigida por el superior del usuario.

Esta organización en sus sistemas de información dispondrá de un registro de los usuarios a quienes se les ha asignado un determinado privilegio de acceso; registro que deberá contener mínimamente la siguiente información: Fecha de la solicitud sea por medio electrónico o físico; nombre del usuario; colaborador de nivel jerárquico que autorizó el otorgamiento del privilegio; duración del privilegio; entre otras. Gases del Caribe podrá solicitar requisitos adicionales respecto de la solicitud realizada en virtud de la necesidad de seguridad. Los sistemas de información almacenarán las transacciones realizadas por el usuario beneficiario del privilegio.

5.5.GESTIÓN DE CONTRASEÑAS

Esta organización al asignar un nombre de usuario creará una contraseña temporal secreta la cual deberá ser cambiada por el usuario antes de acceder a los sistemas y servicios de información que le fueron habilitados para el desempeño de sus funciones. De este cambio y de los posteriores cambios en la contraseña secreta de cada usuario se conservará el registro correspondiente con el fin de establecer la responsabilidad de cualquier incidente de seguridad en que esté involucrado el nombre de usuario asignado a una persona.

Todo usuario asignado por esta organización deberá tener presente que el nombre de usuario y su contraseña son confidenciales, lo cual deberá constar en el contrato respectivo.

5.6. REVISIÓN DE LOS DERECHOS DE ACCESO

Los derechos de acceso a los sistemas y servicios de información de esta organización serán revisados bajo los siguientes parámetros:

La periodicidad de la revisión como regla general será cada seis (6) meses y de tres (3) meses para aquellos accesos privilegiados; lo anterior, sin perjuicio de revisiones que en caso de un incidente de seguridad o sospecha de este sean necesarias.

Cuando haya cambio en las funciones desempeñadas por un usuario resultado de un ascenso, cambio de funciones, suspensión o terminación de la relación laboral.

6. RESPONSABILIDAD DE LOS USUARIOS

Es obligación de los usuarios evitar el acceso no autorizado o realizar conductas que pongan en peligro la información tratada a través de los sistemas y servicios de información de esta organización.

El incumplimiento de los deberes de secreto y confidencialidad son conductas que pueden generar indemnización de perjuicios a favor de esta organización.

6.1. USO DE CLAVES SECRETAS

Todos los usuarios de los sistemas y servicios de información digital dispuestos por esta organización para que estos desempeñen sus funciones deben ser informados por el área de Dirección Digital al momento de recibir las cuentas a los sistemas de información. Estas responsabilidades son las siguientes:

- Mantener confidencial la contraseña secreta vinculada al nombre de usuario asignado.
- Mantener confidencial la contraseña secreta de carácter grupal que haya sido autorizada a un grupo determinado de usuario, cuando ello aplique.
- Abstenerse de permitir y/o facilitar a terceros el acceso a los sistemas y servicios de información de esta organización.
- Cooperar en las investigaciones de los incidentes de seguridad en los que pueda estar involucrado o no el nombre de usuario asignado.
- Informar cualquier sospecha de acceso no autorizado a los sistemas y servicios de información de esta organización, una vez tenga conocimiento de estos.
- Evitar accesos no autorizados a los sistemas y servicios de información.
- Abstenerse de escribir o mantener un registro en cualquier soporte de la clave secreta individual o grupal vinculada a un nombre de usuario individual o grupal.
- Cambiar la clave secreta cuando exista sospecha o indicio de un posible peligro; o cuando la organización lo exija, según sus necesidades.
- Escoger claves secretas de fácil recordación para el usuario, pero de difícil conocimiento para terceros; por tanto, deberán evitar claves que coincidan con el documento de identidad, teléfonos personales, fechas de nacimiento, nombre de los seres queridos, consecutivos numéricos, entre otros.

- Abstenerse de usar la misma contraseña asignada al nombre de usuario registrado en esta organización para acceso a sistemas y/o servicios de información de uso personal o doméstico.
- Abstenerse de intentar acceder a los sistemas y servicios de información en horarios no autorizados o durante períodos de vacaciones, suspensiones o después de terminada la relación contractual.

Durante el proceso de inducción del personal o al inicio de la relación contractual, el usuario deberá firmar el documento de Confidencialidad correspondiente en el cual se conserva evidencia escrita del entendimiento y aceptación de estas responsabilidades.

6.2. TRATAMIENTO DE CLAVES SECRETAS POR PARTE DEL PERSONAL DE SOPORTE

Deberá regularse la prohibición de solicitar información de los usuarios como contraseñas de acceso a los sistemas de información dispuestos por esta organización para soportar la operación de los diferentes servicios.

Así mismo, deberá asegurarse en los sistemas de información que las contraseñas de acceso estén protegidas con medidas de seguridad robustas con el fin de impedir el acceso de terceros no autorizados.

7. CONTROL DE ACCESO A LA RED

Para efectos de evitar el acceso no autorizado a la red, esta organización establece los siguientes parámetros para controlar el acceso a los sistemas y servicios de información dispuestos para soportar la operación de esta organización.

7.1. USO DE SERVICIOS DE LA RED

La red privada de esta organización solo está habilitada para los usuarios registrados en el directorio activo o identificados bajo un nombre de usuario autorizado y aprobado previamente. Por tanto, cualquier acceso que desconozca esta premisa será considerado un acceso abusivo a un sistema de información.

Las conexiones no autorizadas tienen el potencial de comprometer la seguridad de la información de esta organización, constituyéndose en un eventual incidente que será objeto de investigación y análisis para establecer si existió compromiso sobre algún activo de información, de cuyo análisis se establecerá igualmente las repercusiones jurídicas de tal acceso.

Toda autorización de acceso a los servicios de red deberá cumplir con el procedimiento definido por esta organización para tal fin.

7.2. AUTENTICACIÓN DE USUARIOS PARA LAS CONEXIONES EXTERNAS

El acceso de cualquier usuario de los sistemas y servicios de información de esta organización vía VPN necesariamente deberá agotar un proceso de identificación y autenticación con el fin de lograr el acceso. La autenticación deberá realizarse a través de métodos robustos como el

ID único de usuarios u otro mecanismo, según las necesidades de la organización o estado del arte.

Toda conexión remota vía VPN deberá cumplir con el procedimiento definido por esta organización.

La creación de accesos vía VPN deberá estar soportados por su respectiva solicitud y aprobadas por el Jefe de departamento o coordinador respectivo.

7.3. IDENTIFICACIÓN DEL EQUIPO EN LAS REDES

Esta organización definirá aquellos equipos cuya autenticación se realice exclusivamente desde estos y ubicaciones fijas y predeterminadas. Así mismo, siempre será necesaria además la identificación y autenticación del usuario.

Toda conexión exitosa debe indicar la red de esta organización a la cual se ha conectado el equipo. En caso de que el usuario observe que la conexión se ha realizado a una red de esta organización diferente a las conocidas o a una red desconocida de terceros inmediatamente deberá realizar la desconexión del equipo a tal red, y procederá a reportar esta situación por medio de la herramienta definida por esta organización.

7.4. PROTECCIÓN DEL PUERTO DE DIAGNÓSTICO Y CONFIGURACIÓN REMOTA

Se brinda el servicio soporte a los usuarios el cual eses prestado por los agentes de soporte correspondiente al sistema y en caso de considerar necesario el acceso remoto a los equipos asignados a los usuarios de esta organización, se toman las medidas necesarias para proteger la información almacenada en el equipo, sistemas y servicios de información dispuestos por esta organización.

7.5. SEGREGACIÓN EN REDES

Para efectos de proteger la información, los sistemas y los servicios de información dispuestos por esta organización es necesario que el acceso a estos activos y recursos se realice a través de redes separadas.

Las redes habilitadas en esta organización y que deben mantenerse separadas se categorizan de la siguiente forma:

- Red de zona exterior: Esta red estará habilitada solo para el acceso a la información contenida en los portales web de esta organización a la cual puede acceder cualquier persona desde el exterior.
- Redes de Servidores: Estas redes estarán habilitadas solo para el acceso a la información almacenada en servidores, servicios de información proveídos por terceros e información contenida en los sistemas que soportan la operación de los servicios de esta organización.
- Red de Funcionarios: Esta red estará habilitada solo para el acceso a la información de esta organización requerida por los colaboradores usuarios finales y terceros proveedores; todo acceso a este activo, a los sistemas y servicios de información deben disponer de forma obligatoria de un proceso de identificación y otro de autenticación por parte de los usuarios.

- Red de contratistas: Esta red estará habilitada solo para el acceso a la información por parte de aquellos usuarios especiales que esta organización defina, que requieren acceder a información crítica y restringida a los demás usuarios finales.
- Red de visitantes: Esta red estará habilitada solo para proveer servicios de navegación en Internet a visitantes, previo el acceso de estos, deberá hacerse un registro e identificación del visitante en el cual indicará su nombre y correo electrónico a través de un portal cautivo.

Los criterios de clasificación de la información constituyen un insumo para el acceso y procesamiento de la información a través de las redes aquí categorizadas.

Por tanto, en todo proyecto de implementación tecnológica debe garantizarse que, previa la entrada en producción de cualquier sistema o servicio de información en esta organización, el acceso se realice exclusivamente a través de redes definidas atendiendo la categorización antes indicada. área responsable de la seguridad de la información.

7.6.CONTROL DE CONEXIÓN A LA RED

Esta organización, de acuerdo con los derechos particulares de acceso otorgados a cada usuario de esta organización, controlará el acceso de estos a las redes, para ello adoptará y aplicará los controles informáticos correspondientes, según las necesidades del negocio y las funciones de cada usuario.

En este sentido, esta organización podrá restringir la capacidad de conexión aplicando controles, que permitan limitar de forma permanente o temporal a cualquier dispositivo que no cumpla con las políticas de seguridad.

7.7.CONTROL DE ACCESO AL SISTEMA OPERATIVO

El acceso a los sistemas operativos existentes en esta organización debe basarse en las siguientes premisas que garanticen un registro seguro:

- El registro debe estar diseñado de manera que se mitigue al máximo la posibilidad de accesos no autorizados.
- Debe evitarse durante el proceso de registro revelar información sobre el sistema operativo o aplicativo que pueda ser usada por terceros o que constituya información que ayude o facilite accesos no autorizados.

7.8.IDENTIFICACIÓN Y AUTENTICACIÓN DEL USUARIO

En esta organización todos los usuarios sin excepción de los sistemas y servicios de información se identificarán con un nombre de usuario y contraseña personal, secreta, confidencial e intransferible, salvo aquellos casos autorizados para nombres de usuarios grupales.

Todo sistema o servicio de información debe disponer de mecanismos de identificación y autenticación que dejen trazabilidad según las buenas prácticas aceptadas; s trazas, huellas o logs.

Los tiempos de conservación de los logs, trazas o huellas, serán definidos de acuerdo con las necesidades de negocio y a los requerimientos normativos que existan para tal fin.

Esta organización, según las necesidades y requerimientos del negocio, podrá optar por mecanismos que complementen el uso del nombre de usuario y su contraseña o que la sustituyan por mecanismos más robustos que otorguen seguridad para el acceso a los sistemas y servicios de información existentes.

7.9. CONTROL DE ACCESO A SISTEMAS Y APLICACIONES

El acceso a los sistemas y servicios de información estará determinado por los derechos otorgados para tal fin considerando la segregación de funciones que debe caracterizar el rol de cada usuario autorizado.

Todo acceso a la información limitado a la segregación de funciones de cada rol de usuario autorizado requiere de la aprobación previa por parte del área encargada por medio de la herramienta definida para otorgar tal privilegio.

Los sistemas y servicios de información dispuestos por esta organización para soportar la operación deberán cumplir, además de los indicados en esta norma, con los siguientes parámetros para controlar el acceso:

- Atender las definiciones de confidencialidad que realice el Servicio de esta organización responsable del sistema de información.
- Adoptar controles que garanticen la confidencialidad de la información cuando el sistema o servicio de información opere en un ambiente compartido en el cual comparta recursos, considerando los riesgos identificados.
- Según la criticidad de la información de esta organización contenida en un sistema o servicios de información garantizar que esta sea tratada atendiendo la categorización de las redes aquí definidas.

7.10. CONTROL DE ACCESO A CÓDIGOS FUENTES:

Los códigos fuentes del software propiedad de esta organización o entregados para su custodia deberán mantenerse en un ambiente seguro protegido contra accesos no autorizados.

Solo los usuarios autorizados podrán acceder a los códigos fuentes del software mencionado, debiendo para ello adoptarse controles que permitan hacer trazabilidad a cualquier acceso a estos.

8. FACULTAD DE MONITOREO

Gases del Caribe comunica a los usuarios de los sistemas y servicios de información dispuestos por esta organización para el desempeño de las funciones de estos, originadas en una relación contractual, legal o reglamentaria, que tiene la facultad de monitorear el cumplimiento de los controles derivados de esta norma, en su condición de garante de la gestión segura de la información propiedad de esta organización o entregada para su custodia

9. CULTURA DE SEGURIDAD

Es fundamental para esta organización el rol proactivo que desempeñe el Área de Auditoria con el fin de fortalecer la cultura de seguridad en los Servicios que soportan la operación de esta organización.

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

Este documento es de uso exclusivo de Gases del Caribe S.A. E.S.P. y se prohíbe su uso a terceros no autorizados.

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