Grupo Corporativo Sightlog
Diagonal 47 # 77B- 09 Int. 5
Bogotá – Colombia
P: (+57- 1) - 746 6775

Bogotá D.C. 15 de Febrero de 2023

PO.IT.01 POLÍTICA DE CONFIDENCIALIDAD DE LA INFORMACIÓN (V.5)

1. PROPÓSITO

El propósito de este documento es definir la política de confidencialidad de la información respecto al uso responsable de la tecnología, documentos, datos, especificaciones, métodos, procesos y en general información relacionada con el objeto social, y los servicios que ofrecen las empresas del Grupo Sightlog, la cual es considerada como **INFORMACIÓN CONFIDENCIAL**.

Se entiende por uso responsable el seguimiento de normas, políticas y buenas prácticas que salvaguarden la seguridad del Know How, datos, sistemas de información y el buen uso de los recursos tecnológicos Institucionales.

Con el presente documento se establecen los controles para:

- Definir los responsables del manejo de la información.
- La creación, administración y asignación de roles.
- La administración de cuentas de acceso a los sistemas de información y correo electrónico.
- Política creación de contraseñas.
- Política para la entrega o divulgación de información física o digital a Clientes, proveedores y entes de certificación.
- Política para la entrega o divulgación de información física o digital a colaboradores.

2. ALCANCE

Esta política aplica para todos los colaboradores de las empresas Intra Mar Shipping S.A.S, Agencia de Aduanas Andinos S.A.S. Nivel 1, Intramar Cargo S.A.S., Intrahealthcare S.A.S., Intrarelo S.A.S e Intrastorage S.A.S cualquiera sea su jerarquía, y en general a cualquier Cliente, proveedor y ente de certificación que tenga o solicite acceso a la información y a los sistemas de informáticos, entendiéndose por sistema de información el compendio de software, hardware y datos de la organización.

Grupo Corporativo Sightlog
Diagonal 47 # 77B- 09 Int. 5
Bogotá – Colombia
P: (+57- 1) - 746 6775

3. RESPONSABLES DEL MANEJO DE LA INFORMACIÓN

Cada colaborador es responsable de almacenar la información generada por la labor que desempeña en https://intramarshipping.sharepoint.com o https://andinossas.sharepoint.com/ plataformas asignadas para el manejo de información general de la organización. Al respecto, los documentos que sean de uso compartido de cada Unidad se deben almacenar en el SharePoint/control individual. Los documentos corporativos, pero de uso personal de cada colaborador (listas de tareas, planes de trabajo, notas rápidas entre otros) se deben guardar en One Drive/Documentos.

Cada cuenta de usuario está configurada para almacenar los datos generados por los aplicativos organizacionales; toda información guardada en otras ubicaciones del equipo no tendrá respaldo.

El proceso de tecnología es el responsable de cumplir y hacer cumplir las políticas y procedimientos establecidos por la organización en el presente documento; así como garantizar que la información este salvaguardada y disponible a través de sistemas de Backup licenciados y seguros.

Cada colaborador es responsable de salvaguardar la confidencialidad de la información que maneja, hacer uso adecuado de sus contraseñas y reportar cualquier correo sospechoso.

4. CREACIÓN, ADMINISTRACIÓN Y ASIGNACIÓN DE ROLES

De acuerdo con los niveles de cargo establecidos en la estructura organizacional se determinan los roles para el acceso a los sistemas de información en cada perfil de cargo. Teniendo en cuenta esta determinación el responsable de tecnología parametriza las herramientas digitales aplicables con el fin de otorgar los permisos y restricciones a cada usuario.

5. ADMINISTRACIÓN DE CUENTAS DE ACCESO A LOS SISTEMAS DE INFORMACIÓN Y CORREO ELECTRÓNICO

5.1. Condiciones generales

- La contraseña es un código único, personal e intransferible, que no debe ser divulgado o compartido con terceras personas, el no observar esta buena práctica constituye una violación a las políticas de seguridad de la empresa y conlleva a sanciones disciplinarias.

- Cada colaborador del grupo corporativo tiene un computador asignado por lo que está prohibido el compartir equipos y por ende contraseñas de acceso, el realizar esta práctica conlleva a sanciones disciplinarias.

Grupo Corporativo Sightlog
Diagonal 47 # 77B- 09 Int. 5
Bogotá – Colombia
P: (+57- 1) - 746 6775

- Un usuario registrado y autorizado en la empresa, se debe autenticar siempre con su contraseña personal para acceder a los sistemas de Información y a los servicios de la plataforma tecnológica.

- Toda cuenta de usuario de la plataforma tecnológica debe identificar una persona en la vida real, colaborador del grupo, no se permite el uso de cuentas genéricas o anónimas, a excepción de la cuentas de uso compartido, creadas para el manejo de procesos críticos p.ej: soporte.tecnico@intramar.com.co; solicitudes.administrativas@intramar.com.co, entre otras, las cuales serán creadas únicamente por solicitud del director de cada Unidad o Alta Gerencia previa evaluación de su pertinencia para la organización.

- En caso de requerirse el acceso a la cuenta de un colaborador que se encuentre fuera de las instalaciones de la empresa (por motivo de incapacidades médicas, vacaciones, calamidad, permisos en general u otros) únicamente el director de unidad o líder de proceso realizará la solicitud escrita al correo soporte.tecnico@intramar.com.co y autorizará para asignar una contraseña temporal con una duración específica, luego la cuenta será desactivada; el solicitante será responsable de lo que suceda con la información y la seguridad de esta por la duración del evento. Una vez el colaborador retorne a las oficinas deberá ser informado del cambio de contraseña y solicitará la activación de su cuenta actualizando su contraseña y manteniendo la confidencialidad de esta.

- El usuario es el responsable de garantizar la seguridad de la información a su cargo, la cual está disponible en medios electrónicos, utilizando para ello en todo momento las mejores prácticas de manejo documental, contraseñas seguras y dándole a esta el uso adecuado.

- Las contraseñas tendrán un periodo de vigencia de CUARENTA Y CINCO (45) días, fecha en la cual se obligará a cambiarse de acuerdo con las mejores prácticas y políticas de seguridad, de lo contrario se desactiva la cuenta.

- Es importante precisar que el usuario y la contraseña, es el mecanismo de identificación de un usuario ante la Empresa para el uso de los recursos tecnológicos y de información, esta identificación, permite manejar los perfiles y permisos de los usuarios, hacer el seguimiento y trazabilidad en caso de problemas de acceso y seguridad.

- Únicamente las contraseñas de administración de la plataforma tecnológica deberán ser escritas, protegidas en un sobre debidamente sellado y almacenadas en un lugar seguro, con los datos del remitente, la fecha y el sistema, para ser utilizados en caso de una contingencia o de ausencia del líder del proceso.

- Está prohibido compartir información confidencial con personas o entidades externas a la organización.

- Las comunicaciones entre colaboradores del grupo se deben realizar a través de Teams, salvo aquellas personas que por la naturaleza de su cargo en el momento no tienen cuenta asignada.

- Está prohibido abrir mensajes de remitentes desconocidos, así como revelar contraseñas. Cualquier mensaje sospechoso debe reportarse inmediatamente a soporte.tecnico@intramar.com.co.

- Las claves iniciales de ERP SIGMA son controladas por el Strategic Controller y actualizadas por el usuario de manera programada por el sistema.

- Los sistemas de información y cuentas de sistema operativo solicitarán automáticamente el cambio de las contraseñas cada 90 días, las del ERP solicitará cambio cada 72 días.

- Cuando ingresa un nuevo usuario se le asigna una clave genérica para su equipo y debe cambiarse el mismo día del ingreso. Las claves de correo electrónico corporativo son asignadas por el área de tecnología y configuradas directamente en los aplicativos que se requieran.

- El no cumplimiento de cualquiera de los puntos expuestos en esta política conlleva a sanciones disciplinarias.

6. POLÍTICA CREACIÓN DE CONTRASEÑAS

6.1 Contraseña Segura o fuerte:

Una contraseña segura, es un código especial para proteger sus recursos informáticos, debe contener letras mayúsculas, minúsculas, números y caracteres especiales sin espacios con finalidad de disminuir la posibilidad de acceso no autorizado o que sea utilizada por un tercero, para suplantación de identidad ante la organización ocasionando fraude o falsificación.

Para esto se deben tener en cuenta ciertas recomendaciones al momento de su creación, como por ejemplo no utilizar datos personales, tales como nombres, números de identificación, fechas que puedan ser utilizados por terceros para adivinar nuestra contraseña.

Reglas para crear contraseñas fuertes, y así evitar el uso de su identidad por parte de personal no autorizado (suplantación):

Grupo Corporativo Sightlog
Diagonal 47 # 77B- 09 Int. 5
Bogotá – Colombia
P: (+57- 1) - 746 6775

- Elija contraseñas largas, de por lo menos 7 caracteres de longitud, o más.
- Utilice dos números en los primeros siete caracteres.
- Dentro de su contraseña no utilice un nombre, una cadena de números, ni ninguna palabra común que aparezca en un diccionario.
- Utilizar mayúsculas y minúsculas intercaladas dentro de los 7 caracteres.
- Algunos caracteres especiales pueden ser utilizados; sin embargo, tenga en cuenta que algunas aplicaciones no pueden aceptar caracteres especiales.
- Uno de los métodos de generación de contraseñas más fáciles de recordar y más difíciles de violar es el de contraseña pseudo-aleatoria. En este caso, la contraseña se genera a partir de una frase fácil de recordar que es importante para el usuario. Esta puede ser una frase de un libro que le gusta en especial, las palabras de una canción que siempre recuerde con facilidad, una frase que usted nunca olvidará.

6.2 Evitar contraseñas débiles:

Al crear contraseñas, evitar el texto siguiente:

- Contraseñas fáciles de adivinar, como contraseñas en blanco o palabras como “contraseña”, “amor”, “súper”, etc.
- Su nombre, nombre del cónyuge o de su hijo.
- El nombre de su mascota.
- Nombres de amigos cercanos o compañeros de trabajo.
- Nombres de sus personajes favoritos de fantasía.
- El nombre de su jefe.
- El nombre, en general, de alguien.
- Cadenas de números o letras, al igual que 1234, abcde.
- El nombre de su equipo.
- Su número de teléfono o su número de placa.
- Cualquier parte de sus documentos de identificación.
- Una fecha de nacimiento.
- Otra información suya que sea fácil de obtener (por ejemplo, dirección, ciudad, oficina).
- Una palabra en un diccionario de cualquier idioma.
- Nombres de lugares o nombres propios.
- Las contraseñas con una sola letra repetida como ’aaaa’.
- Patrones simples de letras en el teclado, como asdf.
- Cualquiera de las anteriores seguida o precedida de un solo dígito (número).

6.3 Caracteres especiales no permitidos

Caracteres excluidos de la lista de caracteres especiales por ser incompatibles con algunos sistemas:

- Espacio
- "Comilla Doble"
- 'Comilla simple'
- `Backtick`
- & Ampersand: &
- Paréntesis (izquierdo o derecho ( )
- | Barra |
- < Inferior a <
- Superior a >

6.4 Garantizar la confidencialidad de la información

Con el fin de garantizar la confidencialidad de la información, la organización establece un acuerdo de confidencialidad y acuerdo de seguridad bilateral; los cuales son firmados por el colaborador en el mismo momento de recibir la respectiva inducción de calidad y seguridad. El incumplir estos acuerdos conlleva a sanciones disciplinarias.

7. POLÍTICA PARA LA ENTREGA O DIVULGACIÓN DE INFORMACIÓN FÍSICA O DIGITAL A CLIENTES, PROVEEDORES Y ENTES DE CERTIFICACIÓN

- No está permitido divulgar, revelar, comunicar, transmitir, grabar, duplicar, copiar o de cualquier otra forma reproducir a clientes, proveedores o entes de certificación la información y documentación a la que tenga acceso en virtud de que la misma constituye un secreto corporativo en términos del artículo 43, numeral 2 del reglamento interno de trabajo y según lo establecido en el FR.DH.05 Acuerdo de confidencialidad; dicha información solo se podrá divulgar, revelar, comunicar, transmitir, grabar, duplicar, copiar o de cualquier otra forma reproducir con la autorización expresa y por escrito del PRESIDENTE, GERENTE, CONTROLLER ESTRATEGICO y/o DIRECTOR DE CALIDAD Y SEGURIDAD.
- Para el caso de auditorías de clientes, proveedores y entes de certificación la unidad de calidad y seguridad es la única responsable para facilitar la consulta de la información solicitada previo a la firma del documento FR.QS.10 Compromiso de confidencialidad del auditor.

Grupo Corporativo Sightlog
Diagonal 47 # 77B- 09 Int. 5
Bogotá – Colombia
P: (+57- 1) - 746 6775

- La información considerada para consulta pública no necesita previa autorización y se encuentra disponible en la RED IAG en documentos de consulta/Información pública a terceros.

8. POLÍTICA PARA LA ENTREGA O DIVULGACIÓN DE INFORMACIÓN FÍSICA O DIGITAL A COLABORADORES

- La divulgación, comunicación, transmisión, grabación, duplica, copia o cualquier otra forma reproducción al interior de la organización se establece en el documento PR.QS.04 Elaboración y control de documentos; el cual es entregado a todos los colaboradores a través de inducción, reinducción y capacitaciones. Este se encuentra disponible en la RED IAG en procedimientos de del proceso Calidad y Seguridad.

ORIGINAL FIRMADO

Nicolás Gärtner Cala
CC. 1.019.039.878
Sightog Group CEO

Grupo Corporativo Sightlog
Diagonal 47 # 77B- 09 Int. 5
Bogotá – Colombia
P: (+57- 1) - 746 6775

Control de cambios.

Versión revisada	Descripción de la modificación o anulación *(incluya la fuente que origina el cambio)*	Versión vigente	Fecha de aprobación.	Fecha de vigencia.
-	Establecimiento de la política de confidencialidad.	1	04/06/2021	04/06/2022
1	Se incluye el numeral 5.2 “Política creación de contraseñas”.	2	19/07/2021	19/07/2022
2	Se reestructura la Política sepárandola en “Política de confidencialidad” y “Política de uso de recursos informáticos”.	3	17/08/2021	17/08/2022
3	Es modificado el titulo del documento. Se amplia el propósito y el alcance. Se organizan los numerales 5 y 6 para mejor entendimiento del documento. Se inlcuye la Política para la entrega o divulgación de información fisica o digital a Clientes, proveedores y entes de certificación. Y la Política para la entrega o divulgación de información fisica o digital a colaboradores.	4	05/01/2022	05/01/2023
4	Se actualzan los sigueintes puntos de la Política: 1 Proposito, 2 Alcance, 3 Responsables del manejo de la informacion y 5.1 Condiciones generales, se asigna codigo a la política para ser formalizada en el sistema de gestion de la calidad de la organización.	5	15/02/2023	15/02/2025

Control de revisión y aprobación.

Revisó / Aprobó	Cargo	Firma	# de páginas revisadas / aprobadas	Fecha de firma
Elaboró	Director Administrativo	ORIGINAL FIRMADO Diana Sandoval	8 de 8	1/02/2023
Revisó	Strategic Controller	ORIGINAL FIRMADO Lina Sáenz	8 de 8	13/02/2023
Aprobó	Sightog Group CEO	ORIGINAL FIRMADO Nicolás Gärtner	8 de 8	15/02/2023