POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

REVISIÓN 02

WWW.DMSLOG.COM

ÍNDICE

1. CONTEXTUALIZACIÓN

DMS LOGISTICS es una empresa proveedora de los procesos más modernos en el segmento de la logística global, posibilitados gracias a la mejora continua de sus servicios tecnológicos con filiales y socios distribuidos en los cinco continentes del mundo.

La política de seguridad de la información tiene como objetivo reducir este riesgo protegiendo a DMS LOGISTICS de amenazas y vulnerabilidades, y del impacto en sus activos, que pueden comprometer la confidencialidad, integridad y disponibilidad de la información.

2. OBJETIVO

DMS LOGISTICS tiene como objetivo establecer directrices y responsabilidades para la gestión de la seguridad de la información y promover la mejora continua de los procedimientos relacionados con la seguridad de los datos y la información, para prevenir, detectar y reducir las vulnerabilidades ante incidentes relacionados con entornos web y *clouds*. De este modo, garantizar la disponibilidad, integridad, confidencialidad, legalidad, autenticidad y auditabilidad de la información necesaria para la realización de los intereses de DMS LOGISTICS y sus partes interesadas.

A discreción exclusiva de DMS LOGISTICS, esta política de seguridad de la información y cibernética podrá ser evaluada y revisada regularmente o en el caso de circunstancias y eventos que justifiquen o requieran dicha evaluación y revisión, con el fin de garantizar su actualización permanente, adecuación, eficacia y protección de los activos de DMS LOGISTICS.

3. Áreas de relación (DESTINATARIOS)

La Política de seguridad de la información, en DMS LOGISTICS, se aplica a todos los socios, administradores, directores, gerentes, agentes, empleados, prestadores de servicios y otros terceros usuarios autorizados por DMS LOGISTICS, que puedan tener acceso y utilizar, en cualquier capacidad y naturaleza, en el ejercicio de sus actividades, datos, información, recursos, herramientas, sistemas, aplicaciones o servicios de propiedad o controlados por DMS LOGISTICS, incluido el trabajo realizado externamente que utiliza el entorno de procesamiento de la Organización o el acceso a información perteneciente a DMS LOGISTICS.

La divulgación de la política a las partes interesadas de DMS LOGISTICS se realiza a través del sitio web de DMS, capacitaciones de incorporación, reciclaje y correos electrónicos al menos una vez al año.

Esta política también se aplica a los empleados en el trabajo a distancia, incluido el teletrabajo y *home office*. DMS LOGISTICS puede establecer, a su entera discreción, políticas, procesos y directrices de seguridad de la información específicas para estos casos.

4. DOCUMENTOS DE REFERENCIA

- Ley n.° 9.279/1996 - Regula los derechos y obligaciones relativos a la propiedad industrial
- Ley 13.709/2018 - Ley general de protección de datos personales (LGPD)

- Ley 13.853/2019 - Modifica la ley general de protección de datos personales, publicada en 2018
- NBR ISO/IEC 27001:2013 – Seguridad de la información
- NBR ISO 9001:2015 – Seguridad de la información

5. AUTORIDAD Y RESPONSABILIDADES

- Directores: es responsabilidad de los Directores de DMS analizar, revisar y aprobar esta Política siempre que sea necesario. Esta política entra en vigor en la fecha de su aprobación por parte de la Junta directiva y deroga cualquier documento que indique lo contrario.
- Responsable de TI e infraestructura: cumplir con los lineamientos establecidos en esta Política, mantenerla actualizada periódicamente con el fin de asegurar que cualquier cambio en la dirección de DMS LOGISTICS se incorpore y aclarar dudas sobre su contenido y su aplicación.
- Gerentes: es responsabilidad del gerente de cada área establecer criterios respecto al nivel de confidencialidad de la información (informes y/o medios) generadas por su área. La información debe clasificarse como: pública, interna, confidencial o restringida.
- Empleados: respetar y garantizar el cumplimiento de esta Política y, cuando sea necesario, consultar con el Responsable de TI e Infraestructura sobre situaciones que impliquen conflicto con esta Política o a través de la ocurrencia de situaciones descritas en la misma. Es esencial que cada persona comprenda el papel de la seguridad de la información en sus actividades diarias y participe en programas de sensibilización.

A su entera discreción, los Directores de DMS LOGISTICS pueden implementar un comité para la evaluación, revisión, implementación y supervisión de esta Política y sus términos y condiciones.

En caso de duda o pregunta sobre las disposiciones de esta política, el empleado debe ponerse en contacto con el Responsable de TI e Infraestructura por los siguientes medios: [__]

DMS LOGISTICS promoverá, desarrollará, actualizará e implementará, de manera regular y continua, las demás políticas, procesos y prácticas necesarios para habilitar y consumar esta política de seguridad de información y cibernética, incluyendo, entre otros: (i) política de continuidad de las operaciones, destinada a garantizar las actividades comerciales críticas y esenciales de DMS LOGISTICS; (ii) política de gestión y recuperación de desastres; (iii) política de evaluación de riesgos de proveedores; (iv) y otras políticas relacionadas que sean necesarias o convenientes, a criterio de DMS LOGISTICS.

6. PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

- Confidencialidad: garantizar que la información solo sea accesible a personas autorizadas;
- Integridad: garantizar que la información, almacenada o en tránsito, no sufra ninguna modificación no autorizada, ya sea intencional o no;
- Disponibilidad: garantizar que la información esté disponible siempre que sea necesario.
- Cumplimiento: garantizar el cumplimiento de los requisitos, que pueden ser obligaciones legales y/o contractuales con las partes interesadas y con aspectos legales y reglamentarios.

- Capacitación: fomentar la realización de capacitaciones en el ámbito de la seguridad de la información.

7. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

DMS LOGISTICS tiene como política ofrecer a nuestros clientes soluciones logísticas de alto rendimiento basadas en la creatividad y la optimización constante de las operaciones, el sistema de gestión de calidad, la seguridad de la información y la seguridad, promoviendo la mejora continua de los procedimientos relacionados con la seguridad de los datos y la información, para prevenir, detectar y reducir las vulnerabilidades ante incidentes relacionados con entornos web y *cloud*. De este modo, garantizar la disponibilidad, integridad, confidencialidad, legalidad, autenticidad y auditabilidad de la información necesaria para la realización de los intereses de DMS LOGISTICS y sus partes interesadas.

DMS LOGISTICS se compromete a:

1. Prestar servicios de agencia de cargas aéreas y marítimas de importación y exportación.
2. Proteger sus activos de información para reducir la vulnerabilidad y los incidentes.
3. Garantizar la disponibilidad, integridad, confidencialidad, legalidad, autenticidad y auditabilidad de la información necesaria para la realización de los intereses de DMS LOGISTICS y sus partes interesadas.
4. Evaluar los riesgos del negocio para garantizar la satisfacción del cliente, los requisitos aplicables y la viabilidad financiera;
5. Alinear la gestión de la seguridad de la información con nuestro negocio.
6. Llevar a cabo la capacitación de la información a lo largo de su ciclo de vida de manera ética y responsable.
7. Garantizar la confidencialidad, integridad y disponibilidad de la información a lo largo de su ciclo de vida: producción, manipulación, reproducción, transporte, transmisión, almacenamiento y eliminación.
8. Identificar, analizar, evaluar y tratar los riesgos que involucran activos de información, a través de evaluaciones periódicas, a intervalos regulares.
9. Adoptar mecanismos de protección contra el uso indebido, fraudes, daños, pérdidas, errores, sabotajes, robo y ataques, a lo largo del ciclo de vida de la información.
10. Supervisar, de forma continua, los activos de información y utilizar procesos, controles y tecnologías para prevenir y responder a los ataques.
11. Difundir la cultura de seguridad de la información a través de un programa permanente de sensibilización, concientización y capacitación.
12. Preservar los requisitos de seguridad de la información en la contratación de servicios o personas y en la relación con empleados, proveedores, terceros, socios, contratados y pasantes.
13. Conceder a los empleados y a terceros solo el acceso a la información necesaria para el desempeño de sus funciones y asignaciones previstas en contrato o por determinación legal.
14. Identificar, a través del control de acceso, a cada usuario de forma individual y en casos debidamente comprobados de tratamiento indebido de la información corporativa que lo responsabilizamos, junto con el administrador que le concedió el acceso.
15. Analizar las ocurrencias de tratamiento inadecuado de la información corporativa bajo los aspectos legales y disciplinarios, atribuyendo responsabilidad, y bajo el aspecto técnico, corrigiendo vulnerabilidades.

16. Satisfacer plenamente las necesidades de nuestros clientes y aumentar constantemente su satisfacción, por lo que damos gran importancia a la promoción de la conciencia de calidad entre nuestros empleados.
17. Invertir en formación y capacitación de nuestro mayor capital, nuestros empleados, para que todos se integren en el sistema de gestión de calidad y seguridad de la información.
18. Trabajar en la mejora continua de procesos y sistemas de calidad y seguridad de la información.
19. Garantizar un equipo dedicado y cualificado con orientación empresarial e innovadora. Los ejecutivos lideran con el ejemplo y crean el entorno interno para alcanzar los objetivos de calidad.
20. Asegurar que las relaciones con nuestros proveedores sean de beneficio mutuo. Esto requiere una comunicación transparente, un acuerdo sobre objetivos comunes en relación con los requisitos de los clientes y la cooperación para mejorar los procesos conjuntos.
21. Promover actividades y recursos asociados para lograr resultados en todo el sistema y en todos los niveles de la jerarquía.

La contratación, el mantenimiento y la implementación de sistemas, aplicaciones, programas y otros recursos y herramientas de información de DMS LOGISTICS siempre deben tener en cuenta los riesgos de seguridad existentes y las respectivas medidas, controles y mecanismos de mitigación. DMS LOGISTICS realizará evaluaciones regulares y continuas, incluso a través de terceros, sobre las medidas, controles y mecanismos de seguridad de sus sistemas, aplicaciones, programas y otros recursos y herramientas de información, incluidos análisis de impacto de riesgos.

8. OBLIGACIONES GENERALES

Todos los empleados de DMS LOGISTICS deben considerar la información como un activo de la organización, uno de los recursos críticos para la realización del negocio, que tiene un gran valor para DMS LOGISTICS y siempre debe ser tratado profesionalmente.

Los empleados deben respetar y cumplir, en todo momento, con lo dispuesto en esta política de seguridad y cibernética, bajo pena de sanciones y medidas legales y contractuales aplicables. DMS LOGISTICS monitorea y supervisa, por cuenta propia o a través del uso de terceros, el cumplimiento y conformidad de sus empleados con las disposiciones de esta política de seguridad y cibernética.

Todos y cada uno de los usuarios de los recursos informáticos de la compañía son responsables de proteger la seguridad e integridad de la información y el equipo informático. La violación de esta política de seguridad es cualquier acto que:

- Exponga a DMS LOGISTICS a pérdidas monetarias reales o potenciales al comprometer la seguridad de los datos, la información o la pérdida de equipos;
- Implique la divulgación de datos confidenciales, derechos de autor, negociaciones, patentes o uso no autorizado de datos corporativos;
- Implique el uso de datos para fines ilícitos, lo que puede incluir la violación de cualquier ley, reglamento o cualquier otro dispositivo gubernamental.

No está permitido retirar ningún aparato, equipo o información de las instalaciones de DMS LOGISTICS sin el permiso expreso por escrito del equipo de seguridad.

Para la ejecución de actividades y servicios, DMS LOGISTICS puede poner a disposición de sus empleados, a su entera discreción, ciertos dispositivos, equipos y recursos, a título de comodato. Los aparatos, equipos y recursos asignados permanecerán, en todo momento, bajo la propiedad de DMS LOGISTICS, y el empleado solo tendrá posesión precaria sobre ellos. En ningún momento se transferirá la propiedad de estos activos cedidos a los empleados. Los empleados deben garantizar, en todo momento, la correcta manipulación y mantener los bienes cedidos en un estado de conservación adecuado y normal, teniendo en cuenta el desgaste natural resultante del uso normal y adecuado de los mismos. Está prohibido el uso de los bienes cedidos para fines distintos de aquellos para los que están destinados. Los bienes cedidos deben mantenerse en un lugar adecuado, apropiado y seguro, de conformidad con las recomendaciones y directrices de DMS LOGISTICS. Siempre que lo solicite DMS LOGISTICS, los empleados devolverán los dispositivos, equipos y recursos que hayan sido cedidos por DMS LOGISTICS para la ejecución de las actividades. Los empleados que, en el ejercicio de sus actividades, tengan en su posesión y utilicen activos de DMS, deben devolverlos y dejar de utilizar las herramientas, recursos y servicios puestos a disposición por DMS, después de la terminación del contrato de trabajo, la prestación de servicios o la base legal aplicable.

Los terceros que tengan acceso a los sistemas de información de DMS LOGISTICS, ya sean proveedores, clientes u otros, deben tener acceso a las normas de seguridad de la información aplicables, y aceptar sus términos y condiciones, para asegurar y garantizar la seguridad de la información de DMS LOGISTICS, antes de que se conceda el acceso, incluidas las normas de confidencialidad.

Estos proveedores siempre adoptarán las mejores prácticas del mercado para la seguridad de la información y serán supervisados regularmente para garantizar el cumplimiento de los requisitos de seguridad de la información aplicables. Los contratos incluirán disposiciones adecuadas para garantizar la seguridad de la información y los sistemas de DMS LOGISTICS.

Los empleados deben recibir formación y capacitación, de forma regular, en materia de seguridad de la información, en relación con la naturaleza y el tipo de amenazas, medidas de seguridad existentes y la necesidad de comunicar sospechas e indicios de problemas. DMS LOGISTICS se compromete a proporcionar formación y capacitación obligatorias a todos los empleados para garantizar la seguridad de la información.

La eliminación definitiva y permanente de medios, *softwares*, sistemas y otros dispositivos y equipos de DMS LOGISTICS irá precedida de la eliminación y destrucción de todos los datos e información contenidos en dichos activos. El mismo procedimiento se aplicará en caso de defecto o fallo de estos activos.

9. PROPIEDAD INTELECTUAL

Es propiedad de DMS LOGISTICS, todos los materiales, obras, diseños, procesos, diagramas de flujo, investigaciones, análisis, creaciones o procedimientos desarrollados por cualquier empleado en el ejercicio de sus actividades para DMS LOGISTICS, sin perjuicio de la aplicabilidad de las disposiciones de la legislación brasileña.

10. POLÍTICA de uso

- No introduzca sus contraseñas o usuarios en máquinas de terceros, especialmente fuera de la empresa.
- Solo acepte la ayuda técnica de un miembro de nuestro equipo técnico previamente presentado e identificado.

- Informe al equipo de seguridad de pedidos externos o internos que no estén de acuerdo con temas anteriores.

11. DATOS DE EMPLEADOS. Dispositivos de los empleados.

Los Datos personales de los empleados que puedan almacenarse se considerarán datos confidenciales.

Los Datos personales de los empleados no se transferirán a terceros, excepto cuando sea requerido por nuestro negocio, y siempre que dichos terceros mantengan la confidencialidad de dichos datos, incluida, en este caso, la lista de direcciones electrónicas (correos electrónicos) utilizadas por los empleados de DMS LOGISTICS. Por otro lado, los empleados se comprometen a no almacenar datos personales en las instalaciones de DMS LOGISTICS, sin la autorización previa y expresa de la junta directiva.

Esta Política también es aplicable a los dispositivos personales y equipos de los empleados que se utilizarán para el ejercicio de sus actividades y servicios, según corresponda, siempre y cuando esté debidamente autorizado y permitido por DMS LOGISTICS.

DMS LOGISTICS podrá establecer, a su entera discreción, políticas, procesos y directrices de seguridad de información específicas, destinadas a regular el acceso y uso de datos, información, herramientas, recursos y servicios de DMS LOGISTICS en dispositivos personales de empleados, proveedores y usuarios autorizados, incluyendo los requisitos, modelos, marcas autorizadas. Estas políticas, procesos y directrices específicos pueden ser modificados por DMS LOGISTICS periódicamente.

Siempre que sea solicitado por DMS LOGISTICS, los empleados dispondrán sus aparatos y equipos personales para: (i) implementación de medidas de seguridad, tales como, actualizaciones de sistemas, servicios y aplicaciones de seguridad para protección y salvaguarda de los datos, información, sistemas y recursos de DMS LOGISTICS: (ii) monitoreo y averiguación de la conformidad de los empleados con las políticas, procesos y prácticas de DMS LOGISTICS; (iii) realización de pruebas y auditorias de seguridad al ambiente, recursos, sistemas, aplicaciones y redes de DMS LOGISTICS; (iv) copias de seguridad de la información, datos, servicios y actividades de DMS LOGISTICS contenidos en los aparatos y equipos personales de los empleados; y (v) remoción, eliminación y desinstalación de datos, información, servicios, recursos, herramientas de DMS LOGISTICS de los aparatos y equipos personales de los empleados, en particular, con el término de la relación contractual aplicable.

12. PROGRAMAS ILEGALES

El uso de programas ilegales (sin licencia) en DMS LOGISTICS está estrictamente prohibido.

Los usuarios no pueden, bajo ninguna circunstancia, instalar este tipo de *software* (programa) en equipos de DMS, incluso porque solo el personal del área de TI está autorizado a instalar programas previamente autorizados dentro de la política de seguridad de la organización. Semestralmente, el Sector de TI realizará controles de los datos de los servidores, unidades de disco y/o computadoras de los usuarios, con el fin de garantizar la correcta aplicación de la presente directriz. Si se encuentran programas no autorizados, estos deben eliminarse de las computadoras.

Todos los empleados firman un término de responsabilidad y uso de equipos y sistemas de DMS, en este término se detalla que:

- Cada individuo tiene su propia estación de trabajo. Esto significa que todo lo que se ejecute desde su estación será su responsabilidad.
- Cada vez que salga de su estación, asegúrese de cerrar la sesión o bloquear la consola.
- No instale ningún tipo de software / hardware sin la autorización del equipo técnico o de seguridad.
- No tenga MP3, películas, fotos y software con derechos de autor o cualquier otro tipo de piratería;
- Todos los datos relacionados con la empresa deben mantenerse en la unidad DMS, donde hay un sistema de copia de seguridad diario y confiable.
- Si es necesario, el empleado puede ponerse en contacto con el equipo técnico para solicitar asistencia.

13. PERMISOS Y CONTRASEÑAS

Cada usuario, para acceder a los datos de la red de DMS LOGISTICS, debe tener un usuario y contraseña previamente registrados por el sector de TI.

Quien debe proporcionar los datos relativos a los tipos de accesos y programas de cada empleado es el responsable directo, quien debe completar un formulario y entregarlo al departamento de Recursos Humanos. Cuando la necesidad de registro de un nuevo usuario para utilizar la «red», sistemas o equipos informáticos de DMS, el sector de origen del nuevo usuario debe comunicar esta necesidad al sector de TI, a través de comunicación interna o correo electrónico, informando a qué tipo de rutinas y programas tendrá derecho de acceso el nuevo usuario y cuáles serán restringidos.

El sector de TI se registrará e informará al nuevo usuario cuál será su primera contraseña, que debe cambiarse inmediatamente después del primer inicio de sesión y después cada 30 (treinta) días. Por motivos de seguridad, el área de TI recomienda que las contraseñas siempre tengan un criterio de seguridad mínimo para que no se copien fácilmente y no se puedan repetir.

Todos los usuarios responsables de la aprobación electrónica de documentos (ejemplo: órdenes de compra, solicitudes, etc.) deben comunicar al sector de TI quién será su reemplazo cuando se ausente de DMS, para que los permisos puedan ser cambiados (delegación de poderes). Cuando haya necesidad de acceso para usuarios externos, ya sean temporales o no, el permiso de acceso debe bloquearse tan pronto como este último haya terminado su trabajo y si hay una nueva necesidad de acceso en el futuro, el personal de TI debe desbloquearlo.

14. estaciones de computadora de trabajo DE LOS EMPLEADOS

Todas las estaciones de computadora de trabajo tienen usuario administrador, para garantizar que no se realicen cambios en la configuración del equipo.

La cuenta de administrador prohíbe a los usuarios descargar e instalar aplicaciones no autorizadas.

15. MONITOREO DE CORREOS ELECTRÓNICOS

El correo electrónico corporativo es accedido por herramientas proporcionadas por DMS LOGISTICS, sin que exista expectativa de privacidad como ocurre con el correo electrónico de uso personal y privado del empleado. El correo electrónico corporativo es una herramienta de propiedad de DMS LOGISTICS.

Por lo tanto, es importante que el empleado no utilice el correo electrónico corporativo de manera inadecuada, negligente o maliciosa.

16. INTERCAMBIO DE DATOS

El uso compartido de carpetas no está permitido en las computadoras, equipos de escritorio y otros dispositivos móviles de la empresa. Todos los datos deben almacenarse en la unidad de DMS y el personal de TI debe proporcionar la autorización para acceder a ellos. Periódicamente, el sector de TI realizará verificaciones de los datos de las unidades y/o las computadoras de los usuarios, con el fin de garantizar que los datos considerados confidenciales y/o restringidos no se almacenen en la red.

Los recursos compartidos de impresoras deben estar sujetos a autorizaciones de acceso de TI. La empresa no está autorizada a compartir dispositivos móviles como memorias USB y otros.

17. MESA Y PANTALLA LIMPIA

- Los documentos en papel y medios electrónicos no deben permanecer sobre la mesa, deben almacenarse en cajones o gabinetes cerrados con llave cuando no estén en uso, especialmente fuera del horario de oficina.
- La información física clasificada como sensible, confidencial, restringida o crítica para DMS debe almacenarse y bloquearse en un lugar seguro y separado.
- Las notas, recados y recordatorios no deben dejarse en la mesa ni pegarse en el escritorio, computadora, monitor, los tableros de anuncios ni paredes.
- No escriba información clasificada como restringida, confidencial, sensible en lugares donde la información puede estar expuesta, como tablones de anuncios, murales y pizarras.
- En los períodos de ausencia de la estación de trabajo, los documentos físicos se deben retirar de los escritorios y otras áreas de superficie;
- Los documentos para uso interno o confidencial en medios electrónicos deben almacenarse en entornos con acceso controlado y contraseñas para evitar el acceso a personas no autorizadas;
- Todos los documentos impresos deben ser destruidos antes de ser desechados en la basura. Los documentos clasificados como confidenciales y restringidos deben destruirse utilizando una máquina destructora de papel o incinerarse.
- Evitar imprimir documentos que puedan leerse en la computadora.
- Cerrar siempre la sesión al salir de su escritorio bloqueando la pantalla de la computadora.
- No dejar abierta la sesión en impresoras ni computadoras cuando esté fuera de la oficina.
- Las pertenencias personales siempre deben guardarse, ya sea en su armario o en su bolso.

- Su contraseña es personal e intransferible, por lo que no se la pase a nadie.
- Al final del día o cuando esté fuera, limpie el escritorio de trabajo, almacene los documentos, cierre los cajones y gabinetes y apague la computadora.
- No ponga en la mesa vasos con agua, jugos, café, etc.

18. ACCESO A INTERNET

- Dentro de las instalaciones del DMS, se proporciona acceso a Internet a sus usuarios autorizados, de acuerdo con las necesidades inherentes al desempeño de sus actividades profesionales;
- El acceso a Internet se puede proporcionar tanto a través de la red corporativa de DMS, como a través de la prestación de servicios de internet móvil, prestados por terceros, contratados por DMS;
- Solo se permite la navegación web. Los casos específicos que requieran otros protocolos deben solicitarse directamente al equipo de seguridad con autorización previa del gerente.
- El uso recreativo de Internet no debe ocurrir durante el horario de trabajo.
- Toda la información a la que se accede, transmite, recibe o produce a través del acceso a Internet proporcionado por DMS está sujeta a monitoreo, y no hay expectativa de privacidad por parte del usuario;
- Durante el monitoreo del acceso a Internet, DMS se reserva el derecho, sin ninguna notificación o advertencia, de interceptar, registrar, leer, copiar y divulgar por, o para, personas autorizadas para fines oficiales, incluidas investigaciones penales, toda la información traficada, ya sea que provenga de su red interna y esté destinada a redes externas o lo contrario;
- Durante el acceso a Internet proporcionado por DMS no se le permitirá descargar, cargar, incluir, poner a disposición, ver, editar, instalar, almacenar y/o copiar cualquier contenido relacionado expresa o subjetivamente, directa o indirectamente, con:
  - Cualquier tipo de explotación sexual;
  - Cualquier forma de contenido para adultos, erotismo, pornografía;
  - Cualquier tipo de pornografía infantil;
  - Cualquier forma de amenaza, chantaje y acoso sexual;
  - Cualquier acto calumnioso, difamatorio, denigrante, vejatorio, degradante o en violación de la moral y las buenas costumbres de la sociedad;
  - Prejuicio basado en color, sexo, elección sexual, raza, origen, condición social, creencia, religión, discapacidades y necesidades especiales;
  - Fomentar el consumo excesivo o recurrente de bebidas alcohólicas, tabaco y sustancias narcóticas, sean o no legales;
  - La comisión y/o incitación de delitos o infracciones penales;
  - La práctica de la propaganda política nacional o internacional;
  - La práctica de cualquier actividad comercial desleal;
  - La falta de respeto a la imagen o a los derechos de propiedad intelectual de DMS LOGISTICS;
  - La propagación de códigos maliciosos y amenazas virtuales;
  - Intentar exponer la infraestructura informática de DMS a amenazas virtuales;
  - Divulgación no autorizada de cualquier información de DMS LOGISTICS clasificada como confidencial, restringida o para uso interno;

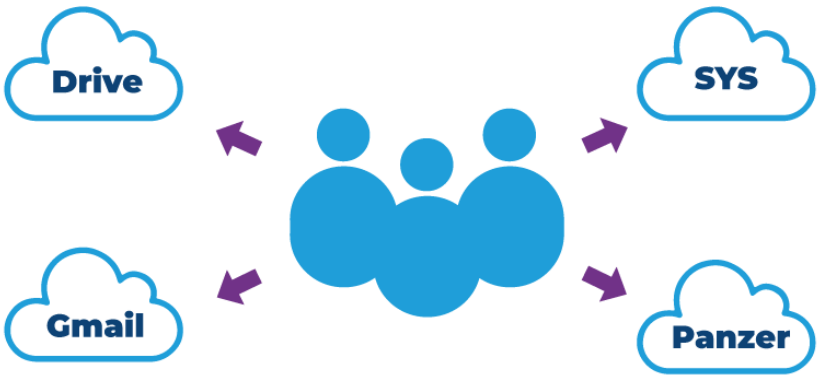
  - Uso de sitios web o servicios que buscan eludir los controles de acceso a Internet.
  - Está prohibido el uso de herramientas P2P (kazaa, Morpheus, etc.).
  - El uso de IM (Instant messengers o mensajería instantánea) no aprobada/autorizada por el equipo de seguridad está prohibido.
- Es importante recordar, nuevamente, que el uso de Internet será constantemente auditado, así como el usuario.
- El empleado será responsable del uso de los aparatos, equipos, recursos, herramientas y servicios puestos a disposición por DMS LOGISTICS para el desempeño de sus actividades.

19. Comportamiento corporativo en medios y redes sociales

Al utilizar sus medios de comunicación privados y redes sociales, los empleados, prestadores de servicios y terceros contratados deben respetar las siguientes restricciones:

- No se permite la publicación de contenido o comentarios directamente relacionados con DMS, sus empleados, terceros contratados y prestadores de servicios;

20. COPIA DE SEGURIDAD Y FIABILIDAD

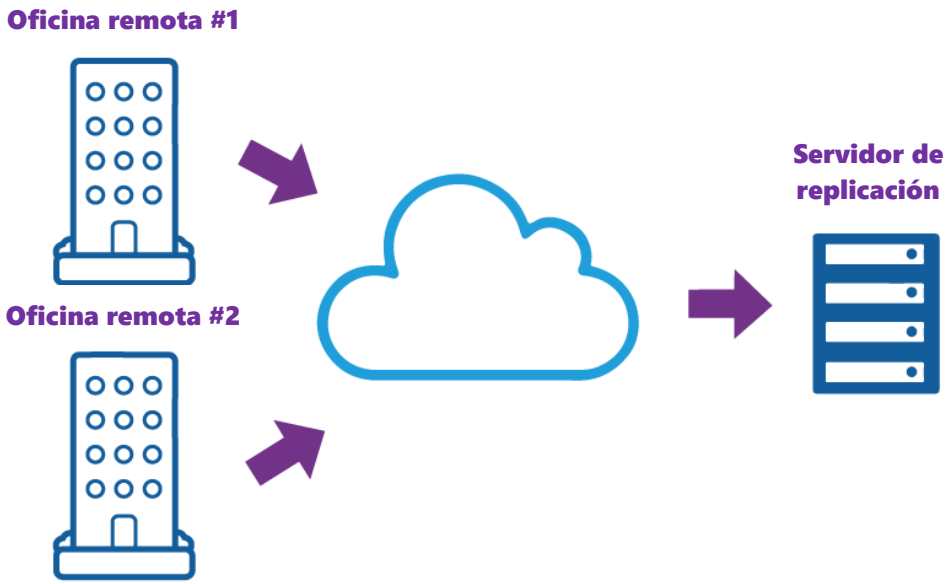


La gestión de la base de datos es responsabilidad exclusiva del Sector de TI, así como el mantenimiento, alteración y actualización de equipos y programas.

El usuario solo tiene acceso al servidor a través de nuestra IP local.

Las copias de seguridad se realizan automáticamente en nuestra nube y servidor, por lo que no hay riesgo de pérdida de datos.

Todos nuestros datos de la nube se replican a otro servidor, por lo que, incluso, si hay algún tipo de problema en la nube, nuestros datos se guardarán en el servidor.



21. ADMISIÓN, DESVINCULACIÓN Y DESPIDO DE EMPLEADO

21.1. IDENTIFICACIÓN DE LA NECESIDAD

El sector de reclutamiento y selección del personal de DMS LOGISTICS debe informar al sector de Informática, cualquier movimiento de admisión, suspensión, interrupción y despido de sus empleados, para que puedan ser registrados o excluidos en los sistemas de

DMS. Esto incluye la provisión de su contraseña y el registro de su nombre de usuario en los sistemas, por parte de la industria informática.

Corresponde al sector de contratación comunicar al sector de Informática las rutinas a las que el nuevo contratado tendrá derecho de acceso. En el caso de los temporales y/o pasantes, también se debe informar el tiempo en el que los mismos prestarán servicio a DMS, de modo que en la fecha de su desvinculación, también puedan darse por terminadas las actividades relacionadas con el derecho de acceso a los sistemas. En caso de despido, el sector de Recursos Humanos debe comunicar el hecho lo antes posible a Informática, para que el empleado desvinculado quede excluido de los sistemas de DMS.

Corresponde al sector de Recursos Humanos dar conocimiento y obtener las firmas de acuerdo adecuadas de los nuevos contratados en relación con la Política de Seguridad de la Información de DMS LOGISTICS. Ningún empleado puede ser contratado sin haber aceptado expresamente esta política.

21.2. ACCESOS DE CORREO ELECTRÓNICO Y PLATAFORMAS CORPORATIVAS - AUSENCIA

Durante el período de separación de la empresa, el sector de TI suspenderá el acceso del empleado a los sistemas informáticos y correos electrónicos y redirigirá automáticamente los correos electrónicos a otro miembro del equipo y mantendremos informados a nuestros clientes y socios de la ausencia del empleado en el período determinado de acuerdo con la decisión del gerente responsable.

21.3. RETORNO AL TRABAJO

Después de que se apruebe el retorno al trabajo, Recursos Humanos debe informar al sector de TI de la liberación del acceso del empleado a los sistemas informáticos y correos electrónicos y suspender la redirección automática de correos electrónicos.

22. PROMOCIÓN Y TRANSFERENCIA DEL EMPLEADO

Cuando un empleado es ascendido o transferido desde el sector o la gestión, el sector de Recursos Humanos debe comunicar el hecho al sector de TI, para que se realicen las adaptaciones necesarias para el acceso de dicho empleado a los sistemas informatizados de DMS.

23. PENALIDADES

El incumplimiento de la Política de Seguridad de la Información de DMS LOGISTICS puede resultar en la aplicación de medidas y sanciones, incluyendo, entre otras, el despido de empleados de acuerdo con la naturaleza y gravedad del suceso.

24. INFORMACIÓN Y COMUNICACIÓN

Todos los destinatarios de esta Política, al identificar una situación de riesgo relacionada con esta Política y otras normas de contenido similar, tienen la responsabilidad de comunicar el hecho a la gerencia y al Departamento de calidad de DMS.

Para ello, se podrán utilizar los siguientes canales de comunicación:

- Canal Disque Denuncia: ouvidoria@dmslog.com (en caso de que quiera hacer una denuncia anónima);
- Llamado a través de DMSYS.

A modo de ejemplo, los empleados deben informar, lo antes posible, de cualquier situación, hecho o evento, incluida la mera sospecha o intento, que involucre, entre otros:

(i) uso, acceso, transmisión, divulgación, intercambio o cualquier otro tipo de procesamiento no autorizado de datos e información de propiedad o controlada por DMS LOGISTICS;

(ii) cualquier iniciativa, interna o externa, destinada a interferir, perjudicar, comprometer la seguridad, disponibilidad, autenticidad, confidencialidad e integridad de los datos e información, o el funcionamiento y rendimiento de los dispositivos, equipos, recursos, herramientas, servicios y medidas de seguridad de DMS LOGISTICS;

(iii) pérdida, daño, fallo, defecto de aparatos, equipos propiedad o bajo el control de DMS, o incluso aparatos personales y equipos de empleados, a través de los cuales tengan acceso a datos e información de propiedad o bajo el control de DMS LOGISTICS;

(iv) cualquier incumplimiento que pueda identificarse con esta Política y otras aplicables a los empleados, tales como acuerdos de confidencialidad, prestación de servicios, contratos de trabajo, entre otros; y

(v) cualquier otra situación, hecho o evento que, por su naturaleza, pueda suponer un riesgo de información y seguridad cibernética para DMS LOGISTICS.

25. TÉRMINOS Y DEFINICIONES

- Información sensible: todos los datos que necesitan ser protegidos.
- Datos personales sensibles: datos personales sobre el origen racial o étnico, convicciones religiosas, opiniones políticas, pertenencia a un sindicato u organización de carácter religioso, filosófico o político, datos relativos a la salud o la vida sexual, datos genéticos o biométricos, cuando estén vinculados a una persona física;
- Garantía de seguridad de la información: capacidad de los sistemas y organizaciones para garantizar la disponibilidad, integridad, confidencialidad y autenticidad de la información.
- Acceso: posibilidad de comunicarse con un dispositivo, medio de almacenamiento, unidad de red, memoria, registro, archivo, etc. para recibir, proporcionar o eliminar datos.
- Almacenamiento: acción o resultado de mantener o conservar datos en almacenamiento.
- Archivado: acto o efecto de mantener un dato registrado aunque ya haya perdido su validez o agotado su validez.
- Evaluación: acto o efecto de calcular el valor sobre uno o más datos.
- Clasificación: forma de ordenar los datos según algunos criterios establecidos.
- Recopilación: recopilación de datos para fines específicos.
- Comunicación: transmitir información relevante para las políticas de acción de datos.
- Control: acción o poder para regular, determinar o monitorear acciones sobre los datos.
- Difusión: acto o efecto de difusión, propagación, multiplicación de datos.
- Distribución: acto o efecto de la eliminación de los datos según los criterios establecidos.

- Eliminación: acto o efecto de eliminar o destruir datos del repositorio.
- Extracción: acto de copiar o eliminar datos del repositorio en el que se encuentra.
- Modificación: acto o efecto de cambiar los datos.
- Procesamiento: acto o efecto del procesamiento de datos.
- Producción: creación de bienes y servicios a partir del procesamiento de datos.
- Recepción: acto de recepción de los datos al final de la transmisión.
- Reproducción: copia de datos preexistentes obtenidos a través de cualquier proceso.
- Transferencia: cambio de datos de un área de almacenamiento a otro, o a un tercero.
- Transmisión: datos móviles entre dos puntos por medio de dispositivos eléctricos, electrónicos, telegráficos, telefónicos, radioeléctricos, neumáticos, etc.
- Uso: acto o efecto del uso de los datos.
- Uso compartido de datos: comunicación, difusión, transferencia internacional, interconexión de datos personales o procesamiento compartido de bases de datos personales por parte de organismos y entidades públicas en cumplimiento de sus facultades legales, o entre estos y entidades privadas, recíprocamente, con autorización específica, para uno o más métodos de procesamiento permitidos por estas entidades públicas, o entre entidades privadas.

26. LA EMPRESA Y LA POLÍTICA DE SEGURIDAD

Todas las reglas establecidas en este documento tienen por objeto proteger a la institución contra el acceso indebido a los sistemas informatizados.

Al recibir la copia de la Política de Seguridad, el empleado se compromete a respetar todos los temas aquí tratados y es consciente de que sus correos electrónicos y navegación por Internet pueden estar siendo monitoreados.

El equipo de seguridad está a su entera disposición para preguntas y asistencia técnica.

27. SITUACIONES NO CUBIERTAS

Esta Política presenta pautas generales, y algunas situaciones específicas pueden no estar cubiertas.

Lo que se espera en estos casos es que cada uno actúe con responsabilidad, prudencia y conciencia ética, evaluando el mejor camino a seguir con la certeza de que la solución adecuada siempre estará regida por el sentido común y los valores que atesoramos.

Cualquier pregunta no especificada en este documento y relacionada con los temas ética y conducta, debe ser sometida a evaluación por la Junta directiva.

Corresponde al Departamento de Recursos Humanos mantener actualizado este documento, de acuerdo con el publicado por el grupo a nivel internacional, poniendo su contenido al conocimiento de todo el Grupo DMS.

28. VIGENCIA

Este Código entra en vigor en la fecha de su publicación, revocando y sustituyendo cualquier comunicación anterior sobre el tema y permanecerá en vigor por un período indefinido.

29. HISTORIAL DE REVISIÓN

Revisión	Fecha	Descripción
00	18/10/2018	Emisión del documento.
01	28/09/2020	Revisión general para incluir en el documento nuevos compromisos con el medio ambiente, la salud y la seguridad de los empleados, y la seguridad y codificación de la información.
02	1/12/2020	Revisión general para cambiar el término web y nubes por web y nube y modificar el modelo del documento.

30. APROBACIÓN Y CLASIFICACIÓN DE LA INFORMACIÓN

Preparado por:	Wellington Ferreira	
Revisado por:	Natalie Corrêa	
Aprobado por:	Eduardo Reis	
Nivel de confidencialidad:	X	Información pública
		Información interna
		Información confidencial
		Información restringida

Anexo I - Documento de compromiso con la Política de Seguridad de la Información

Declaro, a todos los efectos, que he recibido una copia de la Política de Seguridad de la Información de DMS LOGISTICS, la cual estaba en un lenguaje claro y fácil de entender, por lo que asumo que tengo conocimiento de mi responsabilidad y me comprometo a cumplirla y respetarla plenamente.

Declaro, además, que soy consciente del cumplimiento en todas las situaciones y circunstancias que están directa o indirectamente vinculadas a mis actividades en DMS LOGISTICS.

Del mismo modo, tengo conocimiento de que el incumplimiento de cualquiera de los términos contenidos en esta Política de seguridad de la información dará lugar a la formación de un sindicato administrativo, que se constituirá para determinar cualquier irregularidad.

Acto continuo, ante la constatación de irregularidades, declaro que soy consciente de que DMS puede promover las medidas apropiadas, tanto en el ámbito administrativo, como en el judicial, buscando reparar todos los daños causados, ya sea en el ámbito penal, civil o laboral.

Por último, por estar de acuerdo, firmo este instrumento.

Lugar y fecha	
Nombre completo	
CPF	
Firma	

NUNCA COMPROMETEMOS LA CALIDAD NI LA ÉTICA EMPRESARIAL

WE NEVER COMPROMISE ON QUALITY AND BUSINESS ETHICS

WWW.DMSLOG.COM