ANDES LOGISTICS
CHILE

POLITICA DE ACCESO A INFORMACIÓN CONFIDENCIAL

v.01

ANDES LOGISTICS DE CHILE S.A. ha dispuesto la presente política para evitar el acceso no autorizado a información confidencial por parte del trabajador u otros, logrando el control total en los accesos, para lo cual:

- Cuando se solicite acceso físico y/o lógico para un colaborador, previo a la autorización debe tener firmado el formato "Declaración Jurada de no Revelar Información Confidencial".
- Cada área o responsable de proceso propietario de activos de información, es responsable de asegurar que a cada usuario solo se le otorgue acceso a la información, en cualquier formato, que necesite para la realización de sus tareas, según su área de trabajo y perfil de cargo.
- Toda persona con activos de información a su cargo es responsable del cuidado de estos y de la información a la que se puede acceder a través de ellos, debiendo resguardar siempre la integridad, confidencialidad y disponibilidad de esta
- Todo(a) usuario(a), al momento de ser autorizado(a) para acceder a un sistema, toma conocimiento de sus derechos de acceso y obligaciones, sin perjuicio de compromisos previos, y de los niveles de seguridad y la clasificación de la información a que accede.
- La eliminación de usuarios(as) dentro de plazos oportunos debe ser gestionada por las áreas directas. Con esto se busca garantizar la consistencia con los niveles de autorización asignados.
- Es responsabilidad de las áreas y/o responsables de proceso revisar al menos semestralmente los derechos de acceso otorgados a los(as) usuarios(as).
- Cuando un(a) colaborador(a) o alguna persona externa deja un puesto de trabajo, la información almacenada en los equipos institucionales o impresa a la que tuvo acceso debe ser revisada por su jefe inmediato, para verificar que no se ha alterado los requisitos de seguridad de la información.
- Está prohibido el uso de herramientas para obtener información de la red, tales como detección de puertos, servicios y archivos en general en los sistemas de información de la Institución. El uso o detección de este tipo de herramientas debe ser reportado como un incidente de seguridad de la información.
- El acceso a páginas web que estén bloqueadas debe ser solicitado formalmente por el área usuaria del requirente y autorizado por el área de Sistemas y/o Gerencia General.
- Está prohibido el uso de cuentas de excolaboradores(as) para acceder a los equipos de trabajo y/o sistemas, a menos que esto sea formalmente solicitado y validada el jefe inmediato y/o Gerente General.

Además, se expresa lo siguiente:

- Todos los equipos de trabajo del personal de la organización deben ser apagados una vez que los(as) colaboradores(as) terminen su jornada de trabajo.
- Es responsabilidad de los responsables de proceso que las áreas físicas con restricciones de acceso estén debidamente señalizadas.
- Toda persona que ingrese a las dependencias físicas de la Institución debe respetar sus vías de acceso, señalizaciones y áreas restringidas. Asimismo, toda persona externa solo debe transitar por las áreas a que ha sido autorizada; constituyendo la transgresión a esta norma como un incidente de Seguridad de la Información.

GERENTE GENERAL

Fecha de Revisión: 03/03/2025