

POLITICAS DETALLADAS DE LA SEGURIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE LOS ACTIVOS DE INFORMACIÓN.

Política de la seguridad de la información - Ref.: ISO/IEC 27001 CL A.5.1.1

- **Definición de la Política:**

LAMINACO desde la alta dirección considera la información como un activo estratégico convirtiéndose en un componente esencial e imprescindible que debe ser protegido para el cumplimiento de los objetivos de LAMINACO. Comprometiéndose en conjunto con las partes interesadas, a apoyar las actividades estratégicas para la protección de la información como parte del plan de administración de riesgos, la consolidación de una cultura de seguridad y el cumplimiento de los requerimientos internos, contractuales y regulatorios vigentes. Promoviendo mejores prácticas y controles dentro de la organización que contribuyan a la mejora continua del sistema de gestión de seguridad de la información.

Política de trabajo en casa - Ref.: ISO/IEC 27001 CL A.6.2.2

- **Definición de política:**

Con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información en un entorno de trabajo en casa, se establece que LAMINACO debe proveer a los colaboradores los recursos necesarios para realizar su labor en el sitio determinado por el equipo de talento humano. A parte de ello se debe definir el modelo de trabajo en casa determinado por la compañía, establecer el protocolo de asignación de recursos para trabajar en el lugar establecido y definir protocolos de monitoreo de actividades de los colaboradores que puedan afectar la confidencialidad, integridad y disponibilidad de la información.

Seguridad de la información para las relaciones con proveedores - Ref.: ISO/IEC 27001 CL. A.15.1.1

- **Definición de política:**

Establecer los requisitos de seguridad de la información para reducir la probabilidad de los riesgos asociados con las autorizaciones otorgadas a los proveedores a los activos de información de LAMINACO, se deben acordar con éstos y se deben documentar, para así asegurar la protección de los activos de la compañía. Se deben seguir los siguientes lineamientos:

- a. Se les incluirá dentro de su contrato una cláusula de confidencialidad de información. A aquellos proveedores o contratistas que tengan relaciones comerciales con la compañía.
- b. Los proveedores no deben tener acceso a información de carácter sensible de LAMINACO. Solo se debe otorgar acceso a los activos de información donde los proveedores vayan a ejecutar las labores de mantenimiento dentro del activo de

información, está se proporcionará con las medidas de seguridad necesarias, con el fin de que no pueda ser modificada o alterada por el proveedor.

- c. Los proveedores no podrán tener acceso a áreas o zonas donde se encuentre información sensible en LAMINACO. Sí fuera necesario su ingreso a determinadas áreas, será necesaria la autorización de un funcionario de la compañía, el cual debe acompañar al contratista durante el tiempo que este permanezca en dicha área.

Política de control y Administración de accesos - Ref.: ISO/IEC 27001 CL. A.9.1.1

- **Definición de la política:**

LAMINACO, define los lineamientos entorno al acceso a sus recursos computacionales:

- a. Se denominan usuarios de la red de LAMINACO todos los colaboradores en misión, los contratistas, los pasantes y terceros, bien sea personas naturales o jurídicas que estén de forma temporal o permanente en LAMINACO.
- b. El acceso a la red por parte de proveedores debe ser autorizada únicamente mediante firma impresa y documentación de aceptación de un acuerdo de confidencialidad hacia la compañía, donde el proveedor este comprometido con el uso exclusivo del servicio para el que fue provisto el acceso para las labores de mantenimiento.

Escritorio limpio y pantalla limpia- Ref.: ISO/IEC 27001 CL. A. 11.2.9

- **Definición de la política:**

Se debe implementar por parte de LAMINACO una política de escritorio limpio para proteger documentos en papel y dispositivos de almacenamiento removibles y una política de pantalla limpia en las instalaciones de procesamiento de información, a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información.

Respaldo de la información. - Ref.: ISO/IEC 27001 CL. A. 12.3.1

- **Definición de la política:**

Las copias de seguridad de la información deben estar almacenadas en soluciones de backup en red con replica en un repositorio en la nube. Se deben hacer copias de respaldo de la información, de los sistemas en función de su criticidad, y hacer pruebas de restauración regularmente con el fin de asegurar la gestión de calidad de copias de seguridad, revisar la integridad y disponibilidad de la información.

Transferencia de la información - Ref.: ISO/IEC 27001 CL. A.13.2.

- **Definición de la Política:**

Se debe prohibir el envío de información confidencial o sensible de LAMINACO a personal externo de la entidad sin autorización previa.

- a. Está prohibido el uso del correo electrónico personal (hotmail, gmail, etc.) para el envío o recepción de cualquier tipo de información relacionada con la compañía. El correo corporativo institucional es el medio oficial de transferencia de información.
- b. Está prohibido el uso de mecanismos de transferencia o almacenamiento de información basados en la nube que no sean autorizados por el equipo de soporte de TIC y para los cuales no se tenga contratado un servicio corporativo que garantice la confidencialidad de la información transferida a la nube.
- c. Cualquier información que entre o salga de la compañía por medio magnético, transmisión electrónica o hardware, deberá tener los mecanismos de cifrado necesarios y registro de los eventos que aseguren la confidencialidad, integridad, auditabilidad y disponibilidad de esta información.