POLÍTICA DE SISTEMAS DE INFORMACIÓN

Para **Ciprés Seguridad y Protección LTDA**., es primordial implementar medidas técnicas y administrativas necesarias para gestionar la seguridad de los datos de carácter personal protegiendo la confidencialidad, integridad, uso, acceso no autorizado y/o fraudulento.

Ciprés Seguridad y Protección LTDA., comprometido con el uso adecuado de los servicios informáticos para el desarrollo de actividades en la organización determina los siguientes lineamientos:

INFORMACION CONFIDENCIAL: Toda la información que se maneja en **Ciprés Seguridad y Protección LTDA**. es de carácter confidencial y esta no podrá ser retirada de la empresa en ningún medio extraíble tal como memoria USB, discos externos o Cd, al igual está totalmente prohibido enviar información vía correo electrónico a personas externas que no forman parte de la relación con la empresa tales como sí lo son los clientes, proveedores y socios de negocios.

PERFIL: De acuerdo a las funciones establecidas para cada cargo, se darán los permisos requeridos.

ALMACENAMIENTO DE LA INFORMACION NUBE WORKSPACE: Toda la información diaria trabajada en cada una de las áreas de la compañía, están sincronizadas en carpetas almacenadas directamente en la nube de cada uno de los correos. Cada correo corporativo de Google workspace posee dominio propio de cipresseguridad.com.co .

En la nube y bajo custodia de la gerencia en el correo gerencia@ se encuentran: El Sistema de Gestión Integral, El archivo activo de todo el personal de la empresa, información del área comercial, bancos, información de la junta de socios, base de datos del personal de la empresa, entre otros.

En la nube bajo la custodia de la coordinación de Talento humano en el correo talentohumano@ se encuentran: Backup talento humano de los años 2014,2015,2016,2017,2018,2019,2020 y todos los archivos diarios de trabajo del área tales como contrataciones, capacitación, desvinculaciones, bienestar, disciplinarios entre otros directos del área.

En la nube bajo la custodia de la dirección y coordinación de operaciones, en los correos director.operaciones@ y operaciones@, se encuentra: Backup operaciones 2014,2015,2016,2017,2018,2019,2020 y todos los archivos diarios de trabajo del área tales como análisis de seguridad, inspecciones, control de armamento, controles de minutas, controles de consignas e instructivos, entre otros del área.

En la nube bajo la custodia del asistente administrativo, en el correo comercial@ , se encuentran: archivo de kardex y manejo de almacén y todos los documentos relacionados con la selección de proveedores, gestión de solicitudes y órdenes de compra entre otros del área.

En la nube bajo la custodia de la central de Monitoreo, en el correo centralcipres@ , se encuentran: Todos los archivos de programación de turnos, archivo de control de horas extras y control de adicionales entre otros documentos del área.

POLÍTICA DE SISTEMAS DE INFORMACIÓN

ENVIO DE CORREOS ELECTRONICOS: Los únicos correos autorizados para enviar información, comunicados, circulares a los funcionarios y asociados de negocio son los asignados por la empresa pertenecientes al dominio @cipresseguridad.com.co, cualquier otro comunicado que no sea enviado desde este correo no será considerado oficial como representación de la empresa.

SEGURIDAD DE LA INFORMACION Y CONTRASEÑAS

- El personal que ingresa como usuario a los equipos de cómputo de la organización debe aceptar las condiciones de confidencialidad, de uso adecuado de los bienes informáticos y de la información.

- Todo el personal nuevo, que de acuerdo a sus funciones y decisiones gerenciales se le otorgue una dirección de correo institucional deberá utilizar este usuario únicamente para actividades relacionadas con sus funciones.

- El personal que ingresa como usuario deberá asegurarse de cargar la información que consideren relevante en la carpeta instalada en el backup para asegurar las copias de respaldo.

- Cuando el equipo sea enviado a reparación o en un tiempo considerable de almacenamiento se deberá asegurar de cargar en la carpeta en la nube del correo asignado, toda la información sensible que se encuentre en el equipo, previendo así la pérdida involuntaria de información, derivada del proceso de reparación.

- Los computadores portátiles y cualquier activo de información, podrá ser retirado de las instalaciones, únicamente con la autorización de la Gerencia.

Uso de Contraseñas

- El personal que ingresa como usuario será el responsable del usuario y contraseña que recibe para el uso y acceso de los equipos de cómputo y correos.

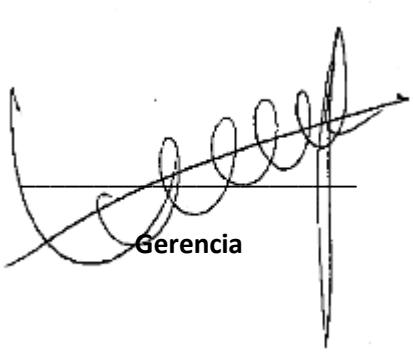
- El personal que ingresa como usuario deberá mantener sus equipos de cómputo con controles de acceso como contraseñas

- Está prohibido que las contraseñas se encuentren de forma legible en cualquier medio impreso y dejarlos en un lugar donde personas no autorizadas puedan descubrirlos.

- Se consideran violaciones graves el robo, daño, divulgación de información reservada o confidencial lo cual conllevara a una causa de despido justificado de la organización.

POLÍTICA DE SISTEMAS DE INFORMACIÓN

Dando cumplimiento al Decreto 1581: 2012, Indicamos que toda información será recibida, salvaguardada y manejada en las Bases de datos almacenadas en el backup de **Ciprés Seguridad y Protección LTDA**. cuyo acceso será restringido. Todo el personal que visite o trabaje en las instalaciones de **Ciprés Seguridad y Protección LTDA**., podrá ser Grabado y monitoreado por su seguridad.



Gerencia

Notifíquese y cúmplase.

Dado en Bogotá a los 10 días del mes de agosto del 2021