

	<b>POLÍTICA DE SEGURIDAD INFORMATICA</b>	Código	M-PL-023
		Versión	1
		Fecha	9/03/23

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:

**INFORMACIÓN 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 INFORMACIÓN 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.

	<b>POLÍTICA DE SEGURIDAD INFORMATICA</b>	Código	M-PL-023
		Versión	1
		Fecha	9/03/23

**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 considere 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 conllevará a una causa de despido justificado de la organización.

### **Restricción en el uso de páginas de Internet**

- Está prohibido en los computadores de la empresa el ingreso a las paginas Facebook, You tube y páginas de contenido para adultos
- Los computadores de propiedad de la empresa tendrán bloqueado el acceso a las páginas Facebook, You tube y páginas de contenido para adultos. Se exceptúa de esta restricción a la página de facebook el departamento de Talento Humano, quien por la necesidad de publicar ofertas laborales por este medio requiere acceso a la pagina.

	<b>POLÍTICA DE SEGURIDAD INFORMATICA</b>	Código	M-PL-023
		Versión	1
		Fecha	9/03/23

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.

### ESCRITORIO LIMPIO

- La pantalla de computador (escritorio) debe estar libre de archivos o enlaces de acceso a archivos, estos deben ubicarse en las debidas carpetas de almacenamiento que se encuentran sincronizadas con el google DRIVE (NUBE WORKSPACE).
- Siempre que el personal se ausente de su estación de trabajo, deberá bloquear las sesiones de sus equipos de cómputo.
- Todos los equipos de cómputo y dispositivos portátiles deberán tener aplicado el cierre de sesión por inactividad, definido por el equipo de seguridad de la información.
- Siempre que el personal se ausente de su estación de trabajo deberá bloquear todos los equipos y dispositivos que de él dependen y/o utiliza.
- Al activarse el protector de pantalla debe bloquear la sesión en los equipos de cómputo y dispositivos móviles de la SSF, este deberá activarse después de 5 minutos de inactividad de cualquiera de estos equipos.

### USO DE DISPOSITIVOS MOVILES

Los dispositivos tipo PC Portátil. Laptop, notebook, teléfonos inteligentes, tabletas o similares se registrarán bajo la presente Política de Seguridad Informática.

- Los usuarios de los dispositivos NO están autorizados a cambiar las configuraciones del equipo, desinstalar software, formatear o restaurar de fábrica los equipos móviles
- No almacenar información personal en los dispositivos móviles asignados
- Está prohibido instalar aplicaciones no autorizadas
- Se autoriza el uso de Whatsapp corporativo
- Toda información que se genere, procese almacene y/o transite por la RED de CIPRES SEGURIDAD se considera propiedad de la empresa.
- Los equipos portátiles están autorizados a ser retirados de las instalaciones de la empresa, únicamente por los usuarios asignados, quienes tendrán la responsabilidad del adecuado uso, de acuerdo a las directrices de la presente Política.

### CONSERVACIÓN DE LOS RECURSOS

- Ciprés Seguridad y Protección LTDA coordinara el mantenimiento preventivo y correctivo de los equipos de cómputo una vez al año.
- Se prohíbe a todos los trabajadores descargar y abrir archivos de remitentes desconocidos o sospechosos

	<b>POLÍTICA DE SEGURIDAD INFORMATICA</b>	Código	M-PL-023
		Versión	1
		Fecha	9/03/23

### **INCUMPLIMIENTO**

En cualquier momento la Gerencia podrá hacer revisión del cumplimiento de la política directamente en los dispositivos móviles.

El incumplimiento de esta política de seguridad Informática traerá consigo consecuencias entre ellas apertura de procesos disciplinarios que conlleven a aplicación de sanciones, incluso la terminación laboral.



Notifíquese y cúmplase.

Dado en Bogotá a los 29 días del mes de septiembre del 2025