GER-F-010	DETECCIÓN SEGURIDAD PRIVADA LTDA.	
Fecha Aprobación 04/03/2026		
Versión: 5	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD	

DETECCIÓN SEGURIDAD PRIVADA LTDA, establece los lineamientos de seguridad de la información para brindar a los usuarios, los recursos tecnológicos e informáticos con estándares de calidad, con la capacidad de soportar las tareas diarias, concientizar al usuario de los riesgos informáticos para evitarlos y así tener continuidad en el servicio los 365 días del año de manera confiable para salvaguardar los intereses y la relación con nuestros clientes, usuarios, empleados, proveedores y demás partes interesadas.

DETECCIÓN SEGURIDAD PRIVADA LTDA, cuenta con personal que trabaja permanentemente en la seguridad digital con el fin de promover un entorno confiable y seguro, que maximice los beneficios económicos y sociales de todos los actores que tienen relación directa con la empresa, garantizando la identificación del impacto de amenazas que ponen en peligro los datos, la continuidad de negocio o la imagen de la compañía.

OBJETIVO:

- Garantizar buenas prácticas del manejo de la información de la empresa, cumpliendo los lineamientos de seguridad a nivel mundial.
- Evitar la fuga de información confidencial de la empresa.
- Conocer e identificar los riesgos a los que están expuestos en el entorno digital.
- Proteger, prevenir y reaccionar ante los delitos y ataques cibernéticos.
- Cumplir con estándares de seguridad, que contribuyen a la protección de la información y por tanto a la prevención del fraude.
- Sensibilizar a los colaboradores de manera que se cree una cultura de ciberseguridad.
- Establecer acuerdos y responsabilidades en cuanto al manejo, uso y gestión de la información, durante el desarrollo de sus funciones.

Este documento contiene una serie de **NORMAS DE OBLIGATORIO CUMPLIMIENTO**, avaladas por la Gerencia General para el uso de los recursos informáticos y su incumplimiento acarreará sanciones disciplinarias.

MANEJO DE HARDWARE (EQUIPOS):

- El área de Medios Tecnológicos es responsable del buen funcionamiento de los equipos de cómputo y es el único departamento autorizado para realizar mantenimientos y mejoras, tales como cambios de procesador, memoria o tarjetas. Se debe evitar que personal ajeno a este departamento manipule los equipos. Está prohibido destapar los dispositivos sin la autorización correspondiente.

- Está prohibido marcar los equipos o colocar cualquier tipo de calcomanía o sticker no autorizado.
- Los equipos solo podrán ser trasladados de lugar con la autorización del área de Medios Tecnológicos y de Gerencia, con el fin de controlar los riesgos derivados de dicho cambio.
- Los empleados deberán reportar cualquier pérdida o daño de los equipos a su cargo que sean propiedad de **DETECCIÓN SEGURIDAD PRIVADA LTDA.**
- La conexión de equipos personales está totalmente prohibida. En caso de ser necesaria, se deberá contar con la autorización previa del área de Medios Tecnológicos y Gerencia.
- Todos los equipos deberán contar con estabilizadores o supresores de picos para reducir el riesgo de pérdida de información debido a cambios de voltaje. De ser posible, se recomienda que los equipos estén conectados a tomas de corriente eléctrica reguladas.
- Los parlantes serán retirados de los puestos de trabajo, y únicamente permanecerán en los lugares donde sean necesarios para funciones laborales específicas. Esta función será monitoreada por el área de Medios Tecnológicos.
- Al crear un nuevo puesto de trabajo o cuando un empleado sea retirado de la compañía, el jefe inmediato deberá informar al área de Medios Tecnológicos para que se realice la inspección correspondiente, se reciba el equipo y se verifique la información que contiene.

MANEJO DE SOFTWARE (PROGRAMAS):

- Solamente el área de Medios Tecnológicos será la encargada de la instalación y puesta en marcha del software que se instale en los equipos, la adquisición de las licencias será realizada en coordinación con el departamento de compras y con el visto bueno de la Gerencia y la Dirección de Medios Tecnológicos.
- Se prohíbe totalmente la instalación de programas de chats, la compañía implementará el Meet y grupos específicos de WhatsApp como herramientas para comunicación y será netamente laboral.
- La utilización del internet debe ser estrictamente para fines laborales.
- La empresa le brinda un correo corporativo, por lo tanto, la utilización de correos personales está totalmente prohibida en horas laborales.
- Los sitios de internet que se encuentran prohibidos son aquellos que según su historia contienen virus, malware, etc., entre ellos se encuentran: bibliotecas musicales, canales de radio y televisión, páginas de descarga masiva y Torrens, redes sociales como Twitter, Facebook, Instagram entre otros.

- El uso de internet será constantemente monitoreado para verificar que se esté usando apropiadamente.
- Cada equipo debe contar con los wallpapers correspondientes a la empresa y estos no se pueden cambiar o modificar.
- Los equipos contarán con un bloqueo automático el cual está programado.

CLAVES DE SEGURIDAD:

- Todos los equipos deben tener contraseña la cual será asignada por el área de Medios Tecnológicos, el usuario tiene prohibido modificar o hacer cambios en las contraseñas establecidas y si lo hace debe informarle de inmediato al área encargada de controlar los cambios en las contraseñas según el tiempo estipulado y los requerimientos de seguridad.
- La contraseña debe tener por lo menos 12 caracteres e incluir caracteres en mayúscula y minúscula y también números, para establecer un mayor nivel de seguridad.
- La utilización de la contraseña es personal e intransferible, cada usuario debe memorizarla y está completamente prohibido darla a conocer a terceros o a sus compañeros de trabajo.
- Los usuarios de los equipos tendrán un nivel de seguridad restringido, es decir no serían administradores de los equipos, esto con el fin de evitar instalación de software y prevenir la pérdida de información, por el olvido de contraseñas.
- Se deben escoger caracteres de fácil recordación, que preferiblemente se puedan digitar sin mirar el teclado y de una forma rápida, pero que no sean palabras comunes ni nombres propios de familiares o allegados.
- El colaborador se compromete a no revelar la contraseña que ha asignado en la compañía, si no es respetado este compromiso, esto acarreará sanciones disciplinarias.
- Por seguridad de la información, se debe cambiar la clave seguridad cada tres meses previo aviso del área de Medios Tecnológicos.
- Los documentos digitales que cuenten con importancia relevante dentro de cada uno de los procesos deben contar con contraseña de apertura, que cada departamento se encargará de la misma.

CONTROL Y USO DE LA EXTRACCIÓN DE INFORMACIÓN:

- La utilización de los puertos extraíbles y de los sistemas de grabación digital estarán restringidos, los únicos que tendrán permisos especiales a estos son los

Directores o las personas que por su trabajo lo requieran con previa autorización de la Gerencia o el área de Medios Tecnológicos.

- La información digital que salga correspondiente a la compañía, solamente se podrá difundir por medio del correo electrónico corporativo autorizado.
- El área de Medios Tecnológicos instalará en cada computador una carpeta que tendrá el nombre del área o el usuario, allí se guardará la información relevante de la compañía y a dicha carpeta se le realizará copia de seguridad en los términos establecidos, si se almacena información en otro sitio diferente será bajo la responsabilidad del usuario del equipo.
- Las copias de seguridad (backups) se configuran automáticamente cada día en el servidor. Estas copias se almacenan en un disco externo, que se reemplaza semanalmente. Los discos externos reemplazados se almacenan en un lugar externo a la sede, bajo la custodia de la Gerencia.
- Los equipos podrán ser utilizados únicamente durante el horario habitual de lunes a viernes y sábados hasta el mediodía. En caso de requerir su uso en horarios diferentes (domingos, festivos, etc.), será necesario enviar un correo electrónico al área de Medios Tecnológicos con copia a Operaciones, solicitando la autorización correspondiente. Excepción a esto, los equipos de seguridad en la central de monitoreo y las cámaras funcionarán de manera continua, 24 horas al día, los 7 días de la semana.
- Estos mecanismos de control y seguridad por disposición de la Gerencia y la Dirección de Medios Tecnológicos se implementarán a partir de la fecha y será notificado a cada uno de los trabajadores.

Publíquese y cúmplase, se firma a los 04 días del mes de marzo del 2026

RICARDO ROMERO BAYONA
Representante Legal