# D-G5-01 MANUAL INTERNO DE POLÍTICAS Y PROCEDIMIENTOS PARA LA SEGURIDAD DE LA INFORMACIÓN

## CONTROL DE CAMBIOS

| Versión | Fecha de Aprobación | Descripción de los cambios realizados |
|---|---|---|
| 1 | 3/11/2023 | Creación del documento |
| 2 | 27/03/2025 | Modificación de estructura, redacción y conceptos |

## CONTROL DE APROBACIONES

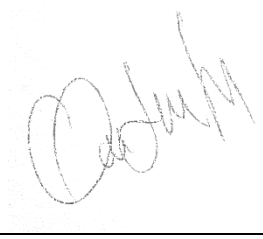
| ELABORACIÓN | | REVISIÓN | | APROBACIÓN | |
|---|---|---|---|---|---|
| **Nombre:** | Cristhian Oviedo | **Nombre:** | Diana Puerto | **Nombre:** | Diana Puerto |
| **Cargo:** | Asistente Soporte TI | **Cargo:** | Gerente | **Cargo:** | Gerente |
| **Firma:** |  | **Firma:** |  | **Firma:** |  |

**TABLA DE CONTENIDO**

## 1 OBJETIVO

Establecer políticas de seguridad de la información en MPI LOGÍSTICA S.A.S., con el propósito de garantizar la confidencialidad, integridad y disponibilidad de la información, así como proteger los activos y recursos de la organización frente a amenazas y riesgos de seguridad.

## 2 ALCANCE

Las políticas de seguridad de la información se aplican a todos los empleados, contratistas, socios comerciales y terceros que accedan a los sistemas y datos de MPI LOGÍSTICA S.A.S. Asimismo, abarcan todos los dispositivos y recursos vinculados a la infraestructura tecnológica de la organización.

## 3 DEFINICIONES

- **Seguridad Informática**: La práctica de proteger sistemas, redes, datos y dispositivos contra amenazas, ataques y accesos no autorizados para garantizar la confidencialidad, integridad y disponibilidad de la información.
- **Confidencialidad**: El principio de seguridad que asegura que la información sensible se mantiene privada y solo se comparte con personas autorizadas.
- **Integridad de Datos**: La garantía de que la información no ha sido alterada de manera no autorizada y que se conserva de manera precisa y completa.
- **Disponibilidad**: La propiedad que garantiza que los sistemas y datos críticos están disponibles y accesibles cuando se necesitan, minimizando el tiempo de inactividad.
- **Autenticación**: El proceso de verificar la identidad de un usuario, generalmente a través de credenciales como contraseñas, tarjetas de acceso o biometría.
- **Autorización**: El proceso de otorgar permisos específicos a usuarios o sistemas para acceder a recursos o realizar acciones dentro de un entorno informático.
- **Firewall**: Un sistema de seguridad que controla y filtra el tráfico de red entrante y saliente para proteger la red de amenazas y ataques no deseados.
- **Malware**: Software malicioso diseñado para dañar, robar o acceder de manera no autorizada a sistemas o datos, incluyendo virus, gusanos, troyanos y ransomware.
- **Phishing**: Una técnica de ingeniería social que implica el uso de correos electrónicos, sitios web o mensajes falsos para engañar a las personas y obtener información confidencial, como contraseñas o datos bancarios.
- **Política de Seguridad Informática**: Un conjunto de directrices, reglas y procedimientos diseñados para establecer y mantener un entorno seguro de tecnología de la información, protegiendo la organización contra amenazas cibernéticas.
- **CCTV**: **CCTV** (siglas en inglés de *Closed-Circuit Television*, o *Televisión de Circuito Cerrado*) es un sistema de videovigilancia que utiliza cámaras para transmitir señales de video a un número limitado de monitores o dispositivos de grabación, con el fin de supervisar, proteger y registrar actividades en áreas específicas.

## 4 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

MPI LOGISTICA SAS. reconoce la importancia de la seguridad de la información, así como la

necesidad de su protección para constituir un activo estratégico dentro de la organización y todas las partes interesadas, es por esto que la organización encamina los esfuerzos de los colaboradores y recurso técnico, para preservar la información y conservar la confidencialidad, integridad y disponibilidad de los activos de información, protegiendo y asegurando en el ciberespacio, los datos, sistemas y aplicaciones que son esenciales para la operación de la empresa.

MPI LOGÍSTICA S.A.S. se compromete a establecer los controles necesarios para alcanzar los objetivos definidos en el presente **Manual de Políticas de Seguridad de la Información.**

## 5 PRINCIPIOS DE SEGURIDAD

- **Confidencialidad**: Proteger la información confidencial de la empresa.
- **Integridad**: Mantener la integridad de los datos y sistemas.
- **Disponibilidad**: Garantizar la disponibilidad de sistemas y recursos críticos.
- **Cumplimiento**: Cumplir con las leyes y regulaciones aplicables.
- **Gestión de Riesgos**: Identificar y gestionar proactivamente los riesgos de seguridad.

## 6 POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

### 6.1 POLITICA DE ACCESO

La política de acceso de MPI LOGÍSTICA S.A.S. tiene como objetivo establecer las pautas y regulaciones necesarias para asegurar un acceso adecuado y seguro a los sistemas, recursos y datos de la organización, garantizando la confidencialidad, integridad y disponibilidad de la información crítica de la empresa.

**Los usuarios son responsables de:**

1. Los usuarios deberán utilizar exclusivamente las credenciales y los métodos de autenticación proporcionados y autorizados por el área TI para el acceso a sistemas, plataformas, redes y equipos de cómputo corporativos.

2. Los usuarios deben verificar el entorno de trabajo antes de ingresar credenciales, asegurándose de que el dispositivo sea confiable, la red esté protegida, evitando redes Wi-Fi públicas, utilizando VPN, revisando que no exista software sospechoso en ejecución y que no esté en presencia de personas no autorizadas cerca, que puedan observar la información.

3. Los usuarios deben mantener contraseñas seguras de acuerdo con lo descrito en el instructivo **Creación de Credenciales Seguras**.

4. Los usuarios deberán acceder exclusivamente a los sistemas, aplicaciones, plataformas y conjuntos de datos que sean estrictamente necesarios para el desarrollo de sus funciones laborales

5. Los usuarios deberán salvaguardar las credenciales de acceso proporcionadas por el área de TI y notificar de inmediato cualquier pérdida, robo o uso no autorizado al equipo de soporte técnico, mediante el correo electrónico “soportetecnico@mpilogistica.com”.

6. Utilizar un entorno de conexión seguro para el acceso remoto, a través de la VPN proporcionada por el área de TI.

**Área TI Es responsable de:**

1. Crear, modificar e inactivar las cuentas de usuario conforme al ingreso, traslado o retiro de los colaboradores, aplicando lo establecido en el instructivo **Creación de Credenciales Seguras**.
2. Configurar y mantener VPN para el acceso remoto seguro.
3. Atender los reportes de los usuarios sobre sospechas o amenazas de acceso no autorizado y registrarlo en el **Registro de Incidentes Sobre los Sistemas de Información**

### 6.2 POLÍTICAS DE SEGURIDAD FÍSICA

Garantizar la protección de los activos físicos de MPI LOGÍSTICA S.A.S., incluyendo la infraestructura tecnológica, equipos, y datos, mediante la implementación de medidas de seguridad física que prevengan el acceso no autorizado, daños a la infraestructura y cualquier interferencia con la información crítica de la organización.

1. Se requiere seguir el procedimiento **Proceso Para Acceso A Las Instalaciones** para el trámite de autorización de ingreso de personal propio, contratistas, terceros y visitantes.
2. Las áreas que contienen información sensible como servidores y centros de datos son consideradas por la organización como áreas críticas, para tener acceso a ellas, debe contar con la autorización y acompañamiento del área de TI.
3. El equipo de TI es responsable de supervisar y gestionar la implementación de controles de seguridad física cómo son sistemas CCTV, control de acceso y de seguridad, así como de realizar inspecciones registradas en el programa de mantenimiento.
4. Se mantendrá un registro de control de acceso que registre la entrada y salida de personal visitante a las instalaciones, el cual está documentado en el formato **Planilla De Control De Ingreso De Visitantes Y Contratistas**
5. Las cámaras de seguridad se instalarán en lugares estratégicos para garantizar la vigilancia y grabación adecuada en diferentes áreas de la Organización.
6. Se brindarán capacitaciones en seguridad física a los empleados, con el objetivo de fortalecer la conciencia, la responsabilidad y las buenas prácticas en la protección de personas, recursos, equipos instalaciones.
7. Todo traslado de activos fijos, como equipos de cómputo o dispositivos de almacenamiento que contengan información propiedad de la compañía, deberá ser notificado previamente a través de los correos electrónicos soportetecnico@mpilogistica.com y diana.puerto@mpilogistica.com informando al área de Tecnología y a la Gerencia.

### 6.3 POLÍTICAS DE SEGURIDAD DE RED

El objetivo de esta política es establecer las pautas y regulaciones necesarias para garantizar la seguridad de la red de MPI LOGÍSTICA S.A.S., minimizando el riesgo de acceso no autorizado, interferencias o intervenciones por parte de terceros en los sistemas de la compañía. Como parte de estos lineamientos, se establecen las siguientes disposiciones:

1. El área de TI deberá configurar reglas de filtrado web en el firewall y la seguridad de red UTM.

2. El área de TI debe establecer mapeo de la red interna mediante máscaras de IP.

3. El área de TI debe mantener los dispositivos de red, sistemas operativos y software actualizados con las últimas versiones y parches de seguridad.

4. El área de TI debe realizar monitoreo de la red para detectar y responder a actividades inusuales o potencialmente maliciosas.

5. El área de TI debe seguir el plan de recuperación de desastres para restaurar la red **Plan De Recuperación De La Red** en caso de un fallo o incidente de seguridad.

6. Los usuarios deben hacer uso de la VPN para conexiones fuera de la red de MPI LOGISTICA SAS.

## 6.4 POLÍTICAS DE SEGURIDAD DE DISPOSITIVOS MÓVILES

La política de seguridad de dispositivos móviles de MPI LOGISTICA SAS tiene como objetivo proteger la información de la empresa y minimizar los riesgos asociados con el uso de dispositivos móviles. La empresa se asegura de que el uso de estos dispositivos sea seguro y apropiado, manteniendo la confidencialidad, integridad y disponibilidad de sus datos.

1. Los colaboradores deben utilizar los dispositivos móviles de manera responsable y exclusivamente con fines laborales o autorizados por la gerencia.

2. Los usuarios deben mantener los dispositivos móviles en óptimas condiciones, limpios, protegidos contra caídas y daños utilizando accesorios que permitan conservar el estado de los dispositivos.

3. El área de TI debe configurar contraseñas seguras y utilizar la autenticación de múltiples factores para proteger los dispositivos en caso de que las aplicaciones cuenten con esta tecnología.

4. Los usuarios deben mantener el sistema operativo y las aplicaciones en dispositivos móviles actualizados con los últimos parches de seguridad.

5. En caso de detectar amenazas de seguridad y actividades inusuales en dispositivos móviles los usuarios deben reportar al área TI mediante correo electrónico “soportetecnico@mpilogistica.com” o acercándose a las oficinas administrativas.

6. Los usuarios deben Informar de inmediato cualquier pérdida, robo relacionado con dispositivos móviles al área de talento humano o al equipo TI.

## 6.5 POLÍTICAS DE CAPACITACIÓN Y CONCIENTIZACIÓN

Con el objetivo de reducir la vulnerabilidad de nuestros colaboradores ante ataques de ingeniería social, buscamos mantener una capacitación continua en el ámbito de seguridad informática. Esto nos permitirá estar preparados para actuar efectivamente en situaciones de este tipo.

1. La organización se compromete a fomentar una cultura de seguridad informática entre todos los empleados. Se proporcionará formación y recursos para aumentar la concientización sobre las amenazas y buenas prácticas de seguridad de la información.

2. Todos los empleados deberán participar en programas regulares de formación en seguridad

informática para estar al tanto de las últimas amenazas y soluciones de seguridad.

### 6.6 PÓLITICA DE COPIAS DE SEGURIDAD

El objetivo es garantizar la disponibilidad y la integridad de los datos críticos de MPI LOGISTICA SAS. A través de la implementación de procedimientos y estrategias de respaldo, se busca proteger la información importante contra la pérdida, el robo, el daño o la corrupción. Esto asegura que, en caso de fallos técnicos, desastres naturales o incidentes cibernéticos, la empresa pueda recuperar sus datos y mantener la continuidad de sus operaciones sin interrupciones significativas.

1. El área de TI será la encargada de supervisar y realizar seguimiento de las copias de seguridad de la información almacenada en el disco duro de cada equipo de cómputo.

2. Los usuarios son los responsables de realizar las copias de seguridad de la información almacenada en el disco duro de su equipo de cómputo y de la información adicional necesaria para la continuidad de su actividad laboral con una periodicidad semanal de acuerdo a los lineamientos descritos en el Instructivo **Copias De Seguridad Para Equipo De Cómputo**.

3. El área TI es responsable de mantener actualizado y socializado el instructivo **Copias De Seguridad Para Equipo De Cómputo**.

4. Los usuarios son los responsables de identificar y salvaguardar la información que requieran mediante el uso de copias de seguridad si los datos cumplen con al menos uno de los siguientes criterios:

- La pérdida de esta información interrumpiría procesos operativos clave
- La pérdida de esta información afectaría la capacidad de cumplir con servicios, entregas o actividades esenciales
- Existen requerimientos legales o normativos que exijan conservar esta información
- Está sujeta a auditorías o revisiones externas
- Es información necesaria para la planeación, análisis o dirección de la empresa
- La información cambia con frecuencia y necesita respaldarse regularmente para evitar pérdida de datos recientes
- Incluye información relacionada con transacciones, contratos, pagos o compromisos con terceros
- Su divulgación no autorizada podría comprometer la reputación, seguridad o ventaja competitiva de la organización
- La recuperación o reproducción de esta información, en caso de pérdida, representaría un alto costo operativo y logístico para la organización
- Otros sistemas o procesos dependen directamente de esta información para funcionar correctamente

5. Será responsabilidad del área de TI velar porque los proveedores tecnológicos implementen y mantengan mecanismos de respaldo de la información de todos los sistemas utilizados por la

organización, con una frecuencia máxima de 24 horas, garantizando la disponibilidad y conservación de los datos corporativos.

6. El área de TI realizara las copias de seguridad de los sistemas de información de la compañía SIESA, QUICK y NAS con una periodicidad no mayor a 24 horas. Las copias de seguridad se almacenarán en el servidor y adicional una copia fuera de las instalaciones ubicada en la residencia del responsable de TI de la organización para mitigar riesgos de desastres naturales o incidentes locales.

7. Se realizarán pruebas regulares no mayores a tres meses de restauración de datos para garantizar que las copias de seguridad sean efectivas y se puedan recuperar los datos de manera oportuna en caso de incidentes.

8. El área de TI, en coordinación con la Gerencia, deberá gestionar proactivamente los volúmenes de almacenamiento disponibles, garantizando la capacidad necesaria para la realización oportuna y continua de las copias de seguridad.