1. OBJETIVO

Establecer directrices y prácticas que garanticen la protección integral de la infraestructura de tecnología de la información (TI) y los datos de la empresa contra amenazas cibernéticas. Esta política tiene como objetivo principal salvaguardar la confidencialidad, integridad y disponibilidad de la información, así como promover un entorno seguro y consciente de ciberseguridad para todos los colaboradores. Además, busca asegurar el cumplimiento de la normativa legal vigente y la satisfacción de las necesidades de las partes interesadas en materia de seguridad informática.

2. ALCANCE

La Política de Ciberseguridad de Maestri On Track abarca todas las operaciones y actividades relacionadas con la infraestructura de tecnología de la información (TI) de la empresa. Incluye a todos los colaboradores, contratistas y terceros que interactúan con los sistemas y datos de la organización. Esta política se aplica a nivel interno y externo, cubriendo aspectos que afectan la seguridad de la información, la infraestructura de TI y el uso de recursos tecnológicos.

3. DEFINICIONES

- ✓ **Ciberseguridad:** La práctica de proteger sistemas informáticos, redes, programas y datos de ataques, daños o accesos no autorizados.
- ✓ **Seguridad de la Información:** La preservación de la confidencialidad, integridad y disponibilidad de la información.
- ✓ **Datos Sensibles:** Información que requiere una protección especial debido a su naturaleza confidencial, como datos personales, financieros o estratégicos de la empresa.
- ✓ **Contraseña:** Secuencia de caracteres utilizada para autenticar a un usuario y acceder a sistemas o datos.
- ✓ **Credenciales:** Combinación de usuario y contraseña que otorgan acceso a sistemas o aplicaciones.
- ✓ **Actualizaciones de Software:** Parches, correcciones y nuevas versiones de software diseñadas para mejorar la seguridad y el rendimiento.
- ✓ **Copia de Seguridad:** Una réplica de los datos críticos almacenados en un lugar seguro, utilizada para recuperación en caso de pérdida o daño.
- ✓ **Seguridad en el Puesto de Trabajo:** Prácticas y políticas destinadas a garantizar la seguridad de los dispositivos y estaciones de trabajo utilizados por los empleados.

- ✓ **Correo Electrónico Seguro:** Normas y pautas para el uso seguro del correo electrónico, incluyendo la identificación de correos electrónicos de phishing y la gestión de archivos adjuntos peligrosos.

- ✓ **Red Inalámbrica (WiFi) Segura:** Normas para el uso seguro de redes inalámbricas, incluyendo la autenticación y la protección contra amenazas.

4. RESPONSABILIDADES

- ✓ **Alta Dirección y Junta Directiva:**

  - Establecer una cultura de ciberseguridad en toda la organización.
  - Aprobar y respaldar las políticas de ciberseguridad.
  - Proporcionar los recursos necesarios para la implementación de medidas de seguridad efectivas.

- ✓ **Coordinador de Sistemas Informáticos:**

  - Desarrollar, implementar y mantener la Política de Ciberseguridad.
  - Supervisar y coordinar actividades relacionadas con la seguridad de la información.
  - Comunicar oportunamente información sobre amenazas de ciberseguridad identificadas a las partes interesadas correspondientes.

- ✓ **Responsables de Departamento:**

  - Implementar y hacer cumplir las políticas de ciberseguridad en sus áreas.
  - Supervisar que los empleados sigan las prácticas de seguridad adecuadas.
  - Informar sobre incidentes de seguridad al equipo de seguridad de la información.

- ✓ **Empleados:**

  - Cumplir con las políticas de ciberseguridad y las prácticas seguras.
  - Notificar inmediatamente cualquier incidente o vulnerabilidad que detecten.

- ✓ **Recursos Humanos:**

  - Administrar los procedimientos de ingreso y salida de empleados, incluyendo la gestión de contraseñas y cuentas.
  - Proporcionar capacitación en ciberseguridad a los empleados nuevos y existentes.

- ✓ **Auditoría Interna:**

  - Realizar auditorías regulares para evaluar el cumplimiento de la Política de Ciberseguridad y las prácticas de seguridad en toda la organización.

- Informar sobre hallazgos y áreas de mejora.

✓ **Proveedores y Terceros:**

- Cumplir con los requisitos de seguridad establecidos en los contratos y acuerdos de servicio.
- Informar sobre cualquier incidente de seguridad que pueda afectar a Maestri On Track.

5. POLITICAS INDIVIDUALES

5.1. Protección de Datos

Maestri On Track se enfoca en garantizar que todos los datos personales recopilados y procesados en nuestras operaciones sean manejados de manera ética, legal y segura, en conformidad con las regulaciones de privacidad aplicables. Esto implica asegurar la limitación de la recopilación de datos a lo estrictamente necesario, el cumplimiento legal y regulatorio, la implementación de medidas de seguridad para proteger los datos, la retención adecuada de información y el respeto de los derechos de las personas cuyos datos manejamos. La política también aborda la formación en privacidad y la respuesta a incidentes de seguridad, asegurando la integridad y confidencialidad de los datos y cumpliendo con las leyes de protección de datos en todas las jurisdicciones en las que operamos.

5.2. Contraseñas

Maestri On Track se centra en garantizar la seguridad y confidencialidad de las contraseñas utilizadas en nuestra empresa. Esto es aplicable a todos los empleados y usuarios que requieren acceso a sistemas y recursos protegidos por contraseñas.

Esta política establece pautas clave para el manejo de contraseñas:

✓ **Creación de Contraseñas Seguras:** Las contraseñas deben ser lo más seguras posible, utilizando combinaciones de letras mayúsculas, minúsculas, números y caracteres especiales. Evitando contraseñas predecibles y fáciles de adivinar.

✓ **Cambio Regular de Contraseñas:** La contraseña inicial de acceso debe ser cambiada la primera vez que acceda al sistema, además, debe ser cambiada mínimo cada 6 meses, o cuando se considere necesario debido a alguna vulnerabilidad en los criterios de seguridad. No se permite el uso de contraseñas antiguas. Es fundamental llevar a cabo este proceso de manera coordinada con el equipo de sistemas informáticos.

La seguridad de las contraseñas es responsabilidad de todos en Maestri On Track. Los empleados deben seguir estas directrices y colaborar para proteger la información y los recursos de la empresa. El equipo de TI supervisará y aplicará esta política, gestionando la administración de contraseñas y asegurando que se cumplan todas las directrices.

Los empleados también deben cerrar sesión o bloquear sus dispositivos cuando no estén en uso para evitar accesos no autorizados. Asimismo, es fundamental que se notifiquen de inmediato cualquier sospecha de violación de seguridad o pérdida de contraseñas para que se puedan tomar medidas rápidas y adecuadas.

5.3. Actualizaciones

Nuestra empresa reconoce la importancia crítica de mantener nuestros sistemas de información seguros y al día. Para lograrlo, hemos establecido la Política de Actualizaciones de Maestri On Track, que establece las siguientes directrices:

- ✓ **Monitoreo Permanente:** Mantendremos un monitoreo constante de las correcciones, actualizaciones y parches proporcionados por los fabricantes de software y sistemas operativos que utilizamos en toda la organización. Esto nos permitirá estar al tanto de las últimas soluciones de seguridad y mejoras de rendimiento.

- ✓ **Implementación Inmediata:** Tan pronto como estén disponibles, implementaremos las actualizaciones críticas y parches. La rapidez en la implementación es esencial para garantizar que nuestras defensas estén alineadas con las amenazas de seguridad más recientes.

- ✓ **Actualizaciones Automáticas:** Se recomienda encarecidamente que todos los dispositivos y sistemas habiliten las actualizaciones automáticas siempre que sea posible. Esto asegura que las actualizaciones esenciales se apliquen de manera oportuna sin depender de intervenciones manuales, reduciendo así la ventana de exposición a posibles riesgos.

- ✓ **Exploración de Vulnerabilidades:** Se realizarán regularmente exploraciones de vulnerabilidades en sistemas y software para identificar posibles riesgos. Las medidas correctivas se aplicarán de manera inmediata.

- ✓ **Responsabilidad Compartida:** Todos los empleados y usuarios de Maestri On Track son responsables de cumplir con esta política. El equipo de TI supervisará y aplicará estas directrices, asegurando que las actualizaciones se realicen de acuerdo con los procedimientos establecidos.

5.4. Almacenamiento y copias de Seguridad

En Maestri On Track, asumimos el compromiso de salvaguardar la integridad y disponibilidad de nuestros activos de información. Nuestra Política de Almacenamiento y Copias de Seguridad se rige por los siguientes principios:

- ✓ **Planificación de Copias de Seguridad:** Determinaremos la frecuencia de las copias de seguridad considerando la naturaleza crítica de los datos y la velocidad requerida de recuperación. Este proceso será coordinado con los responsables de los activos de información, y los detalles se documentarán de forma transparente y comprensible.

- ✓ **Designación de Responsables:** Nombraremos a personal autorizado y competente para gestionar las operaciones de copias de seguridad. Estos individuos serán los únicos con acceso a los datos respaldados y responsables de llevar a cabo restauraciones en caso necesario.

- ✓ **Procedimientos de Copias de Seguridad:** Estableceremos procedimientos detallados para realizar, almacenar y recuperar copias de seguridad. Todos los colaboradores deben seguir estos procesos de manera rigurosa.

- ✓ **Restricción de Acceso:** El acceso a los datos almacenados en copias de seguridad será restringido estrictamente al personal designado. La autenticación y autorización de los responsables de las copias de seguridad serán aplicadas para garantizar la seguridad de los datos respaldados.

5.5. Seguridad en el puesto de trabajo

La Seguridad en el Puesto de Trabajo es un componente fundamental de nuestra estrategia de seguridad de la información. Nuestra política, centrada en el bienestar de nuestros empleados y la salvaguardia de los recursos de TI, se rige por los siguientes principios:

- ✓ **Responsabilidades y Obligaciones del Personal:** Reconocemos que la seguridad en el puesto de trabajo es una tarea compartida. Cada empleado debe comprender y asumir sus responsabilidades en materia de seguridad, y la empresa se compromete a proporcionar la formación necesaria para fomentar este entendimiento.

- ✓ **Uso Ético y Adecuado de Recursos:** Fomentamos un uso ético y adecuado de los recursos tecnológicos en el trabajo. Esto implica un manejo seguro de ordenadores de sobremesa, portátiles, dispositivos móviles, impresoras, redes Wi-Fi y otros recursos tecnológicos proporcionados por la empresa.

- ✓ **Seguridad de Datos en el Puesto de Trabajo:** La confidencialidad de la información es de suma importancia. Esperamos que cada empleado participe en la preservación de la seguridad de los datos, evitando accesos no autorizados y garantizando la privacidad de la información.

- ✓ **Seguridad de Redes y Dispositivos Móviles:** Los dispositivos móviles, como smartphones y tablets, también son elementos clave de nuestro entorno laboral. Los empleados deben seguir directrices específicas para salvaguardar los datos almacenados o transmitidos a través de estos dispositivos.

- ✓ **Normas de Uso y Concienciación:** Estableceremos normas claras para el uso adecuado de los recursos tecnológicos y promoveremos la concienciación en seguridad informática. Esto incluye prácticas seguras para proteger las contraseñas, detectar correos electrónicos fraudulentos y prevenir amenazas cibernéticas.

5.6. Uso del correo electrónico

En Maestri On Track, la seguridad de la información es una prioridad. Nuestra Política de Seguridad del Correo Electrónico se establece para garantizar el uso adecuado de esta herramienta de comunicación y proteger a nuestra organización y empleados de riesgos y malos usos. Esta política se sustenta en los siguientes principios:

- ✓ **Normativa de Uso:** Establecemos pautas claras y reglas para el uso del correo electrónico. Todos los empleados deben cumplir con estas normas, que abarcan desde la comunicación interna hasta la correspondencia con partes externas.

- ✓ **Seguridad de Contenido:** Implementamos soluciones de seguridad, como aplicaciones antimalware y antispam, para proteger nuestra red y sistemas contra amenazas cibernéticas. La seguridad de contenido garantiza que los correos electrónicos no contengan malware ni spam.

- ✓ **Cifrado y Firma Digital:** Fomentamos el uso de cifrado y firma digital cuando sea necesario para proteger la confidencialidad y autenticidad de nuestros mensajes. Esto se aplica especialmente a comunicaciones con información sensible.

- ✓ **Seguridad del Contenido:** Para minimizar riesgos, desactivamos la visualización automática de contenido HTML y la descarga de imágenes desde fuentes externas. Esto previene la exposición a contenido potencialmente malicioso.

- ✓ **Uso Apropiado del Correo Corporativo:** Recordamos a nuestros empleados que el correo corporativo es un recurso de trabajo y, como tal, debe utilizarse de manera apropiada y profesional. Evitamos el envío de contenido no relacionado con el trabajo o de naturaleza ofensiva.

- ✓ **Contraseñas Seguras:** Para garantizar la seguridad, instamos a todos los empleados a utilizar contraseñas seguras y cambiarlas regularmente. El uso de contraseñas fuertes contribuye a proteger el acceso a las cuentas de correo electrónico.

- ✓ **Identificación de Correos Sospechosos:** Educamos a nuestros empleados sobre cómo identificar correos electrónicos sospechosos o posibles intentos de phishing. Esta capacitación mejora la seguridad y reduce el riesgo de ataques de suplantación de identidad.

- ✓ **Gestión de Enlaces:** Inspeccionamos y verificamos los enlaces incluidos en los correos electrónicos para evitar la exposición a sitios web maliciosos o fraudulentos. Esta medida adicional refuerza la seguridad de nuestros empleados.

5.7. Uso de Wifi

La movilidad es esencial en nuestro entorno laboral actual, y entendemos que nuestros empleados a menudo necesitan acceder a datos corporativos fuera de la oficina. Nuestra Política de Uso de Redes Inalámbricas (Wi-Fi) tiene como objetivo establecer las condiciones y circunstancias para el acceso remoto a servicios corporativos, garantizando la seguridad de los datos y la información de nuestra empresa.

Principales Directrices:

- ✓ **Acceso Autorizado:** El acceso a servicios corporativos a través de redes Wi-Fi externas solo está permitido a empleados autorizados. La autorización se otorga de acuerdo con la función y las necesidades laborales del empleado.

- ✓ **Seguridad de Red:** Cuando se accede a través de redes Wi-Fi externas, se requiere el uso de una Red Privada Virtual (VPN) para garantizar la confidencialidad y la integridad de los datos transmitidos.

- ✓ **Protección de Dispositivos:** Los empleados son responsables de garantizar que sus dispositivos estén protegidos con medidas de seguridad adecuadas, como contraseñas y actualizaciones de seguridad.

- ✓ **Normas de Uso:** Los empleados deben cumplir con las normas de uso de las redes Wi-Fi externas, incluida la prohibición de compartir información confidencial y la identificación de amenazas de seguridad potenciales.

- ✓ **Actualizaciones y Formación:** Maestri On Track proporcionará formación y recursos actualizados sobre el uso seguro de redes Wi-Fi externas a los empleados.

- ✓ **Información Confidencial:** Los empleados deben ser conscientes de que la política de confidencialidad se aplica en todo momento, incluso cuando se utilizan redes Wi-Fi externas.

5.8. Acceso Remoto

Para garantizar la seguridad y confidencialidad de los recursos de Maestri On Track, el acceso remoto a la infraestructura de tecnología de la información se realizará exclusivamente a través del Escritorio Remoto. Este método de conexión desde ubicaciones externas a las instalaciones físicas de la empresa es fundamental para mantener un entorno informático seguro.

Los empleados que requieran acceso remoto deben contar con credenciales de acceso autorizadas y únicas. Estas credenciales son proporcionadas por el departamento de sistemas informáticos y deben ser tratadas con la máxima confidencialidad.

Además, cualquier acceso remoto debe ser previamente reportado al área de sistemas informáticos. Este proceso garantiza un seguimiento adecuado, facilita la gestión de la seguridad y permite una respuesta rápida en caso de eventos inusuales o potenciales amenazas.

6. DISPOSICIONES FINALES

Esta Política de Ciberseguridad de Maestri On Track entrará en vigor a partir de la fecha de su aprobación. Esta política se revisará y actualizará periódicamente para garantizar su eficacia continua y su alineación con los cambios en las amenazas de seguridad cibernética y la normativa aplicable. Las actualizaciones y revisiones se comunicarán a todos los empleados y partes interesadas relevantes.

Los empleados de Maestri On Track son responsables de cumplir con las directrices y normas establecidas en esta política. El incumplimiento de esta política puede dar lugar a medidas disciplinarias según lo determine la alta dirección.

La seguridad cibernética es responsabilidad de todos los empleados. La empresa promoverá una cultura de concienciación y capacitación continua en seguridad para asegurar que todos los miembros del personal estén debidamente informados y preparados para enfrentar los desafíos de la ciberseguridad.

La alta dirección de Maestri On Track respalda plenamente esta política y se compromete a proporcionar los recursos necesarios para su implementación y cumplimiento. La seguridad cibernética es un aspecto crítico para la operación y la reputación de la empresa, y todos los empleados desempeñan un papel fundamental en su preservación.

Esta política y los procedimientos de ciberseguridad se revisarán al menos una vez al año y se actualizarán cuando se presenten cambios en el contexto interno o externo, o cuando se materialice algún riesgo. Cualquier consulta o aclaración con respecto a esta política puede dirigirse al departamento de sistemas informáticos.

7. ANTECEDENTES NORMATIVOS

- ✓ Ley 23 de 1993 y Ley 44 de 1993: Derechos de autor.
- ✓ Ley 679 de 2001 y Ley 1336 de 2009: Pornografía Infantil.
- ✓ Ley 1266 de 2008: Habeas Data.
- ✓ Ley 1273 de 2009: Delitos Informáticos.
- ✓ Ley 201 de 2012: Ley TLC.

- ✓ Ley 1581 de 2012: Protección de datos personales.
- ✓ Circular Externa 042 de 2012: Capitulo décimo segundo: Requerimientos
- ✓ mínimos de seguridad y calidad para la realización de operaciones.
- ✓ Circular Externa 007 de 2018: Requisitos mínimos para la gestión de riesgos de Ciberseguridad.

Control de Cambios		
Versión	**Fecha de Entrada en Vigencia**	**Naturaleza del cambio**
1	El documento entra en vigencia a partir de su publicación en el SIG.	Creación del documento en el SIG

Ruta de Aprobación					
Elaboró		**Revisó**		**Aprobó**	
Nombre	Carlos Leonardo Maje Ríos	**Nombre**		**Nombre**	
Cargo	Coordinador de Sistemas Informáticos	**Cargo**		**Cargo**	