POLÍTICA DE USO ACEPTABLE DE RECURSOS TECNOLÓGICOS

Campo	Dato
Código	MDC-PUART-01
Versión	1
Fecha de emisión	Junio 2026
Elaborado por	Director Comercial y TI
Revisado por	Control Interno y Responsable BASC
Aprobado por	Gerente General
Ciudad	Barrancabermeja, Colombia

CONFIDENCIALIDAD

Este documento es de carácter interno y contiene lineamientos de obligatorio cumplimiento para todos los colaboradores, contratistas y terceros de MADOCO XXI SAS BIC. Su uso está restringido a personal autorizado. Queda prohibida su reproducción o divulgación sin previa autorización de la organización.

1. OBJETIVO

Establecer los lineamientos y condiciones de uso aceptable de los recursos tecnológicos de MADOCO XXI SAS BIC — equipos de cómputo, dispositivos móviles, correo electrónico, plataformas de comunicación, almacenamiento en la nube, internet, software e Inteligencia Artificial — garantizando su uso responsable, la protección de la información corporativa y el cumplimiento del estándar BASC y la normativa vigente en Colombia.

2. ALCANCE

Esta política aplica a:

- Todos los recursos tecnológicos de propiedad de MADOCO XXI SAS BIC o administrados por la organización: equipos de cómputo, portátiles, celulares corporativos, tablets, impresoras, servidores, redes y plataformas digitales.
- Todo el personal: colaboradores de todas las áreas, aprendices, practicantes, contratistas y terceros con acceso a recursos o información de la organización.
- El ecosistema Microsoft 365 completo: Exchange Online, Teams, SharePoint Online, OneDrive Empresarial, Microsoft Intune y Entra ID.
- El ERP Odoo, las redes corporativas (WiFi y LAN) y cualquier otra plataforma o herramienta tecnológica utilizada en la organización.
- Las sedes de Barrancabermeja (sede principal), Cartagena y Llanos.

3. DEFINICIONES

Término	Definición
Recurso tecnológico	Equipo, dispositivo, plataforma, red o herramienta de software propiedad o bajo administración de MADOCO XXI SAS BIC.
Uso aceptable	Utilización de los recursos tecnológicos para fines laborales autorizados, de forma responsable y conforme a esta política.
Uso no aceptable	Cualquier uso de los recursos tecnológicos para fines personales, ilegales, que represente riesgo de seguridad o que viole esta política.
Ecosistema Microsoft 365	Conjunto de plataformas corporativas: Exchange Online, Teams, SharePoint, OneDrive, Intune y Entra ID, operadas bajo el tenant madoco21.com.
Software autorizado	Aplicación o programa cuya instalación y uso ha sido aprobado formalmente por el Departamento de TI.
Inteligencia Artificial (IA)	Herramienta de IA generativa autorizada por el Departamento de TI para apoyo en tareas laborales, bajo los lineamientos de uso responsable establecidos.
Incidente de seguridad	Evento que compromete o puede comprometer la confidencialidad, integridad o disponibilidad de los recursos o información de la organización.

4. MARCO NORMATIVO

- MDC-PGSI-01 — Política General de Seguridad de la Información.
- MDC-PCAGC-01 — Política de Control de Accesos y Gestión de Contraseñas.
- MDC-PUART-01 — Política de Uso Aceptable de Recursos Tecnológicos.
- Estándar BASC — Business Alliance for Secure Commerce, versión vigente.
- ISO/IEC 27001 — Seguridad de la Información (referencial).
- Ley 1273 de 2009 — Delitos informáticos en Colombia.
- Ley 1581 de 2012 — Protección de datos personales.
- Reglamento Interno de Trabajo de MADOCO XXI SAS BIC.

5. RESPONSABILIDADES

Rol	Responsabilidades
Director Comercial y TI (Duvan M. Pulido B.)	Definir y mantener esta política. Autorizar herramientas de IA y software. Gestionar incidentes derivados del uso indebido de recursos tecnológicos.
Departamento de TI	Implementar controles técnicos de uso aceptable. Autorizar software e instalaciones. Monitorear el cumplimiento. Gestionar y configurar el ecosistema Microsoft 365 e Intune.
Control Interno (Mónica Zambrano)	Verificar el cumplimiento de esta política. Reportar hallazgos de incumplimiento a la Dirección.
Líderes de Área	Promover el cumplimiento de esta política en su equipo. Reportar al Departamento de TI cualquier uso indebido detectado.
Todos los usuarios	Usar los recursos tecnológicos exclusivamente para fines laborales autorizados. Conocer, aceptar y cumplir esta política. Reportar incidentes al Departamento de TI.

6. USO DE EQUIPOS DE CÓMPUTO Y DISPOSITIVOS CORPORATIVOS

6.1 Principios generales

- Los equipos corporativos (computadores, portátiles, celulares, tablets) son herramientas de trabajo. Su uso es exclusivo para actividades laborales autorizadas.
- Cada colaborador es responsable del cuidado, custodia y buen uso del equipo asignado. El deterioro por mal uso puede generar responsabilidad económica.
- Los equipos corporativos son administrados por el Departamento de TI a través de Microsoft Intune. La empresa podrá realizar controles, revisiones y configuraciones remotas en cualquier momento.
- Al retiro del colaborador, el equipo debe devolverse en buen estado con todos sus accesorios, conforme al acta de entrega).

6.2 Seguridad obligatoria en equipos

- El bloqueo automático de pantalla debe estar activo en todo momento — máximo 5 minutos de inactividad. Al ausentarse del puesto, el colaborador debe bloquear o cerrar sesión manualmente.
- Está prohibido compartir el equipo o dejar sesiones activas en equipos de uso compartido o público.
- El cifrado de disco debe estar habilitado conforme a las políticas aplicadas vía Intune.
- Está prohibido desactivar, modificar o eludir cualquier control de seguridad configurado por el Departamento de TI.

6.3 Software e instalaciones

- Está prohibido instalar software, aplicaciones, extensiones o plugins que no hayan sido previamente autorizados por el Departamento de TI.
- Está prohibido el uso de software pirata, sin licencia, de origen desconocido o con condiciones de uso no verificadas.
- Cualquier solicitud de instalación de software debe realizarse a través del Departamento de TI, quien evaluará la pertinencia y el riesgo de seguridad.
- El Departamento de TI podrá desinstalar remotamente cualquier software no autorizado detectado en los equipos corporativos.

6.4 Dispositivos de almacenamiento externo

- El uso de memorias USB, discos externos u otros dispositivos de almacenamiento está restringido y requiere autorización previa del Departamento de TI.
- Todo dispositivo externo debe ser verificado por TI antes de su conexión a equipos corporativos.
- Está terminantemente prohibido transferir información corporativa confidencial a dispositivos externos no autorizados.
- El almacenamiento de información corporativa debe realizarse en OneDrive Empresarial o SharePoint Online dentro del tenant madoco21.com.

6.5 Equipos fuera de las instalaciones

- El uso de equipos corporativos fuera de las instalaciones debe hacerse con especial responsabilidad, evitando su exposición en lugares públicos o inseguros.
- Está prohibido conectarse a redes WiFi públicas o no seguras sin VPN corporativa para acceder a recursos internos.
- Las operaciones críticas (pagos, accesos a sistemas financieros, información confidencial) deben realizarse únicamente desde redes seguras de la empresa.
- Cualquier pérdida, robo o daño del equipo fuera de las instalaciones debe reportarse al Departamento de TI de forma inmediata.

6.6 Celulares corporativos

- El celular corporativo es una herramienta de trabajo. Su uso para fines personales no debe comprometer la seguridad, el rendimiento del equipo ni el plan de datos corporativo.
- El colaborador es responsable de la custodia del dispositivo y debe reportar de inmediato cualquier pérdida, robo o daño al Departamento de TI.
- Al retiro del colaborador, el celular debe devolverse con todos sus accesorios. El Departamento de TI realizará el borrado remoto del equipo antes de su reasignación.
- La SIM Card corporativa es propiedad de la empresa y debe ser devuelta junto con el equipo.

7. USO DEL CORREO ELECTRÓNICO Y CANALES DE COMUNICACIÓN

7.1 Correo electrónico corporativo

- El correo electrónico corporativo (@madoco21.com, gestionado por Exchange Online) es la vía oficial de comunicación externa e interna formal.
- El uso del correo corporativo es exclusivo para actividades laborales. Está prohibido su uso para fines personales, suscripciones no relacionadas con el trabajo o envío de contenido inapropiado.
- No se deben abrir enlaces ni archivos adjuntos de remitentes desconocidos o sospechosos. Ante cualquier duda, reportar al Departamento de TI antes de abrir.
- Está prohibido reenviar información confidencial o sensible a cuentas externas sin autorización del líder de área y del Departamento de TI.
- Está prohibido usar cuentas de correo personales (Gmail, Yahoo, Hotmail u otras) para gestionar asuntos laborales o enviar información corporativa.

7.2 Canales oficiales de comunicación

Con la migración completa al ecosistema Microsoft 365, los canales oficiales son:

Canal	Uso autorizado	Restricciones
Microsoft Teams	Comunicación interna, reuniones, colaboración en equipo	Canal oficial — uso prioritario para comunicación interna
Exchange Online (@madoco21.com)	Comunicación formal interna y externa	Canal oficial — para instrucciones, decisiones y aprobaciones
SharePoint / OneDrive	Gestión documental y colaboración en archivos	Único repositorio autorizado de documentos corporativos
WhatsApp	Comunicación informal y rápida	⚠ Solo informal. No válido para aprobaciones, instrucciones formales ni información sensible
Gmail / Google Chat	Ninguno para uso corporativo	✗ No autorizado. La organización migró completamente a Microsoft 365
Dropbox	Ninguno para uso corporativo	✗ No autorizado. Toda la información debe estar en OneDrive / SharePoint

Toda comunicación que implique instrucciones, decisiones, aprobaciones o información sensible debe realizarse exclusivamente por Teams o Exchange Online. Lo comunicado por WhatsApp que tenga carácter formal debe ser formalizado posteriormente por estos canales.

7.3 Buenas prácticas en comunicaciones

- No se debe compartir información confidencial por canales no autorizados (WhatsApp, redes sociales, plataformas externas).
- Ante la recepción de correos sospechosos, solicitudes de datos o intentos de phishing, reportar de inmediato al Departamento de TI sin hacer clic en ningún enlace.

- Las reuniones virtuales que involucren información sensible deben realizarse en Microsoft Teams con los controles de seguridad activos.

8. USO DEL ALMACENAMIENTO EN LA NUBE Y GESTIÓN DOCUMENTAL

- Toda la información corporativa debe almacenarse exclusivamente en SharePoint Online o OneDrive Empresarial dentro del tenant madoco21.com. Está prohibido el uso de Dropbox, Google Drive, iCloud u otros servicios de almacenamiento en la nube externos.
- La sincronización de OneDrive se limitará a carpetas específicas autorizadas por el Departamento de TI. Está prohibido sincronizar bibliotecas completas de SharePoint en equipos locales sin autorización.
- Está prohibido compartir documentos o carpetas de SharePoint con personas externas a la organización sin autorización previa del líder de área y del Departamento de TI.
- Los documentos corporativos no deben descargarse en dispositivos personales o almacenarse fuera del ecosistema Microsoft 365.

9. USO DE INTERNET

- El acceso a internet desde la red corporativa es para uso laboral. La navegación personal está permitida en horarios no laborales y sin comprometer la seguridad o el rendimiento de la red.
- Está prohibido acceder, descargar o distribuir contenido ilegal, pornográfico, violento, discriminatorio o que represente un riesgo de seguridad para la organización.
- Está prohibido acceder a plataformas de torrents, sitios de descarga ilegal o servicios de streaming no autorizados desde la red corporativa.
- El firewall Fortinet aplica filtrado de contenido. Toda navegación en la red corporativa puede ser monitoreada por el Departamento de TI conforme a las necesidades de seguridad de la organización.
- El acceso a recursos corporativos desde redes externas debe realizarse siempre mediante VPN corporativa.

10. USO RESPONSABLE DE INTELIGENCIA ARTIFICIAL (IA)

10.1 Principios generales

- La Inteligencia Artificial es una herramienta de apoyo, no un sustituto del criterio humano. Toda información generada con IA debe ser revisada, validada y aprobada por el responsable del proceso.
- Solo se podrán utilizar herramientas de IA previamente autorizadas por el Departamento de TI. No está permitido el uso de múltiples IAs sin control, versiones no licenciadas o servicios de origen desconocido.
- Ante cualquier duda sobre el uso de una herramienta de IA, consultar al Departamento de TI antes de utilizarla.

10.2 Información prohibida en herramientas de IA

Está estrictamente prohibido ingresar a cualquier herramienta de IA la siguiente información:

- Contraseñas, usuarios o credenciales reales de cualquier sistema.
- Información financiera sensible: estados financieros, NIT, cuentas bancarias, facturación, nómina.
- Bases de datos de clientes, proveedores o contactos comerciales.
- Información estratégica, contratos, precios confidenciales o negociaciones en curso.
- Datos personales sensibles de colaboradores o terceros.

- Configuraciones reales de sistemas, backups o llaves de seguridad.

Regla práctica: si la información no se puede enviar por correo externo, tampoco se puede enviar a una herramienta de IA.

10.3 Usos permitidos y no permitidos por área

Área	Usos permitidos	Usos no permitidos
Comercial	Redacción de propuestas, mejora de correos y presentaciones, argumentos de venta.	Precios reales, información de clientes, contratos, estrategias comerciales sensibles.
Contabilidad	Consultas conceptuales contables o tributarias, estructura de informes, explicaciones normativas.	Estados financieros reales, NIT, cuentas bancarias, información del ERP Odoo.
Marketing	Ideas para contenido, textos publicitarios, mejora de redacción y organización.	Bases de datos de clientes, información estratégica de campañas, material confidencial sin anonimizar.
Producción y Calidad	Documentación de procesos, mejora de instrucciones, análisis general de riesgos.	Planos técnicos críticos, procesos propietarios, fórmulas o información que represente ventaja competitiva.
Diseño	Ideas conceptuales, referencias visuales, apoyo en redacción técnica descriptiva.	Archivos finales, diseños propietarios, planos de fabricación, información técnica sensible.
HSEQ	Redacción de procedimientos, análisis preliminar de riesgos, estructura de planes.	Reportes reales de incidentes, datos personales del personal, evidencias de auditorías.
Talento Humano	Redacción de políticas, mejora de perfiles de cargo, apoyo en planes de capacitación.	Datos personales reales, hojas de vida, nómina, evaluaciones, información médica.
TI / Sistemas	Documentación técnica, análisis de riesgos, borradores de políticas, preparación BASC.	Usuarios, contraseñas, configuraciones reales, backups, datos productivos, llaves de seguridad.
Gerencias y Dirección	Redacción de comunicados, organización de ideas y documentos internos.	Información estratégica sensible, decisiones críticas sin análisis adicional.

11. USO DEL ERP ODOO

- El acceso al ERP Odoo es por usuario y contraseña individuales conforme al cargo y módulos asignados. Está prohibido compartir credenciales de acceso al ERP.
- Cada usuario solo tiene acceso a los módulos y datos correspondientes a sus funciones, conforme al principio de mínimo privilegio.
- Está prohibido extraer, exportar o compartir información del ERP Odoo con herramientas de IA, servicios externos o personas no autorizadas.
- Los cambios en permisos o módulos del ERP deben ser solicitados formalmente al Departamento de TI por el líder de área.
- Toda acción en el ERP queda registrada en los logs del sistema para fines de auditoría y trazabilidad BASC.

12. INCUMPLIMIENTO Y SANCIONES

El incumplimiento de esta política constituye una falta de seguridad y será tratado conforme a lo establecido en la TI-POL-001 y el Reglamento Interno de Trabajo. Las sanciones van desde amonestación escrita hasta terminación del contrato, según la gravedad. Los incidentes que constituyan delito informático conforme a la Ley 1273 de 2009 serán reportados a las autoridades competentes.

Conductas que generan sanción inmediata:

- Instalar software no autorizado o software pirata en equipos corporativos.
- Transferir información corporativa confidencial a servicios de almacenamiento externos no autorizados (Dropbox, Google Drive, etc.).
- Ingresar información confidencial de la organización a herramientas de IA no autorizadas.
- Usar cuentas de correo personales para gestionar información corporativa sensible.
- Acceder a contenido ilegal, pornográfico o malicioso desde equipos o redes de la empresa.
- No reportar la pérdida o robo de un equipo corporativo de forma inmediata.
- Compartir credenciales de acceso al ERP Odoo, Microsoft 365 o cualquier sistema corporativo.

13. REVISIÓN Y ACTUALIZACIÓN

Esta política será revisada anualmente o cuando se presenten cambios significativos en la tecnología, en los sistemas de información, en los requisitos del estándar BASC o en la normativa colombiana aplicable. Las actualizaciones serán aprobadas por la Gerencia General y comunicadas a todo el personal mediante los canales oficiales.

CONTROL DE CAMBIOS

Versión	Fecha	Descripción	Responsable	Aprobó
1.0	Junio 2026	Creación inicial del documento	Duvan Manuel Pulido Bautista	Martha Domínguez Correa