POLÍTICA DE CONTROL DE ACCESOS Y GESTIÓN DE CONTRASEÑAS

Campo	Dato
Código	MDC-PGSI-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 críticos de seguridad de la información de MADOCO XXI SAS BIC. Su uso está restringido a personal autorizado. Queda prohibida su reproducción, distribución o divulgación sin previa autorización de la organización.

1. OBJETIVO

Establecer los lineamientos y controles para la gestión segura de accesos e identidades en todos los sistemas de información de MADOCO XXI SAS BIC, definiendo los requisitos mínimos para la creación, administración y protección de contraseñas, la asignación de privilegios, el uso de autenticación multifactor y la correcta gestión del ciclo de vida de los usuarios, garantizando el cumplimiento del estándar BASC y la protección de los activos de información de la organización.

2. ALCANCE

Esta política aplica a:

- Todos los sistemas de acceso corporativo: Microsoft 365 (Entra ID, Exchange Online, SharePoint Online, OneDrive, Teams), ERP Odoo, red corporativa (WiFi y LAN) y cualquier otro sistema o plataforma de la organización.
- Todo el personal: colaboradores, aprendices, practicantes, contratistas y terceros con acceso a sistemas de MADOCO XXI SAS BIC.
- Todos los dispositivos corporativos inscritos en Microsoft Intune y administrados por el Departamento de TI.
- Las sedes de Barrancabermeja (sede principal), Cartagena y Llanos.

3. DEFINICIONES

Término	Definición
Credencial	Combinación de usuario y contraseña que permite autenticar a una persona en un sistema.
Contraseña segura	Contraseña que cumple con los criterios mínimos de longitud, complejidad y unicidad definidos en esta política.
MFA / 2FA	Autenticación multifactor o de dos pasos: mecanismo que exige un segundo factor de verificación además de la contraseña.
Privilegio mínimo	Principio por el cual cada usuario recibe únicamente los accesos necesarios para realizar sus funciones.
Cuenta privilegiada	Cuenta con permisos administrativos sobre sistemas, plataformas o datos críticos de la organización.
Portal cautivo	Mecanismo de autenticación en la red WiFi que solicita credenciales o voucher antes de otorgar acceso a internet.
VLAN	Red de área local virtual que segmenta el tráfico de red para aislar grupos de dispositivos por tipo o función.
Entra ID	Servicio de gestión de identidades y accesos de Microsoft (antes Azure AD), utilizado como directorio central de usuarios corporativos.

Cuenta suspendida	Cuenta bloqueada que no permite inicio de sesión, aplicada inmediatamente ante retiro o incidente de seguridad.

4. MARCO NORMATIVO

Esta política se articula con los siguientes documentos y marcos:

- MDC-PGSI-01— Política General de Seguridad de la Información
- MDC-P-GUDAM-01— Procedimiento de Gestión de Usuarios, Dispositivos y Accesos en Microsoft 365.
- Estándar BASC — Business Alliance for Secure Commerce, versión vigente.
- ISO/IEC 27001 — Gestión de Seguridad de la Información (referencial).
- Ley 1273 de 2009 — Delitos informáticos en Colombia.
- Ley 1581 de 2012 — Protección de datos personales.

5. RESPONSABILIDADES

Rol	Responsabilidades en materia de accesos y contraseñas
Director Comercial y TI	Definir y mantener esta política. Supervisar la implementación de controles de acceso. Autorizar cuentas privilegiadas y excepciones. Gestionar incidentes relacionados con accesos.
Area de TI	Crear, modificar y bloquear cuentas. Administrar grupos de seguridad en Entra ID. Configurar MFA. Auditar accesos periódicamente. Gestionar el portal cautivo y las VLANs.
Control Interno	Verificar el cumplimiento de esta política. Revisar periódicamente los registros de acceso. Reportar hallazgos de incumplimiento.
Líderes de Área	Solicitar formalmente la creación o modificación de accesos. Notificar oportunamente el ingreso o retiro de personal. Validar que los accesos de su equipo correspondan al cargo actual.
Todos los usuarios	Proteger sus credenciales. No compartir contraseñas. Reportar accesos sospechosos. Cambiar contraseña temporal en el primer inicio de sesión.

6. GESTIÓN DE CONTRASEÑAS

6.1 Requisitos mínimos de contraseña

Todas las contraseñas de sistemas corporativos de MADOCO XXI SAS BIC deben cumplir los siguientes criterios:

Criterio	Requisito mínimo
Longitud	Mínimo 12 caracteres

Complejidad	Debe contener mayúsculas, minúsculas, números y caracteres especiales (ej. @, #, $, !)
Vigencia	Cambio obligatorio cada 90 días para cuentas estándar; cada 60 días para cuentas privilegiadas
Historial	No se puede reutilizar ninguna de las últimas 5 contraseñas
Contraseñas prohibidas	Nombres propios, fechas de nacimiento, nombres de la empresa, secuencias simples (1234, abcd) o contraseñas iguales al usuario
Primer inicio de sesión	La contraseña temporal asignada por TI debe cambiarse obligatoriamente en el primer acceso

6.2 Protección y uso de contraseñas

- Las contraseñas son personales e intransferibles. Está terminantemente prohibido compartirlas, anotarlas en lugares visibles o enviarlas por correo, WhatsApp u otro medio de comunicación.
- Si un usuario sospecha que su contraseña fue comprometida, debe reportarlo de inmediato al Departamento de TI (soporte@madoco21.com / soportetecnico@madoco21.com) y cambiarla sin demora.
- Está prohibido utilizar la misma contraseña corporativa en servicios externos o cuentas personales.
- El Departamento de TI nunca solicitará la contraseña de un usuario por ningún medio. Cualquier solicitud de este tipo debe reportarse como incidente de seguridad.

6.3 Cuentas privilegiadas

- Las cuentas con privilegios de administrador del tenant de Microsoft 365 requieren contraseñas de mínimo 16 caracteres y cambio obligatorio cada 60 días.
- Las cuentas administrativas son de uso exclusivo para tareas de administración; no se usarán para actividades cotidianas.
- Toda acción realizada con cuentas privilegiadas quedará registrada en los logs de auditoría de Microsoft 365 y Entra ID.

7. CONTROL DE ACCESOS

7.1 Principio de mínimo privilegio

Cada usuario recibirá exclusivamente los accesos necesarios para el desempeño de sus funciones, conforme al cargo y área definidos en el organigrama corporativo. Los accesos se asignan mediante grupos de seguridad en Entra ID; está prohibido asignar permisos directos a usuarios individuales en SharePoint o cualquier otra plataforma.

7.2 Ciclo de vida de usuarios

Etapa	Acciones del Departamento de TI

Ingreso	Crear cuenta en Entra ID con correo corporativo @madoco21.com. Asignar licencia Microsoft 365 según cargo (Premium o Standard). Agregar a grupos de seguridad correspondientes. Inscribir dispositivo en Intune. Comunicar credenciales de forma segura y directa.
Cambio de cargo	Revisar y ajustar grupos de seguridad y permisos según el nuevo rol. Revocar accesos del cargo anterior. Registrar el cambio en la Matriz de Accesos (Matriz BASC Ciberseguridad).
Retiro	Bloquear la cuenta de forma inmediata al conocer el retiro. Revocar todas las sesiones activas (revoke sign-in sessions en Entra ID). Retirar al usuario de todos los grupos de seguridad. Liberar la licencia. Registrar la fecha de retiro y accesos revocados en la Matriz de Accesos.
Inactividad	Las cuentas sin actividad por más de 30 días serán revisadas y suspendidas preventivamente hasta confirmar su vigencia con el líder de área.

7.3 Autenticación Multifactor (MFA)

La autenticación multifactor es obligatoria para los siguientes perfiles y accesos:

Perfil / Acceso	Obligatoriedad MFA
Cuentas de administrador del tenant	✓ Obligatorio — sin excepción
Gerencias y Dirección	✓ Obligatorio
Acceso desde fuera de las instalaciones	✓ Obligatorio
Colaboradores con acceso a información confidencial	✓ Recomendado / progresivo
Cuentas de buzón compartido	— No aplica (no tienen inicio de sesión directo)

El segundo factor de autenticación es personal e intransferible. Se utilizará la aplicación Microsoft Authenticator como método preferido. La configuración del MFA es responsabilidad del Departamento de TI al momento de la creación del usuario.

7.4 Revisión periódica de accesos

- El Departamento de TI realizará una auditoría mensual de usuarios activos, grupos de seguridad y licencias asignadas, utilizando el Centro de administración de Microsoft 365 y los reportes de Entra ID.
- Control Interno validará trimestralmente que los accesos en la Matriz BASC de Ciberseguridad estén actualizados y correspondan con los roles vigentes.
- Los resultados de cada auditoría quedarán documentados como evidencia para la certificación BASC.

8. ACCESO A LA RED CORPORATIVA

8.1 Segmentación de red

La red de MADOCO XXI SAS BIC está segmentada en tres VLANs con propósitos distintos y accesos controlados:

Red / VLAN	Rango IP	Uso y acceso
Corporativa	192.168.100.x /24	Colaboradores internos. Requiere usuario y contraseña corporativos mediante portal cautivo. Solo dispositivos autorizados.
Invitados	192.168.50.x /24	Visitantes y terceros. Acceso mediante voucher por portal cautivo. Sin acceso a recursos internos. Salida a internet con restricciones.
CCTV y Alarmas	192.168.10.x /24	Exclusivo para cámaras de seguridad y sistema de alarmas. Sin acceso a internet ni a otras VLANs. Administrado únicamente por TI.

8.2 Reglas de acceso a la red

- La red corporativa (192.168.100.x) es de uso exclusivo para dispositivos autorizados por el Departamento de TI. La conexión requiere autenticación con credenciales corporativas (@madoco21.com) a través del portal cautivo administrado en la plataforma OMADA.
- Los visitantes y terceros solo podrán conectarse a la red de invitados (192.168.50.x) mediante voucher de tiempo limitado. Bajo ninguna circunstancia se les proporcionará acceso a la red corporativa.
- El firewall Fortinet es el perímetro de seguridad de la red. Todas las reglas de tráfico entre VLANs, acceso a internet y conexiones externas son administradas exclusivamente por el Departamento de TI.
- Está prohibido conectar dispositivos personales a la red corporativa sin autorización expresa del Departamento de TI.
- El uso de redes WiFi públicas para acceder a recursos corporativos está prohibido sin el uso de VPN corporativa.

8.3 Plataformas de comunicación autorizadas

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

Canal	Uso	Estado
Microsoft Teams	Comunicación interna, reuniones, colaboración	✓ Oficial y autorizado
Exchange Online (@madoco21.com)	Comunicación formal externa e interna	✓ Oficial y autorizado
SharePoint / OneDrive	Gestión documental y colaboración en archivos	✓ Oficial y autorizado

WhatsApp	Comunicación informal rápida únicamente	⚠ Solo informal — no para información sensible
Gmail / Google Chat	Correo externo personal	✗ No autorizado para uso corporativo
Dropbox	Almacenamiento en nube externo	✗ No autorizado — migrar a OneDrive/SharePoint

9. GESTIÓN DE DISPOSITIVOS Y SESIONES

- Todos los equipos corporativos deben estar inscritos en Microsoft Intune con las políticas de seguridad aplicadas: bloqueo automático de pantalla (máximo 5 minutos de inactividad), cifrado de disco habilitado y control de aplicaciones instaladas.
- Los equipos deben tener bloqueo de sesión activo en todo momento cuando el usuario no esté presente (política de escritorio limpio).
- Al finalizar la jornada laboral o al ausentarse del puesto de trabajo, el usuario debe cerrar sesión o bloquear el equipo.
- Está prohibido dejar sesiones activas en equipos compartidos o de acceso público.
- El acceso remoto a sistemas corporativos se realizará únicamente mediante canales seguros definidos por el Departamento de TI. El uso de herramientas de acceso remoto no autorizadas está prohibido.

10. 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 pueden ir desde amonestación escrita hasta terminación del contrato, según la gravedad. Los incidentes que constituyan delitos informáticos conforme a la Ley 1273 de 2009 serán reportados a las autoridades competentes.

Conductas que generan sanción inmediata:

- Compartir credenciales de acceso con terceros o compañeros.
- Acceder a sistemas con credenciales de otro usuario.
- Instalar software para captura de contraseñas o acceso no autorizado.
- Conectar dispositivos no autorizados a la red corporativa.
- Ignorar una alerta o sospecha de compromiso de credenciales sin reportarla.

11. REVISIÓN Y ACTUALIZACIÓN

Esta política será revisada anualmente o cuando se presenten cambios en la infraestructura tecnológica, en los requisitos del estándar BASC, en la normativa colombiana aplicable o ante la ocurrencia de un incidente de seguridad significativo. Las actualizaciones requieren aprobación de la Gerencia General.

CONTROL DE CAMBIOS

Versión	Fecha	Descripción	Responsable	Aprobó
1.0	Junio 2026	Creación inicial del documento	Director comercial TI	Gerente General