POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

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

1. OBJETIVO

Establecer el marco general de seguridad de la información de MADOCO XXI SAS BIC, definiendo los principios, responsabilidades y lineamientos que deben seguir todos los colaboradores, contratistas, aprendices y terceros que accedan, procesen o administren información de la organización, con el fin de garantizar su confidencialidad, integridad y disponibilidad, y cumplir con los requisitos del estándar BASC y la normativa vigente en Colombia.

2. ALCANCE

Esta política aplica a:

- Toda la información de MADOCO XXI SAS BIC, independientemente del formato o medio en que se encuentre (digital, física, verbal).
- Todos los sistemas de información, plataformas y herramientas tecnológicas utilizadas por la organización, incluyendo el ecosistema Microsoft 365 (Entra ID, Intune, SharePoint Online, OneDrive, Teams y Exchange Online).
- Todo el personal interno: colaboradores de todas las áreas y niveles jerárquicos definidos en el organigrama corporativo.
- Aprendices, practicantes, contratistas y consultores externos con acceso autorizado a los recursos de la organización.
- Las sedes operativas de la organización: Barrancabermeja (sede principal), Cartagena y Llanos.

3. DEFINICIONES

Término	Definición
Seguridad de la información	Conjunto de medidas y controles que garantizan la confidencialidad, integridad y disponibilidad de la información.
Confidencialidad	Propiedad que garantiza que la información solo sea accesible a personas autorizadas.
Integridad	Propiedad que garantiza que la información no sea alterada de manera no autorizada.
Disponibilidad	Propiedad que garantiza que la información esté accesible cuando sea requerida por personas autorizadas.
BASC	Business Alliance for Secure Commerce. Estándar internacional de gestión de seguridad en comercio exterior.
Microsoft 365	Plataforma corporativa de productividad y colaboración utilizada por MADOCO XXI SAS BIC.
Entra ID	Servicio de gestión de identidades y accesos de Microsoft (antes Azure AD).
Intune	Plataforma de administración de dispositivos y políticas de seguridad de Microsoft.

Incidente de seguridad	Evento que compromete o tiene potencial de comprometer la confidencialidad, integridad o disponibilidad de la información.
Usuario autorizado	Persona que ha recibido formalmente acceso a los sistemas e información de la organización.

4. MARCO NORMATIVO Y REFERENCIAL

Esta política se fundamenta en los siguientes marcos normativos y estándares:

- Estándar BASC (Business Alliance for Secure Commerce) — versión vigente.
- ISO/IEC 27001 — Sistema de Gestión de Seguridad de la Información (referencial).
- Ley 1581 de 2012 — Protección de datos personales en Colombia (Habeas Data).
- Decreto 1377 de 2013 — Reglamentación de la Ley de Protección de Datos.
- Ley 1273 de 2009 — Delitos informáticos en Colombia.
- Políticas internas de MADOCO XXI SAS BIC y procedimientos del Departamento de TI.

5. PRINCIPIOS DE SEGURIDAD

La gestión de la seguridad de la información en MADOCO XXI SAS BIC se rige por los siguientes principios:

5.1 Mínimo privilegio

Cada usuario recibirá únicamente los accesos estrictamente necesarios para el desempeño de sus funciones. No se otorgarán permisos globales ni accesos a información de otras áreas sin justificación formal aprobada por el líder del área y el Departamento de TI.

5.2 Segregación de funciones

Se evitará que un mismo usuario tenga control sobre procesos incompatibles o sensibles. Los roles de administrador de sistemas estarán separados de los roles operativos.

5.3 Trazabilidad y control

Todas las acciones sobre los sistemas de información deberán quedar registradas mediante logs de auditoría en Microsoft 365, Entra ID, SharePoint Online e Intune, permitiendo la trazabilidad completa de accesos y cambios.

5.4 Gestión centralizada

La administración de identidades, dispositivos y accesos se realizará exclusivamente desde la plataforma Microsoft 365 del tenant corporativo (madoco21.com). Queda prohibida la creación de configuraciones locales no controladas por el Departamento de TI.

5.5 Mejora continua

La seguridad de la información es un proceso dinámico. Esta política y los controles asociados serán revisados periódicamente para adaptarse a nuevas amenazas, cambios organizacionales y requisitos del estándar BASC.

6. RESPONSABILIDADES

6.1 Gerencia General

- Aprobar y respaldar esta política y los recursos necesarios para su implementación.
- Promover una cultura de seguridad de la información en toda la organización.
- Asegurar el cumplimiento de los requisitos BASC en materia de seguridad de la información.

6.2 Director Comercial y TI

- Elaborar, mantener y actualizar esta política y los procedimientos asociados.
- Supervisar la implementación de controles técnicos y organizativos de seguridad.
- Gestionar los recursos tecnológicos de la organización de manera alineada con esta política.
- Coordinar la respuesta ante incidentes de seguridad y escalar a Gerencia General cuando corresponda.

6.3 Control Interno

- Revisar y validar esta política antes de su aprobación por Gerencia General.
- Verificar el cumplimiento de los controles de seguridad establecidos en esta política.
- Reportar hallazgos de incumplimiento a la Gerencia General.

6.4 Departamento de TI

- Implementar y administrar los controles técnicos de seguridad en Microsoft 365.
- Gestionar usuarios, licencias, dispositivos y accesos conforme al procedimiento TI-PR-001.
- Realizar auditorías periódicas de accesos, dispositivos y permisos.
- Atender y gestionar los incidentes de seguridad reportados.
- Mantener actualizadas las evidencias de cumplimiento para las auditorías BASC.

6.5 Líderes y Gestores de Área

- Solicitar la creación, modificación o retiro de accesos mediante el canal formal establecido.
- Informar oportunamente al Departamento de TI sobre el ingreso o retiro de personal.
- Validar que los accesos de su equipo correspondan al rol y funciones actuales.
- Promover el cumplimiento de esta política entre su equipo de trabajo.

6.6 Todos los Colaboradores, Contratistas y Terceros

- Conocer, aceptar y cumplir esta política y las políticas complementarias de seguridad.
- Utilizar los recursos tecnológicos únicamente para fines laborales autorizados.
- Proteger sus credenciales de acceso y no compartirlas bajo ninguna circunstancia.
- Reportar de inmediato cualquier incidente al Departamento de TI (soporte@madoco21.com / soportetecnico@madoco21.com).
- No instalar software no autorizado en los equipos corporativos.

7. LINEAMIENTOS GENERALES

7.1 Control de accesos

- Todo acceso requiere cuenta corporativa en el dominio madoco21.com, gestionada por Entra ID.
- Los accesos se asignan mediante grupos de seguridad; está prohibido asignar permisos directamente a usuarios individuales.

- Se aplicará autenticación multifactor (MFA) para cuentas con acceso a información sensible o privilegios administrativos.
- Las contraseñas temporales deben cambiarse en el primer inicio de sesión.
- Al retiro de un colaborador, el Departamento de TI bloqueará la cuenta, revocará sesiones, retirará al usuario de todos los grupos y liberará la licencia.

7.2 Gestión de dispositivos

- Todos los equipos corporativos deben estar incorporados a Entra ID e inscritos en Microsoft Intune.
- Está prohibido el uso de dispositivos personales para acceder a información corporativa sin autorización previa del Departamento de TI.
- Las políticas de seguridad vía Intune incluyen cifrado de disco, bloqueo automático de pantalla y control de aplicaciones.

7.3 Gestión de la información en Microsoft 365

- La información corporativa debe almacenarse en SharePoint Online o OneDrive Empresarial dentro del tenant madoco21.com.
- La sincronización de OneDrive se limitará a carpetas específicas autorizadas; está prohibido sincronizar bibliotecas completas.
- El correo Exchange Online es la única vía oficial de comunicación externa.

7.4 Uso aceptable de recursos

- Los recursos tecnológicos son de uso exclusivo para actividades laborales.
- Está prohibido el acceso, descarga o distribución de contenido ilegal, inapropiado o que represente un riesgo de seguridad.
- El personal no debe acceder a información de otras áreas sin la autorización correspondiente.

7.5 Gestión de incidentes

- Todo incidente de seguridad debe reportarse de inmediato al Departamento de TI.
- El Departamento de TI registrará, clasificará y gestionará el incidente siguiendo el procedimiento establecido.
- Los incidentes que puedan afectar el cumplimiento BASC deben escalarse al Director Comercial y TI y a la Gerencia General.

7.6 Copias de seguridad

- El Departamento de TI garantizará la existencia de copias de seguridad de la información crítica almacenada en los sistemas corporativos.
- Se realizarán pruebas periódicas de restauración de backups para verificar su efectividad.

7.7 Capacitación y concientización

- Todo el personal recibirá capacitación en seguridad de la información al momento de su vinculación y de manera periódica.
- Se documentará la asistencia y comprensión de esta política mediante acuse de recibo firmado.

8. INCUMPLIMIENTO Y SANCIONES

El incumplimiento de esta política podrá dar lugar a medidas disciplinarias que van desde la amonestación verbal hasta la terminación del contrato, según la gravedad de la falta y lo establecido en el Reglamento Interno de Trabajo y la normativa colombiana vigente. Las infracciones que constituyan delito informático conforme a la Ley 1273 de 2009 serán reportadas a las autoridades competentes.

9. REVISIÓN Y ACTUALIZACIÓN

Esta política será revisada al menos una vez al año o cuando se presenten cambios significativos en la organización, en los sistemas de información, en los requisitos del estándar BASC o en la normativa legal aplicable. Las actualizaciones serán aprobadas por la Gerencia General y comunicadas a todo el personal.

CONTROL DE CAMBIOS

Versión	Fecha	Descripción del cambio	Responsable	Aprobado por
1.0	Junio 2026	Creación inicial del documento	Director Comercial y TI	Gerente general