POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIA

Campo	Dato
Código	MDC-PEPL-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 todo el personal de MADOCO XXI SAS BIC. Queda prohibida su reproducción o divulgación sin previa autorización de la organización.

1. OBJETIVO

Establecer los lineamientos para garantizar que los puestos de trabajo físicos y las pantallas de los dispositivos corporativos de MADOCO XXI SAS BIC no expongan información confidencial o sensible, reduciendo el riesgo de acceso no autorizado, pérdida o filtración de información y asegurando el cumplimiento del estándar BASC.

2. ALCANCE

Esta política aplica a:

- Todos los colaboradores, aprendices, practicantes, contratistas y terceros con acceso a las instalaciones o sistemas de MADOCO XXI SAS BIC.
- Todos los puestos de trabajo físicos en las sedes de Barrancabermeja, Cartagena y Llanos.
- Todos los dispositivos corporativos: computadores de escritorio, portátiles, celulares y tablets, administrados por Microsoft Intune.
- Áreas de impresión, salas de reuniones y cualquier espacio donde se maneje información corporativa.

3. DEFINICIONES

Término	Definición
Escritorio limpio	Práctica que consiste en mantener el área de trabajo física libre de documentos, dispositivos o cualquier material con información sensible cuando no está siendo utilizado activamente.
Pantalla limpia	Práctica que consiste en bloquear o apagar la pantalla del dispositivo cuando el usuario se ausenta de su puesto, evitando la exposición de información a personas no autorizadas.
Información sensible	Cualquier dato cuya divulgación no autorizada pueda comprometer la seguridad, privacidad o intereses de MADOCO XXI SAS BIC o sus colaboradores (datos financieros, personales, comerciales o estratégicos).
Bloqueo de pantalla	Mecanismo que protege el acceso al dispositivo cuando no está en uso, requiriendo autenticación para retomar la sesión.
Microsoft Intune	Plataforma de administración de dispositivos que aplica automáticamente las políticas de bloqueo de pantalla en todos los equipos corporativos.

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 (ítem l: cerrar/bloquear sesión en equipos desatendidos).

- ISO/IEC 27001 — Control A.11.2.9: Política de escritorio limpio y pantalla limpia (referencial).
- Ley 1581 de 2012 — Protección de datos personales en Colombia.

5. RESPONSABILIDADES

Rol	Responsabilidades
Director Comercial y TI	Definir y mantener esta política. Supervisar su implementación técnica a través de Intune. Gestionar incidentes derivados de su incumplimiento.
Area TI	Configurar y mantener las políticas de bloqueo automático de pantalla en todos los dispositivos vía Intune. Verificar su aplicación. Atender reportes de incumplimiento técnico.
Control Interno	Verificar el cumplimiento de esta política mediante recorridos periódicos. Reportar hallazgos de incumplimiento a la Dirección.
Líderes de Área	Promover el cumplimiento de esta política en su equipo. Reportar incumplimientos detectados al Departamento de TI y Control Interno.
Todos los usuarios	Mantener el escritorio físico y la pantalla limpia conforme a esta política. Bloquear el equipo manualmente al ausentarse. Guardar o destruir documentos físicos con información sensible.

6. LINEAMIENTOS DE ESCRITORIO LIMPIO

6.1 Puestos de trabajo

- Al finalizar la jornada laboral o al ausentarse del puesto por periodos prolongados, el colaborador debe retirar o guardar en cajón o archivador bajo llave todo documento físico que contenga información sensible (contratos, datos financieros, información de clientes, reportes internos).
- No está permitido dejar documentos con información confidencial visibles sobre el escritorio cuando el colaborador no se encuentra presente.
- Los documentos físicos que ya no sean necesarios deben ser destruidos de forma segura mediante destructora de papel; está prohibido desecharlos en papeleras comunes.
- Las llaves de archivadores, cajones o espacios con información sensible deben guardarse en lugar seguro y no dejarse sobre el escritorio.
- Los dispositivos de almacenamiento externo (USB, discos) deben guardarse bajo llave cuando no estén en uso; está prohibido dejarlos conectados a los equipos al ausentarse.

6.2 Áreas de impresión

- Los documentos impresos que contengan información sensible deben ser recogidos inmediatamente de la impresora. Está prohibido dejar documentos impresos en la bandeja de salida.
- Si se detectan documentos impresos abandonados con información confidencial, deben entregarse al responsable o destruirse de forma segura.

- Está prohibido imprimir información confidencial en impresoras de uso compartido sin asegurarse de que la impresión será recogida de inmediato.

6.3 Salas de reuniones y espacios comunes

- Al finalizar una reunión, todo material físico con información sensible (presentaciones impresas, notas, documentos) debe recogerse y guardarse o destruirse.
- Los tableros o pizarras que contengan información sensible deben borrarse al concluir la reunión.
- Está prohibido dejar equipos conectados y sesiones abiertas en salas de reuniones al finalizar su uso.

7. LINEAMIENTOS DE PANTALLA LIMPIA

7.1 Bloqueo automático — configuración Intune

El Departamento de TI aplica mediante Microsoft Intune la siguiente configuración obligatoria en todos los dispositivos corporativos:

Parámetro	Configuración aplicada
Tiempo máximo de inactividad	5 minutos — bloqueo automático de pantalla
Método de desbloqueo	Contraseña corporativa o PIN seguro
Protector de pantalla	Activado con contraseña requerida al reanudar
Cifrado de disco	Habilitado en todos los equipos vía Intune (BitLocker)
Dispositivos aplicados	Todos los equipos corporativos inscritos en Microsoft Intune

7.2 Bloqueo manual — responsabilidad del usuario

- Al ausentarse del puesto de trabajo, aunque sea por un tiempo breve, el colaborador debe bloquear manualmente la pantalla (Windows: tecla Win + L / Mac: Ctrl + Cmd + Q).
- Al finalizar la jornada laboral, el colaborador debe cerrar sesión completamente en el equipo; no basta con bloquear la pantalla.
- Está prohibido dejar sesiones activas en equipos de uso compartido o en salas de reuniones.
- Está prohibido desactivar, eludir o modificar la configuración de bloqueo automático aplicada por Intune.

7.3 Pantallas en espacios con visibilidad externa

- Los monitores ubicados en zonas con visibilidad para visitantes, clientes o personal externo deben estar orientados de forma que no permitan la lectura de información sensible desde el exterior.
- En atención al público o recepción, los equipos deben mostrar únicamente la información estrictamente necesaria para la atención. El resto de aplicaciones y documentos deben estar minimizados o cerrados.
- Durante videollamadas o presentaciones en Teams, verificar que el fondo compartido no exponga información sensible visible en el entorno físico o en otras ventanas del equipo.

7.4 Dispositivos móviles corporativos

- Los celulares corporativos deben tener activado el bloqueo automático de pantalla con un tiempo máximo de 2 minutos de inactividad.
- El desbloqueo debe realizarse mediante PIN, patrón o biometría. No está permitido desactivar el bloqueo de pantalla en celulares corporativos.
- Al dejar el celular sobre el escritorio, este debe estar bloqueado o boca abajo para evitar la visualización de notificaciones con información sensible.

8. VERIFICACIÓN Y CONTROL

8.1 Frecuencia de verificación

Actividad	Frecuencia	Responsable
Verificación técnica de políticas Intune (bloqueo)	Mensual	Departamento de TI
Recorrido de escritorios y puestos de trabajo	Trimestral (o sin previo aviso)	Control Interno
Revisión de zonas de impresión y salas de reunión	Trimestral	Control Interno + Líder de Área
Revisión general de cumplimiento de la política	Anual	Director Comercial y TI

8.2 Lista de verificación — escritorio y pantalla limpia

La siguiente lista puede ser utilizada por Control Interno o líderes de área en recorridos de verificación:

Ítem a verificar	Detalle	¿Cumple?
Escritorio libre de documentos sensibles	No hay papeles, reportes ni contratos visibles sin custodia	☐ Sí ☐ No
Documentos guardados o bajo llave	Cajones o archivadores cerrados con información sensible	☐ Sí ☐ No
No hay USB ni dispositivos externos conectados	Memorias o discos desconectados y guardados	☐ Sí ☐ No

Pantalla bloqueada en equipos desatendidos	Bloqueo visible o protector de pantalla activo	☐ Sí ☐ No
Bandeja de impresora vacía	No hay documentos impresos abandonados	☐ Sí ☐ No
Tableros de reunión borrados	Información sensible eliminada tras la reunión	☐ Sí ☐ No
Celular corporativo bloqueado al dejarlo	Pantalla bloqueada o boca abajo	☐ Sí ☐ No
Sesión cerrada al final de la jornada	No solo bloqueada — cerrada completamente	☐ Sí ☐ No
Monitor orientado correctamente	Sin visibilidad desde zonas de acceso externo	☐ Sí ☐ No
Documentos obsoletos destruidos	Uso de destructora de papel para información sensible	☐ Sí ☐ No

9. 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 verbal hasta medidas disciplinarias formales según la gravedad y la reincidencia.

Conductas que generan llamado de atención inmediato:

- Dejar documentos con información sensible visibles sobre el escritorio sin custodia.
- No bloquear la pantalla al ausentarse del puesto de trabajo.
- Dejar sesiones activas en equipos compartidos o salas de reunión.
- Desechar documentos con información confidencial en papelera común sin destruir.
- Desactivar o eludir la configuración de bloqueo automático aplicada por Intune.
- Dejar documentos impresos con información confidencial abandonados en la impresora.

10. REVISIÓN Y ACTUALIZACIÓN

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

CONTROL DE CAMBIOS

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