POLÍTICA DE SEGURIDAD Y GESTIÓN DE REDES

Campo	Dato
Código	MDC-PSGR-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 información crítica sobre la infraestructura de red 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, controles y criterios de seguridad para la gestión, operación y protección de la infraestructura de red de MADOCO XXI SAS BIC, garantizando la confidencialidad, integridad y disponibilidad de la información transmitida a través de las redes corporativas, previniendo accesos no autorizados y asegurando el cumplimiento del estándar BASC y la normativa vigente en Colombia.

2. ALCANCE

Esta política aplica a:

- Toda la infraestructura de red de MADOCO XXI SAS BIC: red cableada (Ethernet), red inalámbrica (WiFi), VLANs, firewall y accesos remotos mediante VPN.
- Los equipos de red administrados: firewall Fortinet (perímetro de seguridad), router ER7206, switch core SG3428, access points EAP610 y controlador centralizado OMADA.
- Todos los colaboradores internos, aprendices, practicantes, contratistas y terceros que se conecten a cualquier red de la organización.
- Los dispositivos corporativos inscritos en Microsoft Intune y cualquier dispositivo que acceda a recursos de la organización.
- Las sedes de Barrancabermeja — Campestre (sede principal), Cartagena y Llanos, interconectadas mediante túneles VPN site-to-site.

3. DEFINICIONES

Término	Definición
VLAN	Red de área local virtual que segmenta el tráfico de red para aislar grupos de dispositivos según su función o nivel de seguridad.
Firewall Fortinet	Dispositivo de seguridad perimetral que controla y filtra todo el tráfico entrante y saliente de la red corporativa.
Controlador OMADA	Plataforma centralizada TP-Link para administración, configuración y monitoreo de todos los dispositivos de red (SDN).
Portal cautivo	Mecanismo de autenticación WiFi que solicita credenciales corporativas o voucher antes de otorgar acceso a la red.
VPN (OpenVPN)	Red privada virtual que establece un túnel cifrado para acceso remoto seguro a la red corporativa desde ubicaciones externas.
Binding IP-MAC	Amarre de dirección IP a la dirección física (MAC) de un dispositivo, aplicado en la red cableada para garantizar que solo equipos autorizados obtengan conectividad.
Voucher / Cupón	Código de acceso temporal generado para usuarios de la red de invitados, con vigencia y restricciones definidas.

Segmentación de red	División de la red en subredes independientes para aislar el tráfico, reducir riesgos y mejorar el control de accesos.
Zero Trust	Principio de seguridad que asume que ningún dispositivo o usuario es confiable por defecto; todo acceso debe ser verificado y autorizado.
Firmware	Software interno de los dispositivos de red que controla su funcionamiento y debe mantenerse actualizado.

4. MARCO NORMATIVO Y CUMPLIMIENTO BASC

Esta política da cumplimiento a los siguientes marcos y normativas:

- MDC-PGSI-01 — Política General de Seguridad de la Información
- MDC-PCAGC-01 — Política de Control de Accesos y Gestión de Contraseñas.
- Estándar BASC — Business Alliance for Secure Commerce (ítems: a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v).
- ISO/IEC 27001 — 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 redes
Director Comercial y TI	Definir y mantener esta política. Autorizar cambios en la infraestructura de red. Aprobar accesos VPN y excepciones de seguridad. Gestionar incidentes críticos de red.
Area de TI (Administrador de Red)	Administrar y monitorear la infraestructura de red. Gestionar el controlador OMADA y el firewall Fortinet. Crear, revocar y auditar accesos a la red. Mantener firmware actualizado. Documentar incidentes y cambios. Generar y controlar vouchers de acceso.
Control Interno	Verificar el cumplimiento de esta política. Revisar registros de acceso y bitácoras de red. Reportar hallazgos de incumplimiento a la Dirección.
Líderes de Área	Notificar el ingreso o retiro de personal para gestión de accesos. Reportar incidentes de red detectados en su área. Velar por el cumplimiento de esta política en su equipo.
Todos los usuarios	Utilizar únicamente las redes autorizadas para su perfil. No compartir credenciales ni vouchers de acceso. Reportar dispositivos o comportamientos sospechosos en la red al Departamento de TI.

6. INFRAESTRUCTURA DE RED

6.1 Arquitectura general

La infraestructura de red de MADOCO XXI SAS BIC se basa en una arquitectura de Red Definida por Software (SDN), administrada de forma centralizada mediante el controlador OMADA. El perímetro de seguridad es gestionado por el firewall Fortinet, que controla todo el tráfico entre VLANs, el acceso a internet y las conexiones externas.

Componente	Modelo / Plataforma	Función
Firewall perimetral	Fortinet	Control de tráfico entre VLANs, filtrado de contenido, defensa DoS y seguridad perimetral.
Router / Gateway	TP-Link ER7206	Enrutamiento, gestión DHCP, firewall SPI y punto de salida a internet.
Switch core	TP-Link SG3428	Conmutación central y distribución de VLANs a toda la infraestructura.
Access Points WiFi	6 × EAP610 (US) v3.0	Cobertura inalámbrica en 3 pisos (Corte, Calidad/Producción, Administración).
Controlador de red	OMADA Controller	Administración centralizada SDN, portal cautivo, vouchers, auditoría de logs y monitoreo.

6.2 Segmentación de red — VLANs

La red está segmentada en tres VLANs con propósitos, rangos de IP y niveles de acceso diferenciados, aplicando el principio de Zero Trust entre segmentos:

Red / VLAN	Nombre	Rango IP	Uso, acceso y restricciones
VLAN Corporativa	VLAN1_CORPORATIVA	192.168.100.x /24	Colaboradores internos con dispositivos corporativos autorizados. Autenticación con credenciales @madoco21.com mediante portal cautivo. Acceso a recursos internos, Microsoft 365 e internet corporativo.

VLAN Invitados	VLAN_GUESTS	192.168.50.x /24	Visitantes, clientes y terceros. Acceso mediante voucher de tiempo limitado por portal cautivo. Solo salida a internet con restricciones. Sin acceso a recursos internos ni a otras VLANs.
VLAN CCTV y Alarmas	VLAN10_SECURITY	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 el Departamento de TI.

La comunicación entre VLANs está restringida por defecto. Cualquier excepción debe ser justificada, aprobada por el Director Comercial y TI, y documentada en la bitácora de cambios de red.

7. CONTROL DE ACCESO A LA RED

7.1 Red corporativa — autenticación y dispositivos autorizados

- El acceso a la red corporativa (192.168.100.x) requiere autenticación con credenciales corporativas (@madoco21.com) a través del portal cautivo administrado en OMADA.
- En la red cableada se aplica Binding IP-MAC: solo los dispositivos con dirección MAC previamente registrada y autorizada en el servidor DHCP del ER7206 obtendrán conectividad.
- Está prohibido conectar dispositivos personales a la red corporativa sin autorización expresa y documentada del Departamento de TI.
- Todo dispositivo corporativo debe estar inscrito en Microsoft Intune antes de recibir acceso a la red.

7.2 Red de invitados — gestión de vouchers

Los visitantes, auditores y terceros acceden exclusivamente a la red de invitados (192.168.50.x) mediante vouchers gestionados desde OMADA. Los tipos de voucher son:

Categoría	Tipo	Vigencia	Uso típico
Corporativo / Gerencial	Permanente	Ilimitado	Equipos de la empresa y alta gerencia.
Temporal / Auditoría	Temporal	4 días	Consultores externos, auditores y visitas técnicas.
Emergencia (SOS)	Emergencia	4 horas	Conferencias rápidas o soporte de emergencia.

- Cada voucher consta de 8 caracteres alfanuméricos. Está prohibido compartir un voucher entre múltiples usuarios; el sistema OMADA permite un solo dispositivo por voucher.
- El Departamento de TI registrará en la bitácora técnica el nombre del usuario y el motivo de entrega de cada voucher, garantizando trazabilidad total.

- Bajo ninguna circunstancia se proporcionará a un visitante o tercero acceso a la red corporativa.

7.3 Gestión de identidades de red

- Las credenciales de administración del controlador OMADA, router y switches son custodiadas exclusivamente por el Departamento de TI y deben cumplir la política de contraseñas definida en TI-POL-002.
- Las credenciales de administración se cambiarán cada 90 días o de forma inmediata ante cualquier sospecha de compromiso.
- Al retiro de un colaborador con acceso a la red, el Departamento de TI ejecutará dentro de las 4 horas siguientes: eliminación del dispositivo en OMADA, revocación de vouchers activos, eliminación del binding IP-MAC y cambio de credenciales administrativas si el colaborador tenía privilegios de administración.

8. SEGURIDAD DE LA RED INALÁMBRICA (WiFi)

- Todos los SSIDs corporativos utilizan cifrado WPA2/WPA3 como estándar mínimo.
- El acceso WiFi corporativo se gestiona exclusivamente mediante portal cautivo con autenticación por credenciales corporativas; no se utilizan claves compartidas (PSK) en la red corporativa.
- Los 6 access points EAP610 están distribuidos estratégicamente en los tres pisos de la sede principal (Piso 1: Corte y Diseño; Piso 2: Calidad y Producción; Piso 3: Administración y Soporte).
- La potencia de transmisión de los access points se ajusta para evitar cobertura innecesaria fuera de las instalaciones.
- El Departamento de TI revisará semanalmente los dispositivos conectados a las redes WiFi para detectar equipos no autorizados.
- Las configuraciones de red WiFi se revisan y validan trimestralmente como evidencia para la auditoría BASC.

9. ACCESO REMOTO SEGURO — VPN

9.1 Lineamientos generales

- El acceso remoto a la infraestructura tecnológica de MADOCO XXI SAS BIC se realiza exclusivamente mediante VPN de mayor seguridad disponible.
- Está prohibido el uso de redes WiFi públicas o no seguras para acceder a recursos corporativos sin estar conectado a la VPN corporativa.
- Cada usuario VPN tiene credenciales individuales; está prohibido compartir cuentas VPN.
- El Departamento de TI es el único autorizado para crear, modificar o revocar accesos VPN.
- Las sedes de Cartagena y Llanos están interconectadas a la sede principal mediante túneles VPN site-to-site, administrados desde el controlador OMADA central.

9.2 Parámetros técnicos de la VPN corporativa

Parámetro	Configuración
Protocolo	OpenVPN (cliente a sitio)

Modo de túnel	Completo — todo el tráfico se enruta por la red corporativa
Puerto de servicio	1194
Rango IP VPN	10.8.0.0/24
Redes accesibles	VLAN1_CORPORATIVA (192.168.100.x) — VLAN10_SECURITY (192.168.10.x)
Autenticación	Usuario y contraseña individuales bajo política TI-POL-002
Gestión	Controlador OMADA — administrado exclusivamente por TI

10. MONITOREO Y DETECCIÓN DE AMENAZAS

10.1 Actividades de monitoreo

Actividad	Herramienta	Frecuencia	Evidencia
Revisión de alertas y amenazas de red	OMADA — Seguridad → Lista de amenazas	Semanal	Exportación CSV/XLSX de amenazas
Auditoría de logs de acceso (intentos fallidos)	OMADA — Registros → Auditoría de Logs	Semanal	Exportación de logs con estado FALLO/ATENCIÓN
Monitoreo de tráfico y comportamiento anómalo	OMADA — Reportes de red	Mensual	Reporte de tráfico RX/TX por área y VLAN
Verificación de dispositivos conectados	OMADA — Dashboard de clientes	Semanal	Listado de dispositivos activos por VLAN
Estado de salud de la infraestructura (APs, switch, gateway)	OMADA — Mapa de red en tiempo real	Diario	Captura de estado operativo sin desconexiones
Revisión de accesos VPN activos	OMADA — VPN → Usuarios conectados	Mensual	Listado de usuarios VPN y logs de sesión

Ante la detección de amenazas, accesos fallidos reiterados o comportamientos anómalos, el Departamento de TI debe: documentar el evento, exportar los logs como evidencia, aplicar las medidas correctivas (bloqueo, aislamiento, revocación de acceso) y reportar al Director Comercial y TI en un plazo máximo de 2 horas.

10.2 Gestión de incidentes de red

- Todo incidente de red (acceso no autorizado, caída de servicio, dispositivo desconocido detectado, saturación de ancho de banda) debe ser reportado, registrado y gestionado conforme al procedimiento de gestión de incidentes de TI.
- Los incidentes deben clasificarse por nivel de riesgo: Crítico, Alto, Medio o Bajo, y documentarse en la bitácora de incidentes con fecha, descripción, impacto, acciones tomadas y responsable.
- Los incidentes que afecten la operación o el cumplimiento BASC se escalarán al Director Comercial y TI y a la Gerencia General.

11. GESTIÓN DE DISPOSITIVOS DE RED

- Todos los dispositivos de red (router, switches, access points, firewall) deben estar registrados en el módulo de Mantenimiento del ERP Odoo, identificados por su dirección MAC y código de activo fijo.
- Los dispositivos que aparezcan activos en el controlador OMADA pero no estén registrados en Odoo deben ser aislados de inmediato hasta su verificación.
- El firmware de todos los dispositivos de red debe mantenerse actualizado. Las actualizaciones se revisarán mensualmente y se aplicarán conforme al plan de mantenimiento.
- Las credenciales de administración de fábrica deben ser reemplazadas antes de la puesta en operación de cualquier dispositivo de red.
- Se realizará una revisión trimestral de la configuración de todos los dispositivos de red como evidencia para la auditoría BASC.
- Las configuraciones de red (OMADA, Fortinet, ER7206) se respaldarán mensualmente y tras cualquier cambio significativo. Las copias se almacenarán en un repositorio seguro dentro del ecosistema Microsoft 365.

12. COPIAS DE SEGURIDAD Y CONTINUIDAD

- Se realizarán copias de seguridad de las configuraciones de todos los dispositivos de red mensualmente o inmediatamente después de cualquier cambio en la infraestructura.
- Las copias de respaldo se almacenarán en al menos dos ubicaciones: local (repositorio seguro en la red corporativa) y remota (OneDrive/SharePoint dentro del tenant madoco21.com).
- Se realizarán pruebas semestrales de restauración de configuraciones para verificar la integridad de los backups.
- Ante una falla crítica de la red, el Departamento de TI activará el plan de recuperación y comunicará el estado a la Dirección en un plazo máximo de 30 minutos.

13. AUDITORÍA Y MEJORA CONTINUA

Actividad de auditoría	Frecuencia	Responsable
Revisión de segmentación de VLANs y reglas de firewall	Trimestral	Departamento de TI
Verificación de dispositivos autorizados en la red	Mensual	Departamento de TI
Revisión de accesos VPN y usuarios activos	Mensual	Departamento de TI

Prueba de restauración de backup de configuraciones	Semestral	Departamento de TI
Evaluación de seguridad de infraestructura TI	Anual	Director Comercial y TI + Control Interno
Revisión y actualización de esta política	Anual	Director Comercial y TI

Los resultados de cada auditoría se documentarán y conservarán como evidencia para la certificación BASC. Las vulnerabilidades identificadas se registrarán con plan de acción, responsable y fecha de cierre.

14. 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 delitos informáticos conforme a la Ley 1273 de 2009 serán reportados a las autoridades competentes.

Conductas que generan sanción inmediata:

- Conectar dispositivos no autorizados a la red corporativa o de CCTV.
- Compartir credenciales de acceso a la red o vouchers con terceros.
- Intentar acceder a VLANs distintas a las autorizadas para su perfil.
- Modificar la configuración de dispositivos de red sin autorización del Departamento de TI.
- Usar redes WiFi públicas para acceder a recursos corporativos sin VPN.

15. 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 y deben comunicarse a todo el personal.

CONTROL DE CAMBIOS

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