COMITE INTERGREMIAL Y EMPRESARIAL DEL VALLE DEL CAUCA – CIEV

www.ciev.co

PROTOCOLO DE ACTUACIÓN ANTE RIESGOS CRÍTICOS — VERSIÓN 2.0

CONTEXTO: PERÍODO ELECTORAL – VALLE DEL CAUCA 2026 | 13 RIESGOS | R-013 NUEVO · R-009 REPRIORIZADO

Basado en ISO 31000:2018 · ISO 31010:2019 · ISO 22301:2019

Documento	Protocolo de Actuación ante Riesgos – CIEV
Versión	2.0
Fecha	Mayo 2026
Elaborado por	Junta Directiva CIEV – Taller de Gestión de Riesgos
Destinatarios	Empresas afiliadas a gremios del CIEV, Gobernación del Valle del Cauca, Alcaldía de Cali, Policía Metropolitana, Ejército Nacional
Clasificación	**USO RESTRINGIDO – GREMIOS AFILIADOS CIEV**

1. OBJETO Y ALCANCE DEL PROTOCOLO

El presente protocolo establece los lineamientos, procedimientos y responsabilidades que deben implementar las empresas afiliadas a los gremios del CIEV ante la materialización de eventos de riesgo críticos identificados en el contexto del período electoral en el Valle del Cauca durante 2026.

Su elaboración se fundamenta en la metodología de gestión de riesgos definida por la norma ISO 31000:2018 y las técnicas de evaluación de riesgos de la ISO 31010:2019, articuladas con los requisitos de continuidad de negocio de la ISO 22301:2019.

1.1 Objetivos específicos

- Establecer mecanismos de prevención, preparación, respuesta y recuperación ante eventos que afecten la movilidad, la seguridad y la operación empresarial.
- Definir roles y responsabilidades articulados entre el sector privado, la Fuerza Pública, la Gobernación del Valle y la Alcaldía de Cali.
- Proveer herramientas prácticas para la toma de decisiones en situaciones de crisis durante el período electoral.
- Contribuir a la resiliencia organizacional de las empresas de los gremios afiliados al CIEV.

1.2 Ámbito de aplicación

Este protocolo aplica a todas las empresas afiliadas a los gremios que conforman el CIEV.

2. CONTEXTO DE RIESGO – VALLE DEL CAUCA 2026

2.1 Situación actual del orden público

El Valle del Cauca enfrenta en 2026 un escenario de riesgo multidimensional caracterizado por:

- Bloqueos de vías estratégicas (Panamericana, corredor Cali-Buenaventura, Buga-Palmira) por comunidades indígenas y movimientos sociales.
- Atentados terroristas contra infraestructura eléctrica y de comunicaciones por grupos armados ilegales.
- Manifestaciones urbanas y disturbios en centros comerciales y áreas empresariales de Cali, Palmira, Tuluá y Buenaventura.
- Actividades de extorsión y amenazas a empresarios por parte de grupos criminales organizados.
- Restricciones a la movilidad aérea por condiciones de seguridad en accesos al Aeropuerto Alfonso Bonilla Aragón.
    - ★ **REPRIORIZADO A EXTREMO:** Desinformación y uso deliberado de noticias falsas como arma táctica desestabilizadora por actores violentos, generando pánico masivo, distorsión de la realidad y debilitamiento de la respuesta institucional.

- ★ **NUEVO RIESGO R-013:** Invasión y ocupación ilegal de terrenos e instalaciones empresariales por grupos organizados. La Ley 1801/2016 (Art. 78) faculta a la Policía para ordenar el desalojo en las primeras 48 horas; la empresa debe denunciar en las primeras 24 horas.

2.2 Riesgos prioritarios identificados (ISO 31010 – Lluvia de Ideas)

CÓDIGO	NIVEL	DESCRIPCIÓN DEL RIESGO	PROBABILIDAD	IMPACTO
R-001	EXTREMO	Bloqueo vías terrestres principales	Casi Seguro (4)	Catastrófico (4)
R-002	ALTO	Atentados infraestructura crítica	Probable (3)	Catastrófico (4)
R-005	EXTREMO	Extorsión y amenazas a empresarios	Casi Seguro (4)	Catastrófico (4)
R-003	ALTO	Disturbios y manifestaciones en áreas urbanas	Casi Seguro (4)	Moderado (3)
R-007	ALTO	Afectación cadena de suministro	Casi Seguro (4)	Moderado (3)
R-009	EXTREMO	Desinformación como arma táctica ★ REPRIORIZADO	Casi Seguro (4)	Catastrófico (4)
R-013	ALTO ★ NUEVO	Invasión de terrenos e instalaciones (Ley 1801/2016)	Probable (3)	Moderado/Alto (3)

3. ESTRUCTURA ORGANIZACIONAL DE RESPUESTA

3.1 Comité de Crisis CIEV

El Comité de Crisis del CIEV es el órgano rector para la coordinación de la respuesta ante emergencias que afecten a los gremios afiliados. Se activa automáticamente cuando se materialice un riesgo ALTO o EXTREMO.

ROL	RESPONSABLE	FUNCIONES PRINCIPALES
Presidente del Comité	Director Ejecutivo CIEV	Declarar estado de crisis, activar protocolo, comunicación con autoridades
Coordinador Seguridad	Comite de Seguridad CIEV	Monitoreo de alertas, coordinación con Policía, Ejército y FFMM
Coordinador Logístico	Rep. Gremio Transporte	Gestión de rutas alternas, abastecimiento, coordinación con transportadores
Vocero Oficial	Director de Comunicaciones CIEV	Manejo de medios, comunicados, redes sociales y mensajes internos
Coordinador RRHH	Rep. Área Gestión Humana	Seguridad de empleados, teletrabajo, comunicación interna a colaboradores
Enlace Autoridades	Rep. designado por Junta CIEV	Coordinación con Gobernación, Alcaldía, Policía Metropolitana, Ejército

3.2 Árbol de Contactos de Emergencia

ENTIDAD	CONTACTO / LÍNEA	OBSERVACIONES
Policía Nacional – DIJIN	Línea 123 / Contacto directo CMD	Activar en caso de bloqueos o amenazas
Ejército Nacional – Brigada	Tercera Brigada Cali – contacto oficial	Atentados, terrorismo, zonas rurales
Gobernación – Sec. Seguridad	Secretaria de Seguridad Gobernación Valle	Coordinación interinstitucional
Alcaldía Cali – Sec. Seguridad	Secretaría de Seguridad y Justicia de Cali	Incidentes urbanos en Cali
Defensa Civil Colombiana	Línea 144	Emergencias y desastres
GAULA (Anti-secuestro)	Línea 165	Extorsión, secuestro, amenazas

Fiscalía General	Línea 122 / URI local	Denuncia de delitos contra empresarios
Aeronáutica Civil	Aerocivil Regional Occidente	Restricciones aéreas
Director CIEV (24/7)	**Completar en taller con contacto directo**	**Activación del Comité de Crisis**

4. PROTOCOLOS DE ACTUACIÓN POR TIPO DE RIESGO

4.1 PROTOCOLO DE MOVILIDAD – Bloqueos Viales (R-001)

NIVEL DE RIESGO: EXTREMO (NR = 16) | Activación: Inmediata ante bloqueo confirmado

FASE 1 – ALERTA TEMPRANA (0-2 horas antes):

1. Monitorear permanentemente el estado de vías mediante: app Waze, Twitter/X, canales de radio (RCN, Caracol), grupos de WhatsApp de gremios de transporte.
2. Activar el árbol de comunicación interno del CIEV en cuanto se detecte amenaza de bloqueo.
3. Notificar a empresas afiliadas con alerta preventiva vía correo y WhatsApp corporativo.
4. Solicitar información a la Policía de Carreteras sobre tiempo estimado y alcance del bloqueo.

FASE 2 – RESPUESTA (durante el bloqueo):

5. Activar rutas alternativas pre-identificadas: (a) Panamericana por Popayán, (b) Cali-Buenaventura por La Paila-Armenia, (c) Vías secundarias Palmira-Buga-Tuluá.
6. Coordinar con Ministerio de Transporte y Gobernación para solicitar escolta militar a convoyes de carga prioritaria (alimentos, medicamentos, exportaciones).
7. Activar modalidad de inventarios de seguridad pre-acordada con proveedores: mínimo 3 días para alimentos perecederos, 15 días para materias primas industriales.
8. Comunicar a clientes sobre la situación con mensajes estandarizados (ver Anexo A).
9. Registrar todas las pérdidas y costos adicionales para posterior reclamo a seguros y/o acciones legales.

FASE 3 – RECUPERACIÓN (tras el levantamiento):

10. Evaluación inmediata de inventarios y estado de pedidos pendientes.
11. Plan de despacho acelerado con priorización de clientes críticos.
12. Informe al Comité de Crisis con lecciones aprendidas.
13. Revisión y actualización del protocolo si el bloqueo tuvo características no previstas.

4.2 PROTOCOLO ANTI-TERRORISMO – Atentados a Infraestructura (R-002)

NIVEL DE RIESGO: ALTO (NR = 12) | Activación: Inmediata ante corte de energía o comunicaciones

ACCIONES INMEDIATAS:

14. Activar generadores de emergencia y sistemas UPS (tiempo de cobertura: verificar en inventario de activos críticos).
15. Cambiar a canales de comunicación alternativa: radio VHF/UHF, teléfono satelital, WhatsApp con datos móviles.
16. Reportar inmediatamente a EMCALI/EPM y solicitar priorización en la reconexión.
17. Notificar al Ejército Nacional (Tercera Brigada) si hay evidencia de sabotaje.
18. Activar protocolo de continuidad de negocio empresarial para operaciones críticas.
19. Estimar el Tiempo Objetivo de Recuperación (RTO) y comunicar a clientes.

4.3 PROTOCOLO DE SEGURIDAD PERSONAL – Extorsión y Amenazas (R-005)

NIVEL DE RIESGO: EXTREMO (NR = 16) | CONFIDENCIAL – Difusión restringida

REGLAS FUNDAMENTALES:

- NO PAGAR extorsiones: el pago alimenta la economía criminal, no garantiza la seguridad y es delito de financiación del terrorismo.
- REPORTAR siempre: toda amenaza o intento de extorsión debe reportarse al GAULA (165) y a la Fiscalía (122).
- CONFIDENCIALIDAD: no difundir el hecho más allá del círculo de necesidad (familia inmediata, asesor de seguridad, autoridades).

PROCEDIMIENTO:

20. Si recibe una amenaza: conservar la calma, no confrontar al interlocutor, memorizar detalles (voz, número, hora, mensaje exacto).
21. Contactar inmediatamente al GAULA en la línea 165 (disponible 24/7, confidencial).

22. Notificar al Oficial de Seguridad del CIEV quien activará el protocolo de protección personal.
23. Evaluar con el GAULA si se requiere protección personal, cambio de rutinas o medidas adicionales.
24. Activar seguro de extorsión/secuestro si la empresa cuenta con esta póliza.

4.4 PROTOCOLO DE SEGURIDAD URBANA – Disturbios y Manifestaciones (R-003)

NIVEL DE RIESGO: ALTO (NR = 12) | Activación: Cuando se confirmen protestas en área de influencia

25. Monitorear en tiempo real las redes sociales y medios locales para anticipar movilizaciones.
26. Emitir alerta interna a todos los empleados con indicaciones de evitar zonas de riesgo.
27. Activar cierre preventivo de establecimientos en área de influencia si la situación lo amerita.
28. Implementar teletrabajo de emergencia para personal administrativo con capacidad para hacerlo.
29. Coordinar con Policía Metropolitana para custodia de instalaciones críticas.
30. Establecer punto de encuentro seguro y comunicar a todos los empleados.
31. No permitir que empleados enfrenten manifestantes: retiro ordenado y seguro.

4.5 PROTOCOLO DE DESINFORMACIÓN ★ REPRIORIZADO A EXTREMO – Arma Táctica (R-009)

NIVEL DE RIESGO: EXTREMO (NR = 16) ★ REPRIORIZADO | Activación: Inmediata ante detección de campaña de desinformación

JUSTIFICACIÓN DE LA REPRIOIRIZACIÓN:

La desinformación ha evolucionado de ser un riesgo reputacional a convertirse en un arma táctica utilizada deliberadamente por actores violentos para: crear pánico masivo, desacreditar a las autoridades y al sector empresarial, fragmentar la respuesta institucional con informaciones contradictorias, movilizar grupos con base en hechos falsos, y generar presión mediática para impedir acciones legales. La velocidad de propagación en redes sociales hace que el daño sea prácticamente inmediato e irreversible si no se actúa en los primeros 30-60 minutos. Por estas razones, el nivel asciende de MODERADO a EXTREMO (P=4, I=4, NR=16).

ACCIONES INMEDIATAS (ventana crítica: 30 minutos):

32. Activar el canal oficial verificado CIEV-Policía: toda información sobre orden público debe confirmarse por este canal antes de difundirse internamente.
33. Emitir comunicado oficial del CIEV con verificación policial en máx. 30 minutos después de detectar la desinformación viral.
34. Etiquetar explícitamente las noticias falsas como INFORMACIÓN FALSA y reportar a la plataforma (WhatsApp, Facebook, X/Twitter) para solicitar retiro inmediato.
35. Mantener fuentes únicas de información verificada: solo canales oficiales de Policía Nacional, Ejército, Gobernación del Valle y Alcaldía de Cali.
36. Investigación y judicialización de los responsables de campañas de desinformación bajo la Ley 1273/2009 (delitos informáticos) y el Código Penal (pánico económico, Art. 302).

4.6 PROTOCOLO DE INVASIÓN DE TERRENOS ★ NUEVO – Ley 1801/2016 (R-013)

NIVEL DE RIESGO: ALTO (NR = 12) ★ NUEVO | Activación: Inmediata al confirmarse la invasión | VENTANA CRÍTICA: 48 horas (Art. 78 Ley 1801/2016)

FUNDAMENTO LEGAL — LEY 1801 DE 2016 (CÓDIGO NACIONAL DE POLICÍA, ART. 78):

Cuando se ocupe de hecho un bien inmueble de ajena pertenencia, el comandante de Estación o Subestación de Policía de la jurisdicción, una vez comprobada la situación, ordenará el desalojo inmediato. Esta facultad administrativa opera EXCLUSIVAMENTE dentro de las primeras 48 horas tras la ocupación ilegal. Vencido este término se requiere proceso judicial (acción de lanzamiento por ocupación de hecho ante juez civil municipal), que puede tardar semanas o meses.

PROCEDIMIENTO EMPRESARIAL — PRIMERAS 24 HORAS (crítico para activar la ventana de 48h):

1. DOCUMENTAR inmediatamente: fotografías y vídeos con geolocalización y fecha/hora; identificación de testigos; número aproximado de invasores y descripción de la situación.
2. DENUNCIAR en la Estación de Policía de la jurisdicción (presencial o al 123) dentro de las PRIMERAS 24 HORAS para que la Policía pueda actuar administrativamente dentro de su ventana de 48 horas.
3. NOTIFICAR al comité de seguridad del CIEV y al abogado de la empresa para iniciar simultáneamente el proceso judicial como medida de respaldo en caso de que se venza la ventana administrativa.
4. NO CONFRONTAR directamente a los invasores: el personal debe retirarse a un lugar seguro para proteger su integridad física.
5. Solicitar a la Policía la diligencia formal de lanzamiento con acta oficial, registro fotográfico y relación de medidas correctivas impuestas a los invasores.

4.7 PROTOCOLO DE COMUNICACIÓN DE CRISIS (Aplica a todos los riesgos)

AUDIENCIA	MENSAJE CLAVE	CANAL	RESPONSABLE
Empleados	Instrucciones de seguridad, estado operativo, medidas a tomar	WhatsApp, correo, llamadas en cadena	RRHH + Gerencia
Clientes	Reconocimiento de la situación, medidas adoptadas, nuevo plazo estimado	Correo formal, llamada directa, CRM	Gerente Comercial
Medios de comunicación	Comunicado oficial CIEV: hechos, impacto, gestión, apoyo esperado de autoridades	Rueda de prensa / comunicado escrito	Vocero CIEV
Autoridades	Magnitud del impacto económico, necesidades del sector privado, propuestas de solución	Reunión directa, carta oficial	Director CIEV + Junta
Redes sociales	Mensajes cortos, verificados, sin especulación. Desmentir desinformación oportunamente	Twitter/X, LinkedIn, Instagram	Dir. Comunicaciones CIEV

5. PLAN DE CONTINUIDAD DE NEGOCIO – MEDIDAS TRANSVERSALES

5.1 Medidas preventivas (ANTES del evento)

- Actualizar el inventario de activos críticos de cada empresa (mínimo anual).
- Establecer y probar rutas alternas de transporte al menos una vez al trimestre.
- Mantener inventarios de seguridad de materias primas críticas para mínimo 15 días de operación.
- Revisar y actualizar las pólizas de seguros (patrimonial, responsabilidad civil, interrupción de negocio, extorsión).
- Implementar sistemas de respaldo energético (UPS, planta eléctrica) en instalaciones críticas.
- Capacitar al personal en el protocolo de actuación (mínimo dos veces al año).
- Establecer acuerdos de ayuda mutua entre empresas del mismo gremio.
- Suscribir convenios con proveedores en otras regiones como contingencia.

5.2 Medidas de mitigación (DURANTE el evento)

- Activar el Comité de Crisis del CIEV en las primeras 2 horas de confirmado el evento.
- Implementar el teletrabajo para personal administrativo y comercial.
- Priorizar la seguridad del personal sobre la continuidad operativa.
- Activar canales de comunicación alternos (radio, satelital, datos móviles de respaldo).
- Coordinar con autoridades para garantizar corredores humanitarios y de carga esencial.
- Documentar en tiempo real todos los impactos económicos para efectos de seguros y reclamos legales.

5.3 Medidas de recuperación (DESPUÉS del evento)

- Evaluación de daños en las primeras 24 horas: activos, contratos, reputación.
- Activar procedimiento de reclamación a aseguradoras con documentación completa.
- Plan de despacho prioritario para ponerse al día con compromisos comerciales.
- Sesión de lecciones aprendidas del Comité de Crisis (máximo 72 horas después del evento).
- Actualización de la matriz de riesgos y del presente protocolo con base en los aprendizajes.
- Informe a la Junta Directiva del CIEV con análisis del impacto y recomendaciones.

6. ARTICULACIÓN CON AUTORIDADES MILITARES, POLICÍA Y GOBIERNO

La efectividad del protocolo depende de la articulación permanente con las entidades del Estado. El CIEV debe mantener canales de comunicación directos y activos con las siguientes instancias:

ENTIDAD	MECANISMO DE ARTICULACIÓN	COMPROMISOS ESPERADOS
Gobernación del Valle Sec. de Seguridad	Mesa de Seguridad Empresarial mensual; alertas tempranas vía WhatsApp oficial	Información anticipada de riesgos, coordinación de corredores humanitarios, mediación en conflictos

Alcaldía de Cali Sec. de Seguridad y Justicia	Comité de Seguridad Empresarial Cali; reunión mensual o ante eventos	Vigilancia de zonas empresariales, respuesta rápida ante disturbios, coordinación tránsito
Policía Metropolitana de Cali Policía de Carreteras	Línea directa con comandante operativo; protocolo de respuesta <30 minutos en zonas empresariales	Custodiar instalaciones empresariales, despejar accesos, escoltar convoyes de carga esencial
Ejército Nacional Tercera Brigada	Contacto directo para alertas de terrorismo y sabotaje; protocolo de denuncia inmediata	Protección de infraestructura crítica, control de zonas en estado de emergencia
Fiscalía / SIJIN / GAULA	Canal de denuncia directa para extorsión, amenazas y sabotaje; reportes confidenciales	Investigación y judicialización de actores criminales que afecten al sector empresarial
Mintransporte / Invías	Reporte de bloqueos para gestión de habilitación de corredores; mesa nacional de logística	Declaratoria de emergencia vial, habilitación de rutas alternativas, corredores humanitarios

7. INDICADORES DE DESEMPEÑO Y MONITOREO (ISO 31000 § 6.6)

INDICADOR	FÓRMULA / MEDICIÓN	META	FRECUENCIA	RESPONSABLE
Tiempo de activación del Comité de Crisis	Tiempo entre alerta y primera sesión del Comité	**< 2 horas**	Por evento	Dir. CIEV
Cobertura del protocolo en gremios	% de empresas afiliadas con protocolo implementado	**>80%**	Trimestral	CIEV
Efectividad de rutas alternas	% de entregas completadas durante bloqueos usando rutas alternas	**>70%**	Por evento	Coord. Logístico
Tiempo medio de recuperación (RTO)	Tiempo entre interrupción y reanudación de operaciones críticas	**< 48h**	Por evento	Gerentes Operac.
Capacitación en protocolo	% de personal clave capacitado en el protocolo	**100%**	Semestral	RRHH
Actualización de la matriz de riesgos	Fecha de última actualización de la Matriz ISO 31000	**< 3 meses**	Trimestral	Of. Seguridad CIEV

8. CICLO DE REVISIÓN Y MEJORA CONTINUA (ISO 31000 § 6.7)

El presente protocolo es un documento vivo que debe actualizarse continuamente con base en:

- Ocurrencia de nuevos eventos de riesgo materializados.
- Cambios en el contexto político, social o de seguridad del Valle del Cauca.
- Lecciones aprendidas de la activación del Comité de Crisis.
- Resultados de los ejercicios de simulacro del protocolo.
- Retroalimentación de las empresas afiliadas y de las autoridades coordinadoras.

ACTIVIDAD DE REVISIÓN	FRECUENCIA	RESPONSABLE	EVIDENCIA
Actualización de la Matriz de Riesgos	Trimestral o por evento	Oficial Seguridad CIEV	Matriz actualizada + acta
Revisión del árbol de contactos	Mensual	Dir. Ejecutivo CIEV	Directorio actualizado
Simulacro del protocolo	Semestral	Comité de Crisis	Informe post-simulacro
Sesión de la Junta Directiva CIEV	Mensual	Presidente CIEV	Acta de reunión
Actualización del protocolo	Cada 6 meses o por evento crítico	Dir. Ejecutivo + Junta	Protocolo versión nueva + registro de cambios

9. APROBACIÓN Y FIRMAS

ELABORÓ	REVISÓ	APROBÓ
Comite de Seguridad CIEV Firma: _____ Nombre: Fecha:	Director Ejecutivo CIEV Firma: _____ Nombre: Fecha:	Presidente Junta Directiva CIEV Firma: _____ Nombre: Fecha:

NOTA LEGAL: Este protocolo es de uso interno del CIEV y sus gremios afiliados. Su implementación es responsabilidad de cada empresa. El CIEV actúa como coordinador y facilitador, sin asumir responsabilidad directa por las decisiones empresariales individuales. Este documento no reemplaza la asesoría jurídica o de seguridad especializada.