



CCD
COMPAÑÍA DE
CIBERSEGURIDAD
Y DEFENSA

RFC 2350 CCD CYBERPRO

octubre de 2026

CCD COMPAÑÍA DE CIBERSEGURIDAD Y DEFENSA S.A.S

Contenido

RFC 2350 CCD CYBERPRO	1
1. INTRODUCCIÓN.....	3
2. INFORMACIÓN DEL DOCUMENTO.....	3
2.1. FECHA DE LA ÚLTIMA ACTUALIZACIÓN.....	3
2.2. LISTAS DE DISTRIBUCIÓN PARA NOTIFICACIONES.....	3
2.3. UBICACIÓN DEL DOCUMENTO.....	3
3. INFORMACIÓN DE CONTACTO.....	3
3.1. NOMBRE DEL EQUIPO.....	3
3.2. DIRECCIÓN.....	3
3.3. ZONA HORARIA.....	3
3.4. NÚMEROS TELEFÓNICOS.....	4
3.5. NÚMERO DE FAX.....	4
3.6. DIRECCIÓN DE CORREO ELECTRÓNICO.....	4
3.7. MIEMBROS DEL EQUIPO.....	4
3.8. INFORMACIÓN ADICIONAL.....	4
3.9. HORARIO DE ATENCIÓN.....	4
3.10. PUNTOS DE CONTACTO PARA LA COMUNIDAD OBJETIVO.....	4
4. CONSTITUCIÓN.....	5
4.1. MISIÓN.....	5
4.2. COMUNIDAD OBJETIVO.....	5
4.3. PATROCINIO Y AFILIACIÓN.....	5
4.4. AUTORIDAD.....	5
5. POLÍTICAS.....	6
5.1. TIPOS DE INCIDENTES Y NIVEL DE SOPORTE.....	6
5.2. COOPERACIÓN, INTERACCIÓN Y DIVULGACIÓN DE LA INFORMACIÓN.....	6
5.3. COMUNICACIÓN Y AUTENTICACIÓN.....	7
6. SERVICIOS.....	8
7. FORMULARIOS DE REPORTE DE INCIDENTES.....	9
8. OMISIÓN DE RESPONSABILIDAD.....	9
9. APROBACIÓN, VIGENCIA Y REVISIÓN.....	9

1. INTRODUCCIÓN

El presente documento describe a CCD CYBERPRO, el Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT) de CCD Compañía de Ciberseguridad y Defensa S.A.S., Su propósito es dar a conocer a la comunidad objetivo, a los equipos pares y a las comunidades de confianza la información de contacto, la constitución, las políticas y los servicios del CSIRT.

Este documento es de carácter público y está clasificado como TLP:CLEAR; puede ser distribuido sin restricción.

2. INFORMACIÓN DEL DOCUMENTO

2.1. Fecha de la última actualización

Versión 1, publicada el 30 de octubre de 2026.

2.2. Listas de distribución para notificaciones

No existe una lista de distribución para notificar cambios en este documento. Las actualizaciones se publican en la ubicación indicada en el numeral 2.3.

2.3. Ubicación del documento

La versión vigente de este documento se encuentra disponible en: <https://ccd.com.co/wp-content/uploads/2026/10/ING-OTR-002-V1-C-RFC-2350-CCD-CYBERPRO.pdf>

3. INFORMACIÓN DE CONTACTO

3.1. Nombre del equipo

CCD CYBERPRO – CSIRT de CCD Compañía de Ciberseguridad y Defensa S.A.S.

3.2. Dirección

Avenida Calle 26 # 68C-61, Edificio Torre Central Davivienda , Oficina 632, Bogotá D.C., Colombia.

3.3. Zona horaria

América/Bogotá (UTC-05:00). Colombia.

RFC 2350 CCD CYBERPRO	CÓDIGO: ING-OTR-002-V1-C
	VERSIÓN: 1
	FECHA DE EMISIÓN: 20-10-2026
	PÁGINA:4

3.4. Números telefónicos

- Línea de soporte 7x24: +57 310 819 9719.
- Teléfono corporativo: +57 601 390 2500.

3.5. Número de fax

No disponible.

3.6. Dirección de correo electrónico

ingenieria@ccd.com.co, mdr@ccd.com.co – canales oficiales la coordinación técnica con CSIRT pares y comunidades de confianza.

soporte@ccd.com.co – Canal oficial de reporte de incidentes de clientes.

3.7. Miembros del equipo

El CCD CYBERPRO es liderado por el Gerente de Operaciones de CCD, con el apoyo del Coordinador de Servicios de Ingeniería. El equipo cuenta con una estructura fija de Ingenieros de Proyectos e Ingenieros de Soporte capacitados para desempeñar las funciones operativas esenciales, cubrir ausencias, con esquemas de respaldo y entrenamiento cruzado que garantizan la continuidad del servicio.

La información de contacto individual de los integrantes se suministra a los equipos pares y a la comunidad objetivo cuando es requerida para la coordinación de incidentes.

3.8. Información adicional

Información general sobre CCD y sus servicios se encuentra disponible en <https://ccd.com.co/portafolio-de-soluciones/>

3.9. Horario de atención

El servicio de detección y respuesta gestionada opera 7x24, los 365 días del año.

3.10. Puntos de contacto para la comunidad objetivo

Los clientes de la comunidad objetivo pueden contactar al CSIRT a través de los siguientes canales:

- Canal primario: soporte@ccd.com.co
- Correo electrónico: mdr@ccd.com.co

- **Canal de emergencia (incidentes P1/P2):** “war room” (virtual o presencial) con responsables técnicos y de negocio, línea de soporte 7x24, contacto telefónico y/o mensajería corporativa autorizada para activación inmediata.
- **Canal fuera de banda:** cuando se sospecha compromiso del correo corporativo del cliente, se utiliza un canal alternativo previamente acordado.

Los CSIRT pares y las comunidades de confianza pueden contactar al equipo por correo electrónico, identificando la etiqueta TLP de la información compartida.

4. CONSTITUCIÓN

4.1. Misión

CCD CYBERPRO tiene como misión prevenir, recibir, analizar, coordinar y responder de manera oportuna y efectiva a eventos e incidentes de seguridad de la información que afecten o puedan afectar a su comunidad objetivo, contribuyendo a la protección de la confidencialidad, integridad y disponibilidad de la información, la continuidad de los servicios, la reducción del riesgo cibernético y la mejora continua de las capacidades de gestión de incidentes.

4.2. Comunidad objetivo

La comunidad objetivo de CCD CYBERPRO está conformada por los clientes de CCD que han contratado los servicios de detección y respuesta gestionada (MDR), búsqueda proactiva de amenazas (Threat Hunting) y gestión de exposición y riesgo (XRM), bajo acuerdos contractuales. Actualmente incluye organizaciones de los sectores de educación, salud, gobierno, empresas privadas y comercio en Colombia.

4.3. Patrocinio y afiliación

CCD CYBERPRO es un equipo interno de CCD Compañía de Ciberseguridad y Defensa S.A.S., empresa colombiana de servicios de ciberseguridad, que lo financia y lo gestiona dentro del proceso de Ingeniería, subproceso de servicios avanzados. CCD CYBERPRO promueve la participación en comunidades técnicas y redes de confianza nacionales, sectoriales e internacionales, incluyendo FIRST.

4.4. Autoridad

CCD CYBERPRO opera bajo el mandato formal otorgado por la Alta Dirección de CCD, que le asigna la responsabilidad de gestionar los incidentes de seguridad de su comunidad objetivo. Dentro de ese mandato, CCD CYBERPRO está autorizado para:

- Coordinar la respuesta ante incidentes en la comunidad objetivo.
- Acceder a los sistemas, registros, telemetría y evidencias estrictamente necesarios para la investigación y atención de incidentes.
- Solicitar o ejecutar acciones de contención, como aislamiento de equipos o bloqueo de cuentas e indicadores de compromiso, conforme a la matriz de autoridad y a los acuerdos con cada cliente.
- Emitir directrices operativas temporales durante la gestión de incidentes.
- Escalar incidentes críticos a la Alta Dirección y a los niveles de gobierno del cliente.
- Intercambiar información técnica con CSIRT pares, CSIRT nacionales y sectoriales, comunidades de confianza y proveedores de tecnología.

5. POLÍTICAS

5.1. Tipos de incidentes y nivel de soporte

CCD CYBERPRO atiende incidentes de seguridad de la información que afecten a su comunidad objetivo, entre ellos: compromiso de cuentas, malware, actividad anómala en endpoints, red o perímetro, amenazas a aplicaciones, filtración o exfiltración de información y otros eventos que, tras el triage, sean clasificados como maliciosos o de alto riesgo.

El nivel de soporte depende de la severidad del incidente, determinada por la criticidad del activo, el impacto real o potencial sobre la confidencialidad, integridad y disponibilidad, el alcance, la evidencia de compromiso y la exposición.

5.2. Cooperación, interacción y divulgación de la información

CCD CYBERPRO reconoce la importancia de la cooperación entre equipos de respuesta a incidentes y coopera con CSIRT pares, CSIRT nacionales y sectoriales, comunidades de confianza y proveedores de tecnología con el fin de prevenir, detectar, contener o resolver incidentes. Este intercambio se rige por los siguientes principios:

- **Confidencialidad por defecto:** toda información relacionada con incidentes, vulnerabilidades, clientes, infraestructura, evidencias o inteligencia de amenazas se trata como confidencial salvo clasificación expresa diferente. La información recibida sin etiqueta se trata inicialmente como confidencial y, cuando es necesario, se solicita aclaración al remitente.
- **Necesidad de conocer y mínimo privilegio:** la información solo se comparte con personas o entidades que requieren conocerla para ejecutar una función autorizada.

RFC 2350 CCD CYBERPRO	CÓDIGO: ING-OTR-002-V1-C
	VERSIÓN: 1
	FECHA DE EMISIÓN: 20-10-2026
	PÁGINA:7

- **Respeto a las restricciones del origen:** el CCD CYBERPRO acata las etiquetas TLP, acuerdos de confidencialidad, contratos y restricciones regulatorias definidas por quien entrega la información. Compartir información más allá de lo permitido por la etiqueta recibida requiere autorización expresa del originador.
- **Protección de la comunidad objetivo:** la información que involucra datos o la identidad de un cliente solo se comparte con su autorización. Cuando es posible se aplica anonimización.
- **Uso exclusivo para fines autorizados:** la información recibida se utiliza únicamente para actividades de prevención, detección, análisis, contención, erradicación, recuperación, coordinación o mejora del servicio.
- **Divulgación responsable de vulnerabilidades:** cuando el CCD CYBERPRO identifica una vulnerabilidad, procura minimizar el riesgo para las partes afectadas y coordina la divulgación con los actores involucrados.
- **Comunicación institucional:** las declaraciones públicas, la atención a medios de comunicación y las notificaciones oficiales a autoridades o reguladores requieren autorización expresa de la Alta Dirección. Las notificaciones a terceros relacionadas con incidentes de un cliente son decisión del cliente, con el soporte técnico de CCD CYBERPRO.
- **Cumplimiento legal:** el tratamiento de datos personales e información regulada se realiza conforme a la legislación colombiana aplicable, las obligaciones contractuales y los acuerdos de confidencialidad. La información sujeta a normas de privacidad de otras jurisdicciones se maneja según las restricciones comunicadas por el originador.

CCD CYBERPRO adopta el Traffic Light Protocol (TLP) versión 2.0 de FIRST como mecanismo mínimo para comunicar restricciones de distribución:

5.3. Comunicación y autenticación

- El correo electrónico es el medio definido para la comunicación con CSIRT pares y comunidades de confianza y clientes de acuerdo al definido en el numeral 3.6 del presente documento.
- La información se transmite por canales aprobados, priorizando comunicaciones cifradas, autenticadas y trazables.
- En correos y mensajes, la etiqueta TLP se ubica en el asunto o encabezado del mensaje; en documentos, se incluye de forma visible en el encabezado.
- Antes de compartir información, el responsable del caso valida que el destinatario está autorizado, que existe necesidad de conocer y que la distribución respeta la etiqueta TLP y cualquier restricción adicional del origen.

6. SERVICIOS

CCD CYBERPRO presta los siguientes servicios, alineados con el FIRST CSIRT Services Framework, a los clientes de su comunidad objetivo de acuerdo con el alcance contratado. Todos los servicios operan en modalidad 7x24.

Servicio	Descripción
Monitoreo y detección	Identificar de forma temprana posibles incidentes, ataques, intrusiones o violaciones de políticas de seguridad.
Análisis de eventos	Clasificar cada alerta como un incidente real (verdadero positivo) o descartarla como falsa alarma.
Recepción de reportes de incidentes de seguridad de la información	Recibir y registrar reportes de incidentes por los canales autorizados, asignando ticket, prioridad y responsable.
Análisis de incidentes de seguridad de la información	Identificar las debilidades o fallas de diseño (causas raíz) que permitieron el éxito del compromiso.
Análisis de artefactos y evidencias forenses	Reconstruir las acciones del atacante, evaluar daños y preservar evidencia digital válida legalmente.
Mitigación y recuperación	Ejecutar planes de contención, aislamiento de activos e identidades y restauración de sistemas.
Coordinación de incidentes de seguridad de la información	Coordinar la respuesta con clientes, CSIRT y proveedores, comunicando estado, acciones y cierre del incidente bajo TLP.
Respuesta a vulnerabilidades	Búsqueda activa mediante escaneos de seguridad en sistemas y despliegue de parches o mitigaciones.
Análisis y síntesis	Evaluación técnica de tendencias internas y externas y búsqueda proactiva de amenazas basada en hipótesis.

7. FORMULARIOS DE REPORTE DE INCIDENTES

Los clientes de la comunidad objetivo reportan incidentes a través del correo soporte@ccd.com.co. Los CSIRT pares y demás partes interesadas pueden reportar incidentes por correo electrónico a mdr@ccd.com.co o ingenieria@ccd.com.co, incluyendo como mínimo la siguiente información:

- Nombre, organización y datos de contacto de quien reporta.
- Fecha y hora de detección.
- Descripción del incidente y activos o servicios afectados.
- Etiqueta TLP de la información compartida (no aplica para clientes).

8. OMISIÓN DE RESPONSABILIDAD

CCD CYBERPRO no asume responsabilidad por errores, omisiones o mal uso de la información contenida en este documento

9. APROBACIÓN, VIGENCIA Y REVISIÓN

El presente documento es aprobado por la Gerencia General de CCD. Su revisión se realizará como mínimo una vez al año o cuando se presenten cambios significativos en la información de contacto, la constitución, las políticas o los servicios del CSIRT. La versión vigente se publicará en la ubicación indicada en el numeral 2.3.