2026

Centro de Respuestas a Incidentes Informáticos
CSIRT Académico UNAD

# DPO como Pilar de la Confianza Digital

## ELEMENTO CLAVE PARA GARANTIZAR TRANSPARENCIA, ÉTICA Y RESPONSABILIDAD EN EL USO DE LA INFORMACIÓN

VIEM
Vicerrectoría de Innovación y Emprendimiento

ECBTI
Escuela de Ciencias Básicas, Tecnología e Ingeniería

Semillero de Investigación
Ceros y Unos

E-boletín Informativo CSIRT Académico UNAD

Medio de divulgación: Correo Electrónico, Sitio Web

Incluye: Noticias, alertas o informes relacionados con la disciplina de la ciberseguridad

Número treinta y seis [36]
Febrero de 2026

Universidad Nacional Abierta y a Distancia (UNAD)
Vicerrectoría de Innovación y Emprendimiento (VIEM)
Escuela de Ciencias Básicas Tecnología Ingeniería (ECBTI)
Maestría en Ciberseguridad
Especialización en Seguridad Informática
CSIRT Académico UNAD

Universidad Nacional Abierta y a Distancia
Calle 14 sur No. 14-23 | Bogotá D.C
Correo electrónico:
csirt@unad.edu.co
Página web: https://csirt.unad.edu.co



Edición electrónica, financiada por la Universidad Nacional Abierta y a Distancia (UNAD)

Vicerrectoría de Innovación y Emprendimiento (VIEM)
Ing. Andrés Ernesto Salinas
Vicerrector

Escuela de Ciencias Básicas Tecnología e Ingeniería (ECBTI)
Ing. Claudio Camilo González Clavijo
Decano

Maestría en Ciberseguridad (ECBTI)
Ing. Sonia Ximena Moreno Molano
Líder Programa de Maestría en Ciberseguridad

**Semillero de Investigación Ceros y Unos, adscrito al Grupo de Byte InDesign**

**Centro de Desarrollo Tecnológico CSIRT Académico UNAD**
Ing. Luis Fernando Zambrano Hernández
Líder CSIRT Académico UNAD

Responsable de la Edición
Ing. Luis Fernando Zambrano Hernandez

Revisó
Adm. Libardo Cárdenas Corral
Analista CSIRT Académico UNAD

Estado legal:
Periodicidad: Mensual
ISSN: 2806-0164

# Contenido

## Introducción

En la actual economía digital, la protección de los datos personales ha dejado de ser una obligación solo de orden normativo para convertirse en un componente esencial de la confianza institucional, la legitimidad organizacional y la sostenibilidad de la transformación digital. En este contexto, la figura del Delegado de Protección de Datos - DPO adquiere una relevancia estratégica al articular principios de transparencia, ética, cumplimiento y gestión del riesgo en torno al tratamiento responsable de la información. Este documento plantea que la confianza digital no se construye únicamente mediante controles técnicos o exigencias legales, sino a partir de una cultura organizacional que reconozca el valor del dato, respete los derechos de los titulares y promueva decisiones informadas desde la privacidad por diseño y por defecto. Asimismo, expone la necesidad de consolidar modelos de gobernanza, métricas de madurez y mecanismos de coordinación entre áreas jurídicas, técnicas y directivas, especialmente en el contexto colombiano, donde la adopción del DPO representa una oportunidad para fortalecer la responsabilidad institucional frente al uso de la información. Así, el DPO emerge no solo como una figura de supervisión, sino como un actor clave para impulsar confianza digital, innovación responsable y protección efectiva de los datos personales

# DPO [1]como Pilar de la Confianza Digital

Elemento clave para garantizar transparencia, ética y responsabilidad en el uso de la información

**Autores**

**Luis Fernando Zambrano Hernandez**
Docente Investigador
Líder CSIRT Académico UNAD
Universidad Nacional Abierta y a Distancia
ORCID: 0000-0002-4690-3526

**Hernando José Peña Hidalgo**
Docente Investigador
CSIRT Académico UNAD
Universidad Nacional Abierta y a Distancia
ORCID: 0000-0002-3477-2645

**Sonia Ximena Moreno Molano**
Líder Maestría en Ciberseguridad
Universidad Nacional Abierta y a Distancia
ORCID: 0000-0003-0392-1983

**Néstor Raúl Cárdenas Corral**
Analista CSIRT Académico UNAD
Universidad Nacional Abierta y a Distancia
ORCID: orcid.org/0000-0003-3691-0148

## La Era de la Confianza Digital: Datos como Activo Estratégico

En el entorno contemporáneo, los datos personales trascienden su carácter documental para convertirse en un activo estratégico que define ventajas competitivas, legitimidad institucional y resiliencia frente a riesgos. La confianza digital, entonces, no es un adorno: es la base sobre la cual las organizaciones deben erigir su modelo de gobernanza de datos. El documento "DPO: Pilar estratégico en la gestión de datos personales" (Muñoz Gutiérrez, 2025) orienta esta mirada al proponer que el DPO no solo administre el cumplimiento, sino que construya puentes entre la ética, la transparencia y la innovación.

Desde una perspectiva global, el fortalecimiento de confianza en las instituciones públicas ha sido adoptada como prioridad por organismos multilaterales. Por ejemplo, el informe Building Trust and Reinforcing Democracy del (OECD, 2022) examina los principales "motores de la confianza" fiabilidad, apertura, integridad, justicia y los vínculos con la gobernanza pública.

Este enfoque es particularmente relevante al trasladarlo al ámbito de la privacidad: si las instituciones de todo tipo, empresas, gobiernos, instituciones académicas no promueven la transparencia en

[1] Delegado de Protección de Datos

el uso de datos, socavan su propio capital reputacional.
Además, experiencias durante la crisis global del COVID-19 evidenciaron cómo las tecnologías de rastreo y uso de big data generaron tensiones entre la salud pública y los derechos individuales. En Big Data, Privacy and COVID-19 - Learning from Humanitarian Expertise in Data Protection, (Zwitter & Gstrein, 2020) analizan cómo las respuestas de emergencia forzaron límites a la protección de datos, subrayando la importancia de contar con marcos éticos y operativos robustos incluso en crisis. Ese equilibrio entre utilidad y respeto de derechos ilustra la urgencia de institucionalizar confianza digital.

Para Colombia, esta era exige un salto cualitativo, pasar de visiones fragmentadas del cumplimiento reglamentario hacia arquitecturas integradas de gobernanza de datos personales. La Ley 1581 de 2012 y las directrices de la Superintendencia de Industria y Comercio crean una base legal obligatoria, pero la confianza digital se consolida cuando las instituciones internalizan principios de privacidad por diseño, transparencia continua y respeto de la autodeterminación informativa.

## Privacidad con Propósito. Hoja de ruta para instituciones

En un mundo donde las amenazas cibernéticas evolucionan constantemente y donde los usuarios exigen mayor control sobre sus datos, la privacidad ya no puede verse como un requisito opcional; debe ser el eje motor de toda estrategia institucional.

Esta hoja de ruta propone que las organizaciones aborden la privacidad con propósito, integrándola desde el diseño hasta la operación, y empoderando al Delegado de Protección de Datos como actor clave en ese proceso.

***Principios de diseño***

Las instituciones deben adoptar desde el inicio los principios de privacidad por diseño y privacidad por defecto, asegurando que cada sistema, servicio o aplicación incorpore salvaguardas técnicas y organizacionales que protejan los derechos de los titulares. (Ježová, 2020) describe con claridad estos conceptos, señalando que la recolección mínima, la anonimización, la separación de datos y los ajustes predeterminados más restrictivos

son esenciales para cumplir con estándares legales y éticos.

Además, el análisis comparativo entre enfoques de "Security by Design Privacy by Design" revela cómo estas estrategias convergen en la práctica para anticipar riesgos y reforzar resiliencia institucional. (Del-Real et al., 2025)

***Tecnologías de mejora de la privacidad (PETs) y métodos técnicos***

Las Privacy Enhancing Technologies (PETs) permiten que las organizaciones realicen análisis de datos de forma segura, preservando la confidencialidad cuando sea posible. El reporte Privacy and Data Protection by Design – from policy to engineering (Danezis et al., 2015) expone un catálogo de estrategias y bloques constructivos (anonimización, encriptación, control de acceso, compartimentación) que pueden adaptarse a las necesidades institucionales. (European Network and Information Security Agency., 2014).

En el contexto del big data y el análisis masivo, D'Acquisto et al. (2015) muestran cómo integrar PETs a lo largo del ciclo de vida del dato desde la captura hasta la visualización permite "big data con privacidad", mitigando riesgos de perfilado y exposición indebida. (Perera et al., 2016). Asi mismo, para entornos IoT (Internet de las cosas), Perera et al. (2016) proponen un marco de evaluación basado en privacidad que ayuda a detectar fallas de diseño y garantizar que cada nodo del sistema respete los principios fundamentales de privacidad

***Gobernanza institucional, cultura y formación***

Implementar privacidad con propósito exige estructuras de gobernanza claras, roles definidos y capacitación constante. En ese sentido, Ciclosi y Massacci conceptualizan al DPO como un rol híbrido: con competencias en derecho, gestión y ciberseguridad. Ellos lo ubican entre quienes auditan cumplimiento y quienes asesoran la estrategia. Un mediador técnico y normativo esencial. (Ciclosi & Massacci, 2023)

Asimismo, Šidlauskas analiza cómo las organizaciones deben evitar conflictos de interés en la designación del DPO, asegurando su independencia funcional, capacitación continua y acceso directo a la alta dirección. (Šidlauskas, 2021). La formación interna debe contemplar cursos modulares técnicos (criptografía, seguridad de redes, análisis de amenazas),

legales (regulación nacional e internacional) y éticos (privacidad como derecho). Además, se recomienda establecer canales de reporte seguros, evaluaciones de riesgo periódicas y auditorías independientes.

***Implementación progresiva: fases y métricas***

Una hoja de ruta pragmática puede seguir fases escalonadas:

Fase 0 – Diagnóstico: mapeo de flujos de datos personales, evaluación de brechas de seguridad y revisión de cumplimiento legal.

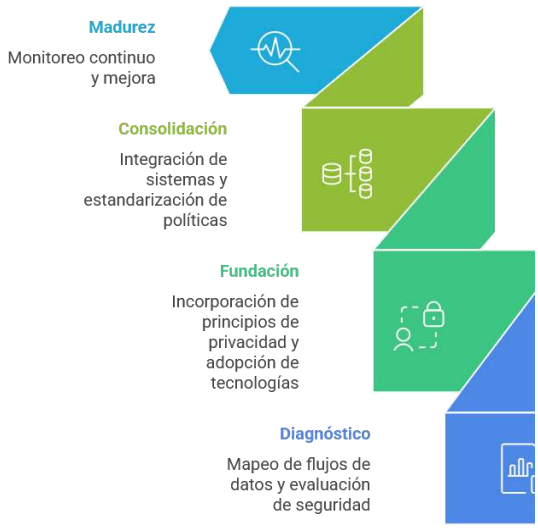
Fase 1 – Fundación: incorporar principios de PbD[2] /PbDf[3] en desarrollos nuevos, adoptar PETs[4] clave (anonimización, cifrado) y designar un responsable institucional de protección de datos.

Fase 2 – Consolidación: integrar los sistemas legados, estandarizar políticas, realizar auditorías internas y pruebas de penetración, capacitar equipos multidisciplinarios.

Fase 3 – Madurez y adaptación continua: monitoreo permanente, cultura de mejora, benchmarking frente a estándares internacionales.

**Ilustración 1.**

*Logro de madurez para la protección de los datos*




Elaboración propia apoyada por IA. Napkin (2026).

Las métricas clave incluyen número de incidentes reportados, tiempos de respuesta, porcentaje de sistemas con privacidad por diseño, nivel de cumplimiento de auditorías y confianza percibida por usuarios.

## Cultura Organizacional y Gobernanza de Datos

Para que la privacidad deje de ser un asunto técnico aislado y se convierta en parte del ADN institucional, las organizaciones deben cultivar una cultura de datos responsable y respaldarla mediante una

[2] Privacidad desde el diseño
[3] Privacidad por defecto
[4] Tecnologías de Mejora de la Privacidad

gobernanza sólida. A continuación, se hace una propuesta de cómo lograr esa transformación desde el liderazgo hasta cada funcionario.

***Gobernanza de datos: arquitectura institucional compartida***

La gobernanza de datos personales no puede residir en una sola dependencia. Debe estructurarse mediante mecanismos claros de coordinación, rol compartido y responsabilidades definidas.

Algunas recomendaciones clave:

- Comité de Gobernanza de Datos: integrado por TI, jurídico, riesgos, seguridad, auditoría y representantes de procesos de negocio. Este comité revisa políticas, auditorías y tendencias emergentes.
- Políticas y manuales de gobernanza: documentos actualizados que guíen la gestión de consentimiento, retención, acceso, anonimización, transferencia y reporte de incidentes.
- Modelos de reporte y escalamiento: definir cómo los incidentes o quejas llegan al DPO, al comité y a la alta dirección.
- Ciclo de vida del dato: mapear flujos de recolección, almacenamiento, uso, cesión, archivo o destrucción de datos personales, para cada sistema y proceso relevante.
- Comité de Ética de Datos (opcional): instancia que evalúa proyectos de innovación (IA, analítica avanzada, machine learning) desde la perspectiva del riesgo de privacidad.

Este modelo institucional facilita la cooperación entre áreas y otorga al DPO el soporte requerido para cumplir su rol estratégico sin que recaiga toda la carga en él.

***La cultura institucional como motor de cambio***

Incorporar la privacidad como valor organizacional implica cultivar mentalidades, hábitos y herramientas entre todos los colaboradores. Por ejemplo:

- Campañas de sensibilización continuas, que pueden ser infografías, cápsulas de formación, casos reales de violaciones de datos para ilustrar consecuencias.
- Formación segmentada, desde ejecutivos hasta operarios de sistemas

según nivel, rol y exposición al dato.
- Embajadores voluntarios en cada área que promueven buenas prácticas de manejo de datos.
- Reconocimiento e incentivos a partir de premios internos o reconocimientos cuando unidades muestran buenas métricas de gobernanza (minimización, cumplimiento de auditorías, innovación segura).
- Espacios de retroalimentación a través de buzones anónimos para reportar preocupaciones de privacidad o sugerencias de mejora.

Cuando la cultura de privacidad se arraiga, la capacidad de adaptación operativa mejora, los empleados actúan con criterio proactivo y se reduce la dependencia de controles rígidos.

**Sinergias entre DPO, TI, seguridad y compliance**

Para que la privacidad opere de forma integrada, el DPO debe coordinar estrechamente con las áreas técnicas y de cumplimiento:

**Tabla 1.**
*Sinergia entre unidades o dependencias, seguridad y cumplimiento*

| Área | Rol complementario con el DPO |
|---|---|
| **TI - Desarrollo de software** | Incorporar controles técnicos (cifrado, acceso mínimo, logging) y evaluar la viabilidad de PETs en proyectos nuevos. |
| **Seguridad informática, de la información y ciberseguridad** | Participar en análisis de riesgos, pruebas de penetración, respuesta ante incidentes y mitigación de vulnerabilidades. |
| **Compliance y/o Auditoría interna** | Validar cumplimiento regulatorio, auditar procesos relacionados con datos personales y proponer mejoras. |
| **Comunicación y Marketing** | Diseñar mensajes transparentes sobre uso de datos, gestionar publicidad responsable y atender peticiones de titulares. |
| **Recursos Humanos** | Incluir cláusulas de privacidad en contratos laborales, formar al personal en manejo de datos sensibles, custodiar expedientes. |

Elaboración propia

Este enfoque colaborativo permite que el DPO actúe como nodo clave entre riesgo legal, riesgo técnico y reputación institucional.

## Modelos de madurez y métricas de gobernanza

Una forma práctica de avanzar es mediante niveles de madurez en gobernanza de datos, así:

- Cumplimiento básico de leyes y controles mínimos.
- Políticas institucionales documentadas y roles asignados.
- Monitoreo de KPI, reportes regulares, auditorías internas sobre privacidad.
- Procesos automatizados, uso de PETs, mejoras proactivas.
- Privacidad integrada, innovación responsable, reputación de confianza.

***Algunas métricas sugeridas:***

- Porcentaje de sistemas con privacidad integrada desde el diseño.
- Número de incidentes de datos detectados vs mitigados.
- Tiempos promedio de respuesta a solicitudes de titulares.
- Número de unidades que cuentan con embajadores voluntarios.
- Resultados de auditorías internas y externas sobre cumplimiento de privacidad.

**Ilustración 2.**

*Etapas de madurez de la privacidad desde el cumplimiento básico hasta la innovación integrada.*


Elaboración propia en Napkin (2025)

## Rol del Delegado de Protección de Datos (DPO) en Colombia

En la economía digital actual, donde la información se ha convertido en el principal activo estratégico de las organizaciones, el Delegado de Protección de Datos DPO emerge como un garante de confianza, transparencia y cumplimiento ético. Su función trasciende la interpretación de la norma: representa la consolidación de un modelo de *gobernanza responsable del dato*, que equilibra los intereses corporativos con los derechos fundamentales de los ciudadanos

***Fundamentos y evolución del rol en el contexto colombiano***

El DPO tiene su origen en el modelo europeo establecido por el Reglamento General de Protección de Datos (GDPR) (UE, 2016), particularmente en los artículos 37 a 39. Allí se define su posición como un asesor independiente, encargado de supervisar el cumplimiento normativo, asesorar a la alta dirección y servir de enlace con las autoridades de control.

En Colombia, aunque la figura del DPO no es aún obligatoria por ley, su adopción se enmarca en las mejores prácticas de cumplimiento y gobernanza de datos recomendadas por la Superintendencia de Industria y Comercio (SIC). La Ley 1581 de 2012 y el Decreto 1377 de 2013[5] establecen los principios rectores del tratamiento de datos personales promueven la designación de un responsable de privacidad que ejerza funciones similares a las del DPO europeo, especialmente en organizaciones que gestionan bases de datos de alto riesgo o gran volumen.

***Funciones estratégicas del DPO***

El DPO se concibe como una figura interdisciplinaria que articula derecho, tecnología, gestión del riesgo y comunicación. Entre sus principales responsabilidades se destacan:

- Asesoramiento normativo: interpretar la Ley 1581/2012, su reglamentación y los principios de la OCDE sobre protección de la privacidad y flujos transfronterizos.
- Supervisión y cumplimiento: verificar la implementación de políticas, procedimientos y medidas de seguridad de la información.
- Gestión de riesgos: liderar evaluaciones de impacto en la protección de datos - DPIA y auditorías preventivas sobre tratamientos de datos sensibles.
- Capacitación y cultura organizacional: impulsar programas de formación interna y estrategias de concienciación.
- Vínculo con la autoridad: actuar como punto de contacto ante la SIC y canalizar las solicitudes o reclamos de los titulares.
- Integración con el ecosistema de ciberseguridad: coordinar acciones con el CISO y las áreas de TI para

[5] https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

fortalecer la resiliencia digital institucional.

La independencia funcional y la autonomía técnica son pilares innegociables de su gestión, tal como señala el Grupo de Trabajo del Artículo 29 de la Unión Europea (WP 243 rev.01), principios que las entidades colombianas pueden adoptar para garantizar imparcialidad y transparencia.

***Desafíos y oportunidades en el contexto nacional***

En Colombia, el DPO enfrenta retos particulares asociados a la fragmentación institucional, la madurez desigual de los programas de privacidad y la falta de profesionalización certificada del rol. Sin embargo, estas limitaciones representan oportunidades para:

Estandarizar la función del DPO en entidades públicas y
Fortalecer la capacitación de profesionales en derecho digital, ciberseguridad y ética de datos.
Incorporar modelos de auditoría basados en ISO/IEC 27701:2025[6], norma que amplía el sistema de gestión ISO 27001 hacia la protección de datos personales.

En la práctica, el DPO se convierte en el eje articulador de la confianza digital, facilitando la convergencia entre protección de datos, seguridad de la información, responsabilidad corporativa y transformación digital sostenible.

## Conclusiones

La consolidación del Delegado de Protección de Datos (DPO) como figura estratégica en las instituciones colombianas representa un paso fundamental hacia una cultura de confianza y responsabilidad digital. Este doucmento pesenta que la privacidad no es un tema exclusivo de la ley o la tecnología, sino una dimensión ética y humana que atraviesa todos los procesos organizacionales.

La confianza digital se construye cuando las organizaciones reconocen el valor del dato como activo y asumen el deber de protegerlo como parte de su misión institucional. En este sentido, el DPO se convierte en el articulador entre el cumplimiento normativo, la seguridad de la información y la innovación tecnológica, promoviendo una relación transparente con los titulares y fomentando prácticas que respeten la dignidad humana.

[6] https://www.iso.org/standard/27701

Las experiencias internacionales muestran que el liderazgo del DPO no se limita a vigilar el cumplimiento, sino a inspirar una transformación cultural basada en la rendición de cuentas, la educación digital y la toma de decisiones éticas. Para Colombia, este camino implica fortalecer la profesionalización del rol, estandarizar su marco de acción y fomentar la colaboración entre sectores público, privado y académico.

Finalmente, el propósito esencial de esta figura y de este esfuerzo colectivo, es promover la confianza digital como un bien común. En la medida en que las instituciones integren la protección de datos en su estructura, sus proyectos y su cultura, estarán no solo cumpliendo con la norma, sino construyendo una sociedad más segura, transparente y consciente de su responsabilidad frente a la información.

## Recomendaciones finales

La protección de datos personales no debe limitarse a cumplir con una norma, sino convertirse en un compromiso institucional con la transparencia, la ética y la confianza digital. A partir de lo planteado, este documento proponen las siguientes acciones para fortalecer la gestión responsable de la información:

1. Designar un Delegado de Protección de Datos - DPO con autonomía técnica y formación interdisciplinaria en derecho, ciberseguridad y gobernanza digital, encargado de liderar la cultura de privacidad dentro de la organización.
2. Implementar políticas y procedimientos de protección de datos que incluyan evaluaciones de impacto - DPIA, principios de privacidad por diseño y por defecto y controles técnicos de seguridad acordes con la norma ISO/IEC 27701:2025.
3. Fomentar la formación continua del talento humano, sensibilizando a todos los niveles sobre el valor ético y estratégico de los datos personales.
4. Consolidar estructuras de gobernanza de datos mediante comités interdisciplinarios que integren las áreas de TI, jurídica, riesgos, seguridad y comunicación, asegurando decisiones coherentes y oportunas.

5. Promover la transparencia y la rendición de cuentas mediante reportes periódicos, auditorías internas y mecanismos de comunicación claros con los titulares de la información.

Adoptar estas prácticas no solo fortalece el cumplimiento normativo, sino que refuerza la credibilidad institucional y contribuye a construir un ecosistema digital más confiable, sostenible y centrado en las personas.

## Referentes

Ciclosi, F., & Massacci, F. (2023). The Data Protection Officer: A Ubiquitous Role That No One Really Knows. IEEE Security & Privacy, 21(1), 66-77. https://doi.org/10.1109/MSEC.2022.3222115

Del-Real, C., De Busser, E., & Van Den Berg, B. (2025). A systematic literature review of security and privacy by design principles, norms, and strategies for digital technologies. International Review of Law, Computers & Technology, 1-32. https://doi.org/10.1080/13600869.2025.2457227

European Network and Information Security Agency. (2014). Privacy and data protection by design: From policy to engineering. Publications Office. https://data.europa.eu/doi/10.2824/38623

Ježová, D. (2020). Principle of Privacy by Design and Privacy by Default. En M. Reljanović (Ed.), Regional Law Review (pp. 127-139). Institute of Comparative Law; University of Pécs Faculty of Law; Josip Juraj Strossmayer University of Osijek, Faculty of Law. https://doi.org/10.18485/iup_rlr.2020.ch10

OECD. (2022). Building Trust and Reinforcing Democracy: Preparing the Ground for Government Action. OECD. https://doi.org/10.1787/76972a4a-en

Perera, C., McCormick, C., Bandara, A. K., Price, B. A., & Nuseibeh, B. (2016). Privacy-by-Design Framework for Assessing Internet of Things Applications and Platforms. https://doi.org/10.48550/ARXIV.1609.04060

Šidlauskas, A. (2021). The Role and Significance of the Data Protection Officer in the Organization. Socialiniai tyrimai, 44(1), 8-28. https://doi.org/10.15388/Soctyr.44.1.1

UE. (2016). REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO. https://www.boe.es/doue/2016/119/L00001-00088.pdf

Zwitter, A., & Gstrein, O. J. (2020). Big data, privacy and COVID-19 – learning from humanitarian expertise in data protection. Journal of International Humanitarian Action, 5(1), 4, s41018-020-00072-00076.

**Contactenos**

📧 **Correo electrónico:** csirt@unad.edu.co

🌐 **Página web:** https://csirt.unad.edu.co

El CSIRT Académico UNAD está siempre disponible para apoyarte ante consultas o inquietudes relacionadas con la protección de la información en la universidad. No dudes en ponerte en contacto con nuestro equipo para recibir asesoría, reportar incidentes o recibir orientación en temas de seguridad digital. ¡Tu seguridad es nuestra prioridad!