

INFORME DE CONSULTORÍA

ANÁLISIS DE RIESGO COMUNICACIONAL DEL USO DEL TÉRMINO “HACKEAR”

Evaluación de una publicación institucional sobre diseño centrado en el usuario

RIESGO ALTO	16/25 en escenario base · puede escalar a crítico si es amplificado políticamente
-------------	---

FICHA DEL ENTREGABLE

FICHA TÉCNICA Y ALCANCE

Objeto	Identificar los riesgos políticos, reputacionales, institucionales y narrativos derivados del uso del término “hackear” en una publicación oficial.
Pieza analizada	Captura de una publicación de la cuenta @habitatbogota sobre diseño centrado en el usuario y HábilLAB.
Enfoque	Comunicación estratégica, prevención de crisis, lenguaje claro, confianza pública y diseño centrado en las personas.
Horizonte	Riesgo inmediato de amplificación y recomendaciones preventivas de corto y mediano plazo.
Metodología	Lectura semántica y contextual, análisis de actores adversos, matriz de probabilidad-impacto y formulación de mensajes alternativos.
Limitaciones	No se contó con métricas, comentarios, citas, hora de publicación, historial de edición ni monitoreo de conversación digital.
Naturaleza	Documento técnico de consultoría; no constituye concepto jurídico ni atribuye conductas ilegales a la entidad o a sus funcionarios.

PREMISA POLÍTICA UTILIZADA PARA EL ANÁLISIS

El solicitante indicó que la publicación se produce en un entorno de oposición o tensión frente al Gobierno Nacional. Este informe no verifica ni califica jurídicamente esa relación política. La utiliza únicamente como un escenario de exposición: en contextos polarizados, las frases institucionales tienen mayor probabilidad de ser recortadas, resignificadas y empleadas como insumo de controversia.

Conclusión central

El riesgo principal no está en que la palabra “hackear” demuestre una conducta ilícita. Está en que permite construir, con una captura real, una acusación políticamente eficaz: “una entidad pública afirma que hackea la mente de las personas”. Esa interpretación sería imprecisa, pero comunicacionalmente explotable.

1 · RESUMEN EJECUTIVO

EVALUACIÓN EJECUTIVA

La publicación presenta un riesgo comunicacional alto porque combina una metáfora de carga negativa — “hackeando la mente”— con una voz institucional, un asunto asociado a innovación digital y un contexto político susceptible de controversia. La frase puede separarse del contenido original y convertirse en un titular o pieza de ataque sin necesidad de alterar la captura.

DIAGNÓSTICO

Riesgo alto en escenario base: 4 de probabilidad × 4 de impacto = 16/25.

POSIBLE ESCALAMIENTO

Riesgo crítico si la captura es amplificada por un actor político o coincide con un incidente de ciberseguridad.

PROBLEMA NARRATIVO

La publicación habla de “hackear” en vez de escuchar, comprender, probar y mejorar con la ciudadanía.

DECISIÓN RECOMENDADA

Sustituir el texto por una versión centrada en beneficios ciudadanos y eliminar metáforas asociadas a intrusión o manipulación.

HALLAZGOS PRINCIPALES

- **La frase es fácilmente recortable.** “Estamos hackeando la mente” conserva una apariencia completa aun cuando se elimina la explicación posterior.
- **La defensa técnica llega tarde.** Aunque la intención sea hablar de innovación, la primera lectura puede activar asociaciones con intrusión, manipulación o ciberataque.
- **Existe contradicción conceptual.** El diseño centrado en el usuario se basa en comprender a las personas, sus tareas y sus contextos, e involucrarlas durante el diseño; no en intervenir o “hackear” su mente. [1]
- **El contexto institucional eleva el estándar.** La comunicación pública debe ser clara, comprensible y útil para que la ciudadanía encuentre, entienda y use la información. [2][3]
- **La tensión política multiplica el daño potencial.** Una cuenta adversa puede presentar la expresión como evidencia de manipulación estatal, aun cuando esa lectura no corresponda a la intención de la entidad.

- **El riesgo jurídico es indirecto, no automático.** El solo uso metafórico de la palabra no acredita un delito. Sin embargo, conductas comúnmente asociadas al “hackeo”, como el acceso no autorizado a sistemas, sí están tipificadas en Colombia; esa cercanía semántica aumenta el riesgo de confusión. [4]

DECISIÓN RECOMENDADA

Retirar o corregir el texto cuando la plataforma lo permita y republicar con lenguaje centrado en escucha, participación, simplificación y mejora de servicios. No emitir una aclaración pública autónoma si la publicación no ha sido ampliada: una respuesta innecesaria podría aumentar su visibilidad.

2 · EVIDENCIA

LECTURA DE LA PUBLICACIÓN ANALIZADA

La captura suministrada contiene la expresión: “Así estamos hackeando la mente del hábitat para dar mejores respuestas al diseño y la mejora de programas y procesos a partir de la innovación”. La vista previa enlazada también utiliza la denominación “Hacker Space de HábiLAB”.



Figura 1. Captura suministrada por el solicitante. No se verificó directamente en la plataforma.

DETONANTES DE RIESGO

“Hackeando”

Puede evocar acceso indebido, vulneración, manipulación o intervención no autorizada.

“La mente”

Traslada la metáfora desde procesos o sistemas hacia las personas y facilita una lectura de manipulación.

“Hacker Space”

Refuerza el campo semántico del hackeo y exige explicación para una audiencia general.

El error de enfoque

La pieza comunica primero el método y la jerga interna, y deja en segundo plano el valor ciudadano. El mensaje debería responder de inmediato qué mejora obtiene la persona: menos pasos, información más clara, procesos más simples o respuestas más oportunas.

Regla de oro: una frase institucional debe sobrevivir al recorte. Si las primeras palabras pueden convertirse en un ataque plausible, el copy debe reescribirse.

DIMENSIONES DEL RIESGO

3.1 Riesgo semántico y de confianza

En una cuenta pública, el lenguaje no se interpreta como el de una marca experimental. La expresión “hackear la mente” puede sugerir que la entidad pretende intervenir, manipular o condicionar a las personas. La confianza institucional se ve afectada cuando el ciudadano debe descifrar si una metáfora es inocente.

3.2 Riesgo político

En un ambiente polarizado, la captura permite una acusación simple, emocional y visualmente verificable: “la Secretaría reconoce que hackea mentes”. La respuesta institucional sería más larga y compleja que el ataque, lo que genera una desventaja narrativa.

3.3 Riesgo mediático

La frase reúne tres atributos de un titular adverso: es corta, sorprendente y atribuible a una cuenta oficial. Un medio o comentarista puede reproducirla sin alterar el contenido y desplazar la conversación desde innovación pública hacia manipulación o seguridad digital.

3.4 Riesgo digital

El ecosistema digital premia fragmentos y capturas. La pieza puede circular fuera del hilo original, sin el video ni el enlace explicativo. Además, el campo semántico del hackeo es sensible para las entidades públicas, que deben gestionar riesgos de seguridad digital y sostener la confianza de ciudadanos y partes interesadas. [5]

3.5 Riesgo institucional

La publicación puede proyectar falta de filtros editoriales o desconocimiento del efecto político del lenguaje. Esto afecta la percepción de profesionalismo del equipo de comunicaciones, incluso si el contenido técnico del laboratorio es sólido.

3.6 Riesgo conceptual

La ISO 9241-210 establece que el diseño centrado en las personas parte de comprender usuarios, tareas y entornos e involucra a los usuarios durante el diseño. La metáfora del hackeo desplaza el énfasis desde la participación hacia la intervención sobre la mente. [1]

3.7 Riesgo de lenguaje ciudadano

Las guías colombianas de lenguaje claro buscan que la comunicación estatal sea comprensible, accesible y útil, y que el ciudadano pueda encontrar, entender y usar la información. La acumulación de “hackear”, “Hacker Space”, “HábilLAB” y “diseño centrado en el usuario” aumenta la carga técnica y reduce la claridad. [2][3]

3.8 Riesgo jurídico reputacional

No existe base para afirmar que la publicación, por sí sola, configure una conducta penal. Sin embargo, la Ley 1273 de 2009 tipifica el acceso no autorizado a sistemas informáticos, una de las conductas socialmente asociadas al hackeo. El peligro es reputacional: que la audiencia confunda una metáfora con una confesión o práctica institucional. [4]

CÓMO PODRÍA SER REINTERPRETADA LA PUBLICACIÓN

Marco	Posible formulación adversa
Manipulación estatal	"La Secretaría admite que busca hackear la mente de los ciudadanos".
Uso indebido de datos	"¿Qué información personal utiliza la entidad para intervenir el comportamiento de los usuarios?".
Improvisación institucional	"La entidad habla como una startup y no como una autoridad pública responsable".
Contradicción ética	"Dicen que el diseño está centrado en el usuario, pero lo tratan como objeto de intervención".
Confrontación política	"Mientras cuestionan al Gobierno Nacional, reconocen prácticas de manipulación desde una cuenta oficial".
	Respuesta estratégica correcta Reconocer que la metáfora fue imprecisa, explicar el propósito real en una sola idea y llevar la conversación a escucha, participación y mejora de servicios.
	Respuesta que debe evitarse Defender públicamente el concepto de "hacking cívico", discutir semántica con críticos o publicar una explicación extensa cuando no existe ampliación verificable.

METODOLOGÍA DE VALORACIÓN

La valoración utiliza una escala cualitativa de 1 a 5. El puntaje se obtiene mediante la multiplicación: probabilidad × impacto. Los valores son una estimación profesional basada en la pieza analizada y el escenario político informado; no son métricas de desempeño observadas.

1–4	5–9	10–14	15–19	20–25
Bajo	Moderado	Significativo	Alto	Crítico

Cálculo del riesgo base: probabilidad alta (4/5) × impacto alto (4/5) = 16/25, clasificado como ALTO.

Riesgo	Detonante	P	I	Puntaje	Nivel	Razonamiento / mitigación
Recorte adverso	Captura aislada de “hackeando la mente”	4	5	20	Crítico	Es altamente replicable. Mitigar mediante sustitución inmediata del copy y monitoreo de citas.
Pérdida de confianza	Lectura de manipulación o intrusión	4	4	16	Alto	Afecta credibilidad y servicio. Reencuadrar en escucha, participación y beneficios.
Ataque político	Uso de la pieza por un actor adverso	4	5	20	Crítico	La acusación es breve y emocional. Preparar una respuesta de una sola idea y evitar debate prolongado.
Asociación con ciberseguridad	Coincidencia con noticia o incidente digital	3	5	15	Alto	El término puede adquirir gravedad adicional. Eliminar metáforas de intrusión en contenidos institucionales.
Incoherencia con DCU	El método se explica como intervención sobre la mente	4	3	12	Significativo	Debilita la pedagogía del programa. Explicar observar, comprender, cocrear, probar y mejorar.
Cuestionamiento editorial	Percepción de ausencia de filtros	3	4	12	Significativo	Implementar lista de verificación y revisión de riesgo antes de publicar.
Confusión jurídica	Interpretación como confesión de conducta ilegal	2	4	8	Moderado	No hay evidencia de delito. Evitar entrar en debate jurídico salvo pregunta directa y documentada.
Efecto Streisand	Aclaración pública sin controversia previa	3	4	12	Significativo	No amplificar. Corregir silenciosamente y responder solo si existe tracción verificable.
Lectura de la matriz El mayor peligro no es una sanción jurídica inmediata, sino la combinación de alta facilidad de recorte y alto impacto reputacional. Dos riesgos alcanzan 20/25: el recorte adverso y el uso político de la captura.						

ESCALAMIENTO POSIBLE DE LA CONVERSACIÓN

moderado.

Escenario 1 · Contenido sin ampliación

La publicación obtiene interacción limitada y no es cuestionada.

Respuesta recomendada: Corregir o sustituir el copy, documentar el aprendizaje y no emitir explicación pública.

alto.

Escenario 2 · Captura por cuenta crítica

Un actor político o ciudadano recorta la frase "hackeando la mente" y la presenta como manipulación.

Respuesta recomendada: Responder una sola vez con claridad, corregir el mensaje original y dirigir la conversación hacia escucha ciudadana y mejora de servicios.

alto a crítico.

Escenario 3 · Amplificación mediática

Un periodista consulta o publica la captura.

Respuesta recomendada: Entregar contexto verificable, reconocer que la metáfora fue inadecuada y explicar el propósito real sin discutir con el medio.

crítico.

Escenario 4 · Coincidencia con incidente de ciberseguridad

La expresión circula cuando existe una noticia sobre filtración, ataque o datos personales.

Respuesta recomendada: Separar inmediatamente ambos asuntos, activar vocería técnica de seguridad digital y retirar cualquier lenguaje ambiguo.

significativo.

Escenario 5 · Defensa institucional extensa

La entidad publica un hilo justificando el concepto de "hacking cívico" sin que exista controversia significativa.

Respuesta recomendada: Evitar sobre-reacción. La explicación larga puede legitimar y ampliar una crítica que aún no existe.

RECOMENDACIONES OPERATIVAS

Acciones inmediatas · 0 a 4 horas

1. Guardar captura, enlace, fecha, hora y métricas disponibles para trazabilidad interna.
2. Revisar respuestas, menciones y publicaciones citadas antes de decidir si se requiere una intervención pública.
3. Editar, retirar o reemplazar el texto, según las funciones de la plataforma, sin alterar ni ocultar evidencia interna.
4. Republicar con un copy centrado en el beneficio ciudadano.
5. No publicar disculpa o aclaración autónoma si no existe ampliación verificable.

Acciones en 24 a 72 horas

1. Revisar las demás piezas de HábilLAB para identificar expresiones como “hackear”, “Hacker Space” o metáforas de intervención sobre personas.
2. Definir una línea de mensajes: escuchar, comprender, cocrear, probar, simplificar y mejorar.
3. Incorporar un filtro de riesgo político y reputacional en la aprobación de copys institucionales.
4. Preparar respuestas breves para prensa, redes y vocería directiva solo en caso de consulta.

Medidas estructurales

1. Crear un glosario de términos recomendados y términos de alto riesgo para las cuentas oficiales.
2. Adoptar una lista de chequeo de “recorte adverso”: leer el primer enunciado como si circulara solo.
3. Capacitar al equipo en lenguaje claro y traducción de conceptos técnicos a beneficios ciudadanos. [2][3]
4. Establecer doble revisión para publicaciones relacionadas con datos, tecnología, seguridad digital, población vulnerable o coyuntura política.
5. Medir comprensión del mensaje, no solo alcance e interacción.

Lista de verificación antes de publicar

- ☐ ¿El ciudadano entiende el beneficio en la primera lectura?
- ☐ ¿La frase puede ser recortada y utilizada en contra de la entidad?
- ☐ ¿Hay palabras asociadas a delitos, violencia, manipulación, vigilancia o intrusión?
- ☐ ¿El texto explica una sigla o concepto interno?
- ☐ ¿El sujeto del mensaje es la ciudadanía o la entidad hablando de sí misma?
- ☐ ¿La publicación expresa escucha y participación cuando afirma estar centrada en el usuario?
- ☐ ¿Existe una versión más simple sin perder precisión?

TRINOS CENTRADOS EN EL USUARIO

Las siguientes versiones priorizan la escucha, la utilidad y los resultados para la ciudadanía. Se evita cualquier metáfora asociada con intrusión, manipulación o ataque informático.

Versión principal · 242 caracteres antes del enlace

En Hábitat, innovar empieza por escuchar. Desde HábilLAB aplicamos diseño centrado en el usuario para comprender necesidades, simplificar procesos y crear servicios más claros y útiles. Dale play y conoce cómo trabajamos con la ciudadanía. □

Versión enfocada en el beneficio

¿Cómo hacemos más simples los servicios de Hábitat? Escuchando a quienes los usan. En HábilLAB identificamos barreras, probamos soluciones y mejoramos procesos con diseño centrado en el usuario. Conoce el ejercicio. □

Versión corta y pedagógica

Innovar no es hablar más difícil: es escuchar mejor. En HábilLAB usamos diseño centrado en el usuario para construir procesos más claros, simples y útiles para la ciudadanía. Dale play. □

Racional de la propuesta

- **Empieza por la ciudadanía.** La primera idea es escuchar, no mostrar la sofisticación del laboratorio.
- **Traduce el método en acciones.** Comprender necesidades, identificar barreras, probar soluciones y mejorar procesos son verbos verificables.
- **Promete beneficios concretos.** Claridad, simplicidad y utilidad permiten que el público entienda para qué sirve el diseño centrado en el usuario.
- **Reduce el riesgo político.** Ninguna frase aislada sugiere manipulación, acceso indebido o intervención sobre la mente.
- **Mantiene la identidad de HábilLAB.** El laboratorio continúa siendo protagonista, pero como herramienta al servicio de las personas.

RESPUESTA SUGERIDA SI EXISTE CUESTIONAMIENTO PÚBLICO

Mensaje base

La expresión se utilizó como una metáfora de innovación, pero reconocemos que no fue la más precisa para una cuenta institucional. HábilLAB no interviene ni manipula a las personas: escucha a la ciudadanía, identifica barreras y prueba soluciones para mejorar servicios y procesos. Por eso ajustamos el mensaje.

Preguntas y respuestas

¿La Secretaría está “hackeando” a los ciudadanos?

No. La palabra fue utilizada de forma metafórica. El trabajo de HábilLAB consiste en comprender necesidades, involucrar usuarios y probar mejoras para que los servicios sean más claros y útiles.

¿La entidad está usando datos personales para manipular comportamientos?

La captura analizada no demuestra esa conducta. Ante una pregunta formal, la respuesta debe limitarse a prácticas verificables de tratamiento de datos y remitir a la política institucional correspondiente.

¿Por qué borraron o cambiaron la publicación?

Porque el lenguaje de una cuenta pública debe ser preciso y comprensible. Se ajustó el texto para explicar mejor el propósito del laboratorio y evitar interpretaciones equivocadas.

¿Esto tiene relación con un ataque informático?

No existe evidencia en la pieza analizada que permita relacionarla con un incidente de seguridad digital. La publicación se refería a una metodología de innovación y mejora de servicios.

Criterio de uso

Esta respuesta no debe publicarse preventivamente. Se utiliza únicamente si existe una pregunta, una captura ampliada o una consulta periodística verificable. La corrección silenciosa es preferible cuando no hay conversación pública.

CONCLUSIÓN DE CONSULTORÍA

El término “hackear” puede funcionar en entornos de innovación cerrados o en comunidades técnicas que comparten su significado metafórico. En una cuenta institucional, y especialmente en un contexto de tensión política, su uso junto a la expresión “la mente” crea una vulnerabilidad narrativa innecesaria. La captura puede ser utilizada para insinuar manipulación, uso indebido de datos o improvisación institucional, aunque ninguna de esas conductas pueda probarse a partir de la publicación.

La recomendación es retirar la metáfora y reconstruir el mensaje desde los principios reales del diseño centrado en el usuario: comprensión del contexto, participación de las personas, prueba de soluciones y mejora continua. [1] La comunicación debe mostrar el beneficio ciudadano con lenguaje claro, accesible y accionable. [2][3]

La decisión más segura es simple: corregir sin sobrereaccionar, monitorear antes de responder y establecer filtros editoriales que impidan que una frase creativa se convierta en un riesgo político evitable.

Recomendación final

No defender la palabra “hackear”. Defender el propósito de HábilLAB: escuchar, comprender y mejorar los servicios con la ciudadanía.

FUENTES CONSULTADAS

REFERENCIAS NORMATIVAS Y TÉCNICAS

- [1] International Organization for Standardization (ISO). ISO 9241-210:2019. Ergonomics of human-system interaction — Part 210: Human-centred design for interactive systems. 2019. [Consultar fuente](#)
- [2] Departamento Nacional de Planeación (DNP). Guía de Lenguaje Claro para Servidores Públicos de Colombia. consulta vigente a 2026. [Consultar fuente](#)
- [3] Departamento Administrativo de la Función Pública. Técnica No. 1: Lenguaje claro. consulta vigente a 2026. [Consultar fuente](#)
- [4] Congreso de Colombia / Gestor Normativo de Función Pública. Ley 1273 de 2009, artículo 269A: acceso abusivo a un sistema informático. 2009. [Consultar fuente](#)
- [5] Ministerio de Tecnologías de la Información y las Comunicaciones. Modelo de Gestión de Riesgos de Seguridad Digital (MGRSD). consulta vigente a 2026. [Consultar fuente](#)

Declaración de precisión: las calificaciones de riesgo son juicios profesionales fundamentados en la evidencia disponible. No sustituyen monitoreo de redes, análisis jurídico ni verificación directa de la publicación y sus métricas.