

 BOGOTÁ	Protocolo de Gestión de Incidentes de la Información para el Distrito Capital	Versión: 1.0 Fecha: 20/05/2023
--	--	-----------------------------------

1. INTRODUCCIÓN

La Oficina de Alta Consejería Distrital de TIC – ACDTIC, a través del presente documento establece la importancia de realizar de manera eficiente la gestión y atención de los incidentes de seguridad de la información que se presenten al interior de las entidades distritales, permitiendo de esta manera que las afectaciones y los impactos generados por su materialización causen el menor daño posible en los servicios prestados por la entidad afectada.

En este sentido, en el presente documento se define el Protocolo de Gestión de Incidentes de seguridad de la información para el Distrito Capital, el cual deberá ser aplicado por todas y cada una de las entidades distritales, permitiendo centralizar y canalizar las respectivas acciones de remediación y/o la gestión realizada por las entidades para la mitigación de los impactos que este genera junto con la recuperación del funcionamiento normal de su misionalidad de conformidad con la Resolución 500 de 2021 del Ministerio de Tecnologías de la Información y las Comunicaciones.

Finalmente, en el presente protocolo se explican las actividades mínimas necesarias que deben ser realizadas por las entidades distritales durante la gestión y atención de incidentes de seguridad que se materialicen al interior de las entidades, logrando la cooperación y coordinación con las instancias superiores

2. OBJETIVO

Establecer un marco estructurado y eficiente que facilite la identificación, contención, mitigación y recuperación de los incidentes de seguridad digital que se materialicen al interior de las entidades distritales, junto con el aprendizaje de lo sucedido, logrando la adecuación de las medidas y/ controles necesarios que eviten que se presente nuevamente una situación similar.

3. ALCANCE

El protocolo desarrolla en cuatro fases: Preparación, Detección y análisis, Contención, erradicación y recuperación, y Post-Incidente. Estas fases definen las etapas clave en la respuesta a un incidente, desde la identificación y clasificación de un evento de seguridad hasta la comunicación y el aprendizaje después de la resolución del incidente.

4. PUBLICO OBJETIVO

Aplica para todas las entidades distritales, que se han visto afectadas por incidentes de seguridad de la información, tanto de alto como de bajo impacto, permitiéndoles atender y reportar de manera eficiente las situaciones a nivel de seguridad que afecten el normal desarrollo de la misionalidad de la entidad en cualquiera de sus principios, confidencialidad, integridad y disponibilidad.

 	Protocolo de Gestión de Incidentes de la Información para el Distrito Capital	Versión: 1.0 Fecha: 20/05/2023
---	--	-----------------------------------

5. ENTRADAS

- Políticas y protocolos de seguridad digital definidos en la Resolución 500 de 2021 y el Decreto 338 de 2022.
- Reportes o alertas de posibles incidentes de seguridad digital.
- Información relacionada con el incidente de seguridad digital (datos de usuario, registros de eventos, logs de sistemas, etc.)
- Tecnología de seguridad digital implementada para la detección, análisis, contención, erradicación, recuperación y gestión de incidentes.
- Acciones y decisiones realizadas durante el manejo de incidentes de seguridad digital.
- Información sobre los sistemas afectados y el alcance del incidente.
- Evidencias digitales recolectadas durante el incidente.
- Información de los titulares de los datos afectados por el incidente.

6. SALIDAS

- Estrategias y acciones de preparación para la anticipación y gestión eficaz ante un incidente de seguridad digital.
- Reportes de detección y análisis de incidentes de seguridad digital.
- Notificaciones al CSIRT DC (Alta Consejería Distrital de TIC) y a ColCERT acerca de los incidentes de seguridad.
- Medidas de contención, erradicación y recuperación aplicadas tras un incidente.
- Restauración de los sistemas y servicios afectados.
- Registro de evidencias recolectadas y acciones realizadas durante el manejo del incidente.
- Reportes de incidentes y acciones realizadas al CSIRT DC (Alta Consejería Distrital de TIC), a ColCERT y a la Fiscalía General de la Nación (cuando aplique).
- Notificaciones a la Superintendencia de Industria y Comercio (si aplica) y a los titulares de los datos (si aplica).
- Sesiones de trabajo post-incidente y lecciones aprendidas para mejorar las medidas de seguridad.
- Documentación de las acciones realizadas en la atención del incidente en cada una de sus fases.

7. PROTOCOLO Y ACTIVIDADES

El protocolo de atención de incidentes de seguridad digital se compone de cuatro fases: Preparación, Detección y Análisis, Contención, Erradicación y Recuperación, y Post-Incidente.

7.1. FASE: PREPARACIÓN

Esta fase tiene como finalidad el realizar actividades que permitan desarrollar la estrategia para anticipación y gestión eficaz ante la materialización de un incidente de seguridad digital, al interior de las entidades distritales, a través de la adopción de tres pilares fundamentales como lo son, personas,

protocolos y tecnologías, permitiendo de esta manera, mitigar riesgos relacionados con la protección y la privacidad de la información.

En este sentido, dichas actividades están contempladas dentro de lo definido en la Resolución 500 de 2021, “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital”, articulado con lo dispuesto en el Decreto 338 de 2022, en donde se [...] “Establecen los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital” [...] emitidas por el Gobierno Nacional, las cuales son de estricto cumplimiento para todos los sujetos obligados definidos en el artículo 2.2.9.1.1.2. del Decreto 1078 de 2015 (DUR-TIC), “Por medio del cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones”.

7.2. FASE: DETECCIÓN Y ANÁLISIS

Esta fase tiene como finalidad el identificar y reportar ante las instancias superiores (CSIRT DC), los incidentes de seguridad que se presenten al interior de cada una de las entidades distritales tanto de impacto alto como bajo, en donde entre otras cosas se debe tener en cuenta los vectores de ataque por los cuales se materializó el incidente junto con la priorización definida por la entidad para la atención del incidente teniendo referente al impacto que este genera tanto a nivel interno como externo, teniendo en cuenta entre otros, el comportamiento evidenciado del incidente para posteriormente según su criticidad reportar al CSIRT DC en los tiempos estipulados a través del formato definido para tal fin.

No.	Nombre	Descripción	Responsable	Informado	Consultado
1.	Identificar un evento	Identificar un evento de seguridad digital	Cualquier persona		
2.	Reportar el evento	Reportar el evento al punto interno de contacto de la entidad	Cualquier persona	Entidad que sufre el incidente	
3.	Evaluar el evento	Evaluar el evento e identificar si es un incidente	Entidad que sufre el incidente		CSIRT DC
4.	Analizar el incidente	Analizar el incidente	Entidad que sufre el incidente		CSIRT DC
5.	Documentar el incidente	Documentar el incidente utilizando el formato establecido ¹	Entidad que sufre el incidente		

¹ [Formato Reporte de Incidentes - CSIRT Gobierno \(Versión 3\)](#)

6.	Determinar la gravedad	Determinar la gravedad del incidente de acuerdo con la metodología establecida	Entidad que sufre el incidente		CSIRT DC
7.	Notificar al CSIRT DC	Notificar el incidente al CSIRT DC (si aplica)	Entidad que sufre el incidente	CSIRT DC	
8.	Notificar a ColCERT	Notificar el incidente a ColCERT	CSIRT DC o Entidad que sufre el incidente	ColCERT	

7.3. FASE: CONTENCIÓN, ERRADICACIÓN Y RECUPERACIÓN.

Esta fase tiene como finalidad limitar el impacto que puede generar la materialización del incidente en las entidades distritales, a través de la adecuada toma de decisiones en donde se deberán aplicar las estrategias de contención que sean necesarias para mitigar los daños que este puede causar junto con la recolección y debida conservación de la evidencia digital a la que haya lugar. Asimismo, durante esta fase se trabajará en articulación con el **CSIRT DC** y otros expertos en seguridad, según sea necesario, para garantizar una respuesta eficiente y efectiva al incidente.

En este sentido, posterior a la identificación del alcance y dispositivos afectados por el incidente de seguridad, se debe realizar la erradicación de la amenaza que materializó el incidente en todos y cada uno de los dispositivos afectados, como lo son entre otros la eliminación del programa maligno identificado, eliminación de usuarios maliciosos y aplicación de parches de seguridad.

En consecuencia, una vez comprobado que dicha acción se realizó de manera satisfactoria, se procederá a realizar la recuperación de los sistemas afectados, a través de la restauración de las copias de seguridad junto con las acciones básicas de configuración, como cambio de credenciales de administración y el monitoreo continuo del funcionamiento de los sistemas restaurados entre otros, asegurando la eliminación en su totalidad de la amenaza que materializó el incidente de seguridad.

No.	Nombre	Descripción	Responsable	Informado	Consultado
9.	Contener, erradicar y recuperar	Contener, erradicar y recuperar el incidente	Entidad que sufre el incidente		CSIRT DC
10	Contener el incidente	Realizar actividades para contener el incidente	Entidad que sufre el incidente		CSIRT DC
11	Recopilar evidencias	Realizar actividades para recopilar evidencias	Entidad que sufre el incidente		CSIRT DC

12	Erradicar	Realizar actividades para erradicar	Entidad que sufre el incidente		CSIRT DC
13	Restablecer servicios	Realizar actividades para restablecer los servicios	Entidad que sufre el incidente		CSIRT DC

7.4. FASE: POST-INCIDENTE

Esta fase tiene como finalidad el aprender y mejorar las medidas de seguridad a través de los sucesos adversos materializados en las entidades distritales, permitiendo de esta manera evolucionar por medio de la toma de conciencia y apropiación de conocimiento de las nuevas amenazas tecnológicas y lecciones aprendidas.

En consecuencia, es necesario realizar sesiones de lecciones aprendidas con las parte involucradas y afectadas por el incidente de seguridad, logrando de esta manera determinar de manera explícita las situaciones que conllevaron a la materialización del incidente de seguridad, en donde entre otros se detallarán aspectos sobre los cambios en las tendencias evidenciado en el incidente junto con la determinación de qué tan efectiva fue la respuesta y atención realizada sobre el incidente de seguridad, permitiendo la identificación de falencias y/o mejoras que deban realizarse en su respectiva gestión.

Asimismo, incluye entre otras acciones el notificar a las autoridades pertinentes y a los titulares de los datos personales (cuando corresponda), documentar las acciones realizadas en la atención del incidente en cada una de sus fases, reportar el incidente junto con sus respectivas acciones a los organismos de coordinación de seguridad (**CSIRT DC y ColCERT**), denunciar el incidente a la Fiscalía General de la Nación (cuando aplique) sumado a la realización de sesiones de trabajo post incidente con el **CSIRT DC**.

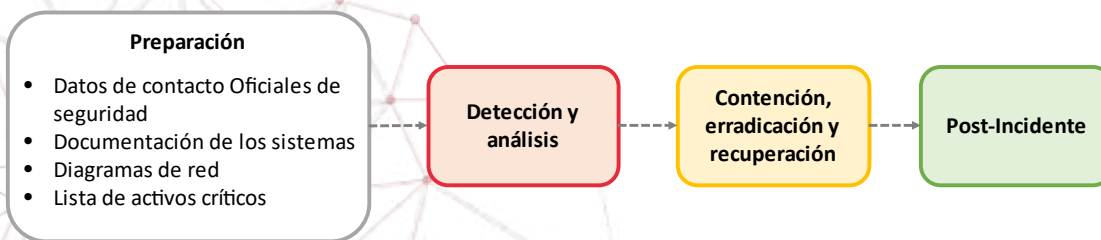
No.	Nombre	Descripción	Responsable	Informado	Consultado
14	Notificar a la SIC	Notificar incidente a la Superintendencia de Industria y Comercio (si aplica)	Entidad que sufre el incidente	CSIRT DC	
15	Informar a los titulares de datos	Informar incidente a los titulares de los datos (si aplica)	Entidad que sufre el incidente	CSIRT DC	
16	Documentar acciones	Documentar acciones realizadas utilizando el formato establecido	Entidad que sufre el incidente		
17	Reportar al CSIRT DC	Reportar al CSIRT DC el incidente y acciones realizadas	Entidad que sufre el incidente	CSIRT DC	

18	Reportar al ColCERT	Reportar al ColCERT el incidente y acciones realizadas	CSIRT DC o Entidad que sufre el incidente	ColCERT	
19	Denuncia a la Fiscalía	Realizar denuncia a la Fiscalía General de la Nación cuando aplique	Entidad que sufre el incidente	CSIRT DC Fiscalía General de la Nación	
20	Mesa de trabajo post incidente	Realizar mesa de trabajo post incidente con CSIRT DC	Entidad que sufre el incidente	ColCERT, CSIRT DC	

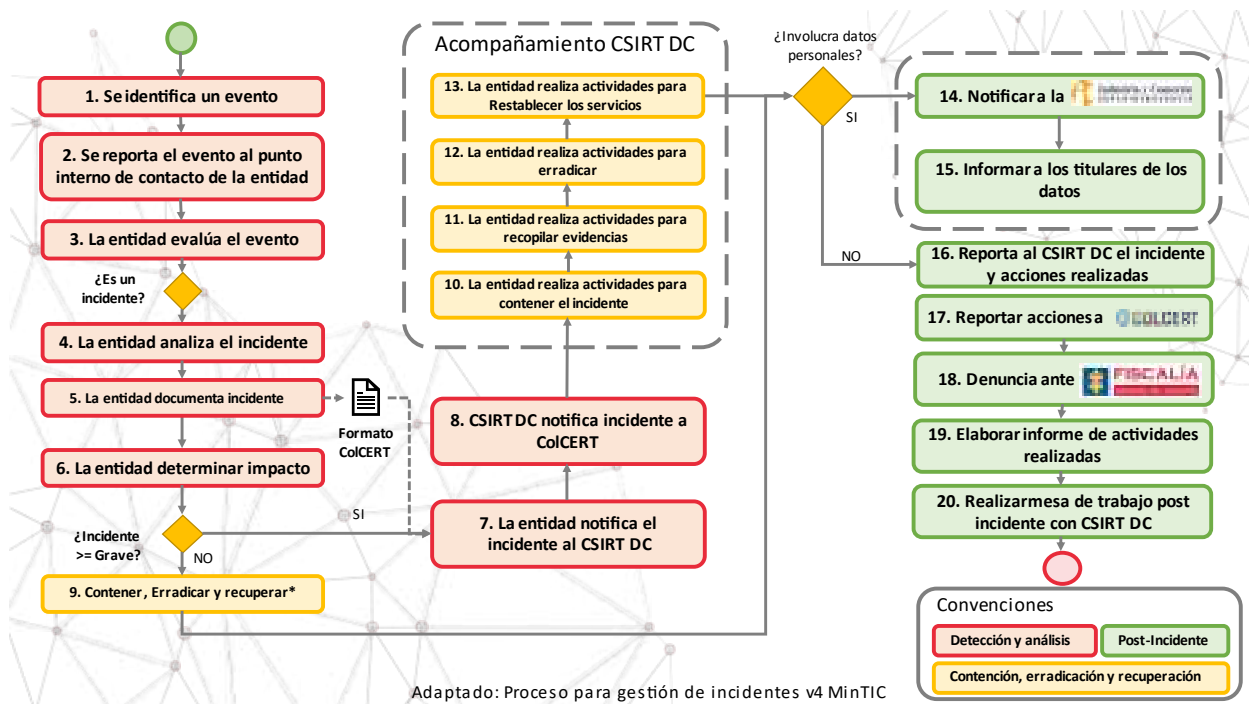
7.5. FLUJO

Protocolo de atención a incidentes de seguridad digital

Objetivo: Establecer un marco de referencia claro y eficiente para la gestión de incidentes de seguridad digital en todas las entidades del Distrito Capital.



Fuente: NIST SP 800-61 Rev2 - Computer Security Incident Handling Guide



8. GLOSARIO

Responsable: Es la persona o grupo que tiene la responsabilidad principal de llevar a cabo una tarea o actividad. Son aquellos encargados de ejecutar las acciones necesarias para lograr los objetivos.

Informado: Son las personas o grupos que deben ser notificados o informados sobre el progreso, las decisiones o los resultados de una tarea o actividad. No participan activamente en la ejecución o toma de decisiones, pero deben mantenerse al tanto de lo que está sucediendo.

Consultado: Son las personas o grupos cuya opinión se busca y se tiene en cuenta antes de tomar decisiones o llevar a cabo una acción. Se les consulta debido a su experiencia o conocimiento especializado, y su aporte es valioso en el proceso de toma de decisiones.

Accountable: Es el individuo o función que tiene la responsabilidad final de asegurar que una tarea se complete correctamente. A menudo, esta persona toma decisiones y es responsable de los resultados. Para el presente protocolo el rol de Accountable corresponde a los delegados por los representantes legales en cada una de las entidades distritales para atender los incidentes que se presenten.

9. BIBLIOGRAFÍA

Computer Security Incident Handling Guide - NIST Special Publication 800-61 Revision 2. (agosto de 2012). Obtenido de Computer Security Resource Center (CSRC) - National Institute of Standards and Technology: <https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final>

	Protocolo de Gestión de Incidentes de la Información para el Distrito Capital	Versión: 1.0 Fecha: 20/05/2023
---	--	-----------------------------------

Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC. (10 de marzo de 2021). *Resolución 500 de 2021*. Obtenido de Diario Oficial No. 51.619: <https://www.suin-juriscol.gov.co/viewDocument.asp?id=30044822>

Ministerio de Tecnologías de la Información y las Comunicaciones. (28 de octubre de 2021). *Guía para la Gestión y Clasificación de Incidentes de Seguridad versión 4*. Obtenido de Modelo de Seguridad y Privacidad de la Información - MSPI: https://gobiernodigital.mintic.gov.co/692/articulos-272951_recurso_1.zip

10. VERSIONES

Versión	Fecha	Elaboró	Revisó	Aprobó
1.0	20/06/2023	Luis Enrique Paris Nicolás Sánchez Barrera	Ivan Durán Pabón Juan Carlos Parada Gallardo	Comisión Distrital de Transformación Digital (20/6/2023)



MAKERS DE SOLUCIONES

MAKERS DE SOLUCIONES
PIONEROS EN
EL HACER *

BY  iBO

Muchas preguntas sin respuesta

Agosto 2022



La respuesta estaba
en los datos

¿Dónde están
los datos?

¿De quiénes
son los datos?

¿Cuántas usan
los servicios ?



¿Qué pasaría si resolvemos
retos de ciudad enamorados
de las primeras ideas?

La solución |

Pistola de cédulas



Superando las barreras de lo obvio

Solución que no es...pero que en el escritorio tenía mucho sentido



Diseño con propósito



Gran inversión tech



Capacitar a los prestadores



Conseguir internet



Base de datos



Utilizar las **cédulas** para capturar la información.

Solución que no es... pero que desde el escritorio tenía mucho sentido



¿cédulas?



“Uno tiene que cuidar mucho su cédula porque a una vecina le sacaron un plan de celular sin ella saber...con la cédula”



¿Qué pasaría si superamos
las barreras de lo obvio y
diseñamos centrado en las
personas?

PROTOTIPO 1

Registro COMUNIDAD DEL SISTEMA DEL CUIDADO DE BOGOTÁ



Creamos basados en insights y no en opiniones

Descubrimos que la respuesta no estaba en la tecnología sino en las CUIDADORAS

INFORMACIÓN 100% COMPLETA en tiempo real

Prototipo de ENROLAMIENTO

Personas registradas

en total

689

Solo **29** personas
iniciaron la
conversación y
desistieron.

de las cuales
fueron

557

Registros
largos

32

Registros
express



611

Mujeres

57

Hombres



20%

31%

49%



556

Carnets
generados

Día lanzamiento

133

Post - lanzamiento

45 variables por
persona

Calificación de experiencia

★★★★★ 86%
★★★★☆ 13%
★★★☆☆ 0.22%
★★☆☆☆ 0.22%

Total de
calificaciones
463

"Es muy
fácil"



"¿Mi mamá lo
puede hacer
desde su casa?"

Reconocer el cuidado y a las CUIDADORAS = CONFIANZA + PERTENENCIA



Diseño con propósito

CALIDAD DE DATOS



Diseño de nuevos y mejores SERVICIOS BASADOS en datos



PROTOTIPO 2

Registro ASISTENCIA a los servicios



Una vez tenemos los datos ¿cómo podemos hacer seguimiento, tomar decisiones y entender el uso de estos lugares ?

¿Quién viene y cada cuánto? ¿A qué viene? Usuarías recurrentes

Tecnología para la LECTURA MASIVA de códigos QR



Datos en DOBLE VÍA

las mujeres dan y reciben información

Hola, Sandra. Sé que eres integrante de la comunidad. ¿Quisieras conocer más sobre labores de cuidado? 🙋

11:00 AM

Hola, Sandra. Vi que ya completaste el curso de 6 clases de informática, ¡felicitaciones por ese logro! 🎉

2:15 PM

Sé que un atributo que te caracteriza es Activa. ¿Sabías que en tu Manzana existe un a Escuela de la Bici? ¡Ánimate a ir! 🚲

5:20 PM

¡Hola, Sandra! Has asistido a 5 clases de yoga este mes, ¡Sigue así! 🙏

10:25 AM

Entregar información a las cuidadoras sobre su progreso en las clases

Hacerles recordatorios de la clase

Compartirles la oferta de clases actualizada

El ingrediente secreto de la innovación son las personas |



FEST iBO.

La



que estamos construyendo


Chatico

El agente virtual de
Bogotá, que nunca te
dejará en visto

Orquestación de Servicios
del Distrito

+57 316 0231524





Chatico es el primer agente virtual de Bogotá que, soportando en inteligencia artificial y procesamiento de lenguaje natural, brinda atención 7/24 sobre trámites, servicios y, en general, información estratégica de la ciudad.

Usa **WhatsApp** como uno de sus canales estratégicos de salida para garantizar mayor alcance ciudadano.

Su nombre hace honor a una tradicional palabra bogotana

Canal estratégico para **promover la participación** ciudadana por canales digitales

CHATICO, NUESTRO ORQUESTADOR DE SERVICIOS, ES UN PROYECTO DONDE TODOS PONEMOS, NO ES DE UNA ENTIDAD, ES DEL DISTRITO PARA LOS CIUDADANOS



¿Qué hacemos hoy a través de nuestro Chatico?



- **Trámites, servicios e información** que se actualizan semanalmente
- **Información sobre oferta para personas** con discapacidad en la ciudad
- Atención en **Lengua Colombiana de Señas** (Línea 195)
- Atención de **agentes humanos** para usuarios que no encontraron en Chatico lo que buscaban (Línea 195)
- Estamos en un trabajo **con IBO, nuestro laboratorio de innovación** para mejorar experiencia de usuario
- Posibilidad de integrar, a través de nuestro aliado tecnológico, procesos para tener **trámites & servicios de punta a punta** que ya estén implementados por las entidades

Aliado tecnológico para potenciar procesos



CULTURA
INTELIGENTE *eTb*



Telcos



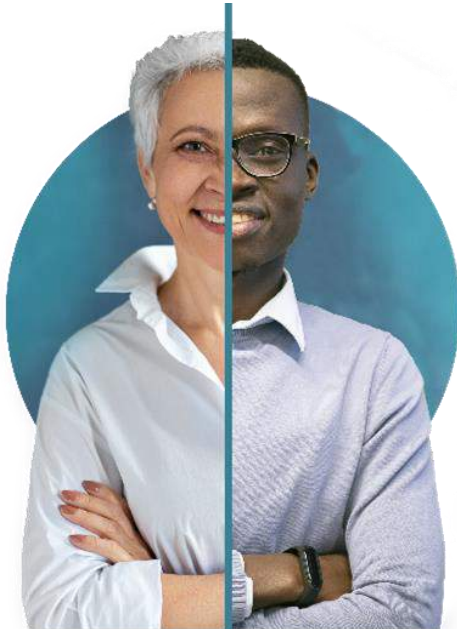
Ciudad



Transporte Público



Retail



Aseguradoras



Colegios



Banca

OMNICALIDAD. COMUNICACIÓN DINÁMICA

INTELIGENCIA ARTIFICIAL. ENTENDER EL LENGUAJE.

FLUJOS CONVERSACIONALES. MÁQUINA DE ESTADOS DEL DIÁLOGO

INTEROPERABILIDAD. CONEXIÓN CON SISTEMAS DE INFORMACIÓN

SEGURIDAD EN TRÁMITES .

POSIBILIDAD DE INTEGRAR CHATS ABIERTOS (GPT)



Chatico es orquestador de diálogos ciudadanos en los ecosistemas digitales para crear una verdadera comunidad digital

CHATICO IDENTIFICACIÓN DE PRÓXIMOS PASOS -2023

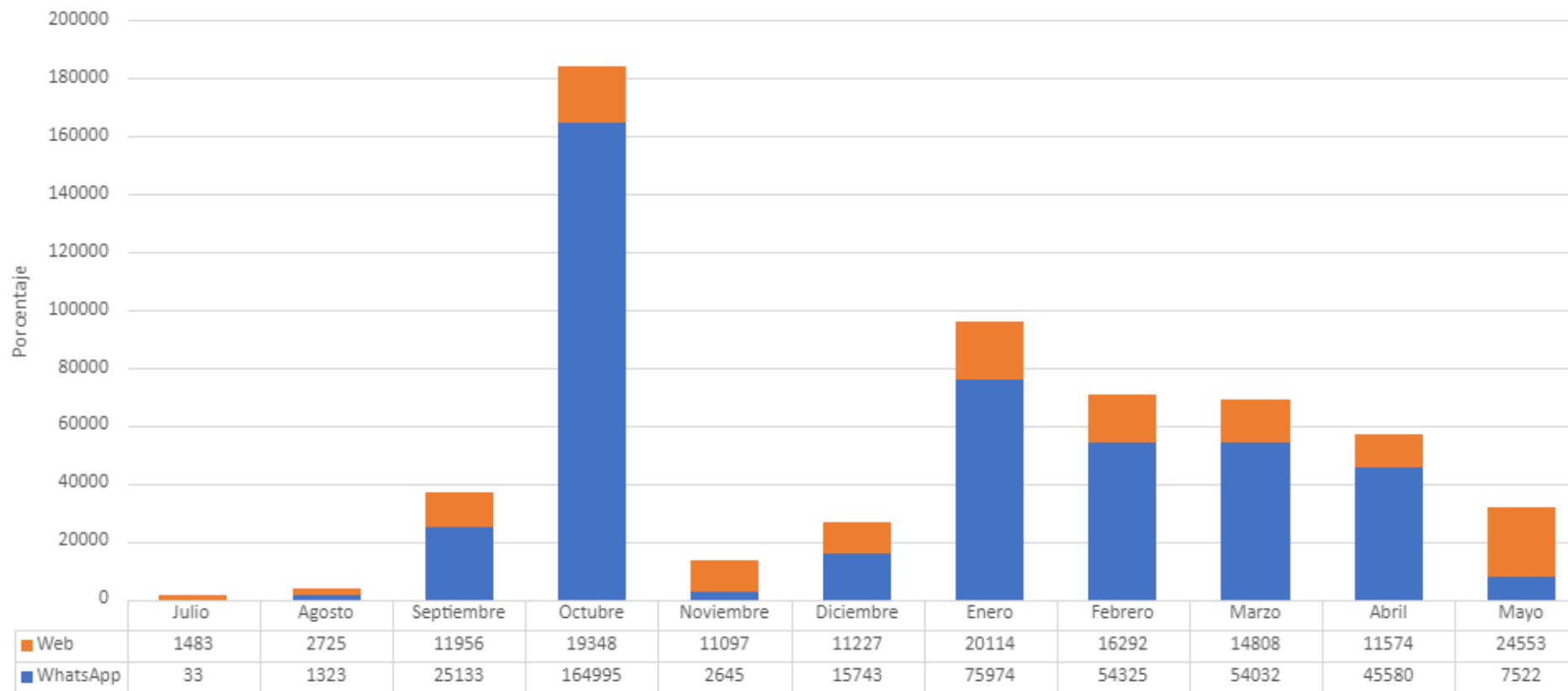


FLUJO	TRANSACCIONAL	INFORMATIVO
DESCRIPCIÓN	<p>Son los que más tracción le pueden dar a la herramienta. Trámites de punta a punta por WhatsApp es un hito en la transformación digital de la ciudad.</p> <p>En esta también se incluyen reportes (Ej. hueco, zona de parqueo) que van directo a la entidad que los gestiona; consulta sobre bases de datos como discapacidad y servicios a Mapas IDECA de lo que pasa en la ciudad (ejemplo: eventos)</p>	<p>La informativa responde a lo que el ciudadano navega y/o pregunta libremente. Para cargar los temas en este ítem nos basamos en:</p> <ol style="list-style-type: none"> 1. Cifras de tráfico de Chatico – Revisión semanal 2. Atenciones de línea 195 – Revisión semanal 3. Atenciones de agente humano por chat chatico – Revisión semanal 4. Preguntas abiertas de usuarios que escriben que no encuentran algo que necesitan
DESAFÍOS	<ol style="list-style-type: none"> 1. Citas médicas 2. Zona de Parqueo Pago 3. Pago de impuestos de punta a punta 4. Presupuestos participativos 2023 5. IDECA. Identificar experiencias a través de los mapas 	<ul style="list-style-type: none"> • Metro de Bogotá • Desarrollo económico • Información Parceros • Secretaría de Seguridad. • Inspección, vigilancia y control • Transmilenio • Invest Bogotá – Somos el destino para invertir

CHATICO – NUESTRAS CIFRAS



Canal de conversación



Chatico tiene un total de **592.482** conversaciones entre julio de 2022 y mayo de 2023

El canal más usado es WhatsApp, lo cual responde a la estrategia del equipo de priorizar este canal por su potencial alcance

CHATICO – ¿QUÉ DICEN LOS DATOS?



¡CHATICO NUNCA TE DEJA EN VISTO!





ALCALDÍA MAYOR
DE BOGOTÁ D.C.

ALTA CONSEJERÍA
DISTRITAL DE TIC

BOGOTÁ

Segunda sesión 2023

Comisión Distrital de
Transformación Digital

La **BOGOTÁ**
que estamos construyendo



El objetivo de la reunión es

llevar a cabo la segunda sesión de la Comisión Distrital de Transformación Digital, la información suministrada será utilizada por el equipo de la Alta Consejería Distrital de TIC para el cumplimiento de las funciones de asignadas a la oficina por el artículo 11 del Decreto 140 de 2021.

En cumplimiento de la Resolución 777 de 2019 por medio de la cual se adopta la Política de Privacidad y Tratamiento de Datos Personales de la Secretaría General de la Alcaldía Mayor de Bogotá, D.C., se solicita la autorización de los participantes para grabar la presente reunión. Esta grabación será utilizada para la elaboración del Acta y consulta del equipo de la ACDTIC.

Se pide a los participantes de la reunión que se abstengan de realizar capturas de pantalla u otras formas de captura de la información, sin contar con la autorización expresa de los presentadores y demás participantes de la reunión. En caso de ser necesario realizar capturas de pantalla se informará a los asistentes y se habilitará un espacio en la reunión para tomar el registro.

Agenda

- 1 Llamado a lista y verificación del quórum.
- 2 Lectura y aprobación del orden del día.
- 3 Apertura de la Comisión a cargo de la Presidencia y Secretaría Técnica.
- 4 Innovación Pública – iBO.
- 5 Presentación Integración Chatico.

- 6 Lineamientos de Seguridad Digital – Protocolo de Atención a incidentes.
- 7 Propositiones y varios.
- 8 Toma de decisiones.
- 9 Compromisos.
- 10 Conclusiones.



3. Apertura de la Comisión a cargo de la Presidencia y Secretaría Técnica.

4. Innovación Pública iBO



ALTA CONSEJERÍA
DISTRITAL DE TIC



5. Presentación Integración Chatico



ALCALDÍA MAYOR
DE BOGOTÁ D.C.

ALTA CONSEJERÍA
DISTRITAL DE TIC


BOGOTÁ





INICIO DEL EJERCICIO DE
SIMULACIÓN CIBERNETICA QUE

6. Lineamientos de Seguridad Digital Protocolo de Atención a incidentes.



- 7 Varios
- 8 Toma de decisiones
- 9 Compromisos
- 10 Conclusiones



ALTA CONSEJERÍA
DISTRITAL DE TIC





ALCALDÍA MAYOR
DE BOGOTÁ D.C.

ALTA CONSEJERÍA
DISTRITAL DE TIC

BOGOTÁ

2023

Alta Consejería Distrital de TIC

Secretaría General - Alcaldía Mayor de Bogotá

Tel: 601 3813000, ext. 2001

Bogotá, Colombia: Carrera 8 # 10 - 65

tic.bogota.gov.co



@ConsejeriaTIC

La **BOGOTÁ**
que estamos construyendo

