UNIVERSIDAD COMPLUTENSE MADRID



INFORME

Observatorio Complutense Desinformación

Elecciones República Dominicana 2024

MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES
Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia
AGENCIA ESTATAL DE INVESTIGACIÓN

AUTORES:

Rafa Rubio
María Garrote
Tamara Álvarez
Vanessa Sánchez
Roelisabel García
Alberto Guevara
Fernanda Rodríguez

UNIVERSIDAD COMPLUTENSE MADRID

ÍNDICE

1. INTRODUCCIÓN 3

1.1 Alianzas 3

2. OBJETIVOS GENERALES Y ESPECÍFICOS 3

2.1 Objetivo general 3
2.2 Objetivos específicos 4

3. DEFINICIONES 5

4. FICHA PAÍS REPÚBLICA DOMINICANA 6

4.1 Datos generales 6
4.2 Datos socioeconómicos de República Dominicana 6
4.3 División política administrativa de República Dominicana 7
4.4 Organización y justicia electoral 8
4.5 Situación política previa 9

5. MARCO NORMATIVO BÁSICO DEL PROCESO DE OBSERVACIÓN 12

5.1 Constitución y legislación electoral 12
5.1.1 Sistema y proceso electoral 12
5.1.2 Leyes de medios de comunicación y acceso a la información 13
5.1.3 Normativa internacional en materia de Derechos Humanos 14
5.2 Marco normativo sobre desinformación electoral 15
5.2.1 Normas específicas sobre desinformación 15
5.2.2 Disposiciones específicas sobre competencia de los órganos electorales 17
5.2.3 Desarrollo reglamentario por parte de los organismos electorales 20

6. ANTECEDENTES 20

6.1 Antecedentes sobre desórdenes informativos en procesos electorales 20
6.2 Antecedentes sobre el organismo electoral. (miembros, valoración general, pacto ético, acuerdos con plataformas 21
6.3 Antecedentes de decisiones jurisdiccionales vinculadas a desórdenes informativos 24
6.4 Antecedentes en materia de ciberseguridad 26
6.4.1 Estrategias nacionales de ciberseguridad de la República Dominicana 26
6.4.2 Ciberataques sufridos en República Dominicana 34
6.4.3 Algunas medidas generales aplicables al contexto electoral que se están aplicando y/o se prevén en los distintos documentos: 37
Plan Estratégico Institucional 2020-2024. Junta Central Electoral 37
Medidas generales derivadas de la Estrategia de Ciberseguridad vigente 39

7. OBSERVACIÓN DE LOS DESÓRDENES INFORMATIVOS 43

7.1 Observación de los desórdenes informativos durante la campaña 43
7.1.1 Criterios de selección de la muestra 43
7.1.2 Análisis de incidentes y recopilación de evidencia 43
7.1.3 Narrativas y metanarrativas detectadas 45
7.2 Análisis de las bibliotecas de anuncios disponibles durante el periodo de la campaña electoral 47
7.2.1 Actores (oficial, órganos electorales, partidos y candidatos, terceros) 47
7.2.2 Importe total e importes más destacados 47
7.2.3 Tipos de anuncios (partidista, integridad electoral) 52
7.3 Incidencias reportadas en materia de ciberseguridad 52

8. REACCIONES Y MEDIDAS ADOPTADAS 53

8.1 Medidas adoptadas por organismos electorales 53
8.2 Medidas adoptadas por las plataformas 54
8.2.1 Contenido orgánico 54
8.2.2 Publicidad 54
8.2.3 Respuesta de las plataformas a las solicitudes de los organismos electorales 55
8.3 Medidas adoptadas por los verificadores 56

9. EVALUACIÓN FINAL Y LECCIONES APRENDIDAS 57

9.1 Evaluación 57
9.2 Lecciones aprendidas 57
9.2.1 Jurídicas 57
9.2.2 Comunicacionales 59
9.2.3 Organizativas 60
9.2.4 Educativas 60
9.2.5 Relaciones interinstitucionales con las plataformas 61
9.2.6 Ciberseguridad 61

OBSERVACIÓN ELECCIONES PRESIDENCIALES Y CONGRESUALES REPÚBLICA DOMINICANA 2024

El **Observatorio Complutense de Desinformación** monitorea los procesos electorales latinoamericanos desde el año 2021. Ha observado procesos en: México, Ecuador, Colombia, Costa Rica, Brasil, Ecuador, Venezuela, Argentina, Chile, España, Panamá y la República Dominicana.

Bajo la metodología basada en el *1st EEAS Report on Foreign Information Manipulation and Interference Threats* de febrero de 2023, elaborado por el servicio de Acción Exterior de la Unión Europea (a partir de ahora Informe EEAS). Esta metodología se ha materializado en un software, elaborado por la Fundación Maldita, que permite integrarla a los sistemas y detectar las metanarrativas a través de la Inteligencia Artificial (IA).

1. INTRODUCCIÓN

Este informe sobre desinformación electoral se centra en analizar los **incidentes de desinformación y la eficacia de las respuestas proporcionadas por la Junta Central Electoral durante las elecciones Presidenciales y Congresuales de la República Dominicana** celebradas el 19 de mayo de 2024. El objetivo es examinar los **desafíos para combatir este fenómeno de desórdenes informativos** en 4 áreas: **jurídica, ciberseguridad, comunicación y educación ciudadana.**

Los **desórdenes informativos** se han convertido en una de las principales amenazas a la democracia, al buscar confundir, manipular e incidir en la opinión y erosionar la confianza de la ciudadanía durante los procesos electorales. Así, la difusión de noticias falsas y desinformación puede distorsionar la realidad, influir en la opinión pública y erosionar la confianza en las instituciones electorales. Contrarrestar la desinformación es crucial para preservar la integridad del proceso democrático y garantizar la toma de decisiones informada por parte de la ciudadanía. Por ello, es esencial implementar estrategias de pedagogía mediática y proporcionar a los ciudadanos las herramientas necesarias para evaluar críticamente la información que consumen. Además, se deben establecer mecanismos de notificación y respuesta para abordar la desinformación de manera eficaz. Esto implica contar con un equipo especializado y el conocimiento para detectar y verificar noticias falsas, establecer un canal de comunicación claro y accesible para que la autoridad electoral actúe oportuna y eficazmente, en tanto la ciudadanía tenga las herramientas para denunciar contenidos engañosos.

El **Observatorio de Desinformación de la Universidad Complutense de Madrid** es una iniciativa del **Grupo de Investigación en Tecnología y Democracia** de dicha universidad, que desarrolla su labor en este ámbito desde 2005. Desde el grupo de investigación hemos desarrollado esta observación de la desinformación electoral y las posibles respuestas en las elecciones en México (2021), Ecuador (2021), Costa Rica (2022), Brasil (2022), España (2023), Argentina (2023), Ecuador (2023), Chile (Plebiscito constituyente 2023), Venezuela (2023), Panamá (2024), República Dominicana (2024) y México (2024).

1.1 Alianzas

El Observatorio ha trabajado en colaboración con la Junta Central Electoral (JCE) y la Pontificia Universidad Católica Madre y Maestra (PUCMM). El país aún no cuenta con ningún verificador certificado que ofreciera suficientes garantías.

2. OBJETIVOS GENERALES Y ESPECÍFICOS

2.1 Objetivo general

El objetivo general de este informe electoral es realizar un análisis exhaustivo y una evaluación detallada de la desinformación durante el proceso electoral y las respuestas ofrecidas por los organismos electorales dominicanos ante el **fenómeno de los desórdenes informativos e Interferencia y Manipulación de la Información (IMI)**, en inglés “Information Manipulation and Interference” (IMI), factores que han afectado y afectan significativamente la percepción y confianza de la ciudadanía en el proceso electoral de la República Dominicana, en sus distintas etapas, a la luz de la experiencia acumulada en la región. De este modo, trataremos de contribuir activamente a la creación de un entorno electoral más seguro y confiable.

La confianza en los procesos electorales es un pilar fundamental que sustenta la democracia. Por lo que la injerencia y manipulación de la información, por parte de distintos actores, no solo distorsiona la realidad, sino que también erosiona la confianza del electorado en sus instituciones, lo que puede llevar a una disminución en la participación ciudadana en los procesos electorales y, en último término, a la deslegitimación de los resultados electorales.

Nuestra labor es **analizar de manera integral las respuestas para combatir estos desórdenes informativos que afectan las democracias y contribuir activamente a la creación de un entorno electoral más seguro y confiable.**

2.2 Objetivos específicos

Para alcanzar los objetivos generales, previamente descritos, se establecen tres objetivos específicos:

I. **Analizar, identificar y clasificar la presencia y actividad de los desórdenes informativos en el contexto electoral.** Este análisis nos permite comprender la magnitud del impacto de la desinformación en la opinión pública. A partir de esta comprensión, podemos desarrollar recomendaciones que busquen mejorar tanto la calidad como la accesibilidad de la información confiable para la ciudadanía.

II. **Medir y valorar la capacidad de respuesta de la JCE y el TSE ante los desórdenes informativos.** Evaluar cómo ambos responden ante la desinformación y ante las incidencias, valorar su desempeño para proteger la integridad del proceso electoral frente a estas amenazas.

III. **Proponer acciones de mejora para combatir los desórdenes informativos en próximos procesos electorales con el propósito de ampliar la capacidad de respuesta de la JCE y el TSE** con el objetivo de cuidar la estabilidad democrática y aumentar la confianza pública en los resultados electorales.

En conjunto, estos objetivos específicos permiten abordar de manera integral los desafíos a los que se enfrentan los procesos electorales.

3. DEFINICIONES

Activos: son los recursos, canales de comunicación, plataformas y herramientas utilizadas por actores para llevar a cabo la interferencia y manipulación de información. Estos activos pueden estar directamente asociados con un actor extranjero o nacional, o ser atribuidos por la comunidad de investigación siguiendo las mejores prácticas actuales. Los activos IMI pueden incluir sitios web, perfiles en redes sociales, estaciones de televisión y otros medios de comunicación, entre otros.

Incidentes: son eventos específicos en los que actores nacionales o extranjeros realizan interferencia y manipulación de información con el objetivo de influir en la percepción, opinión pública, políticas o procesos democráticos en un país objetivo, creando narrativas de desinformación. Estos incidentes pueden involucrar la difusión de información errónea, desinformación, propaganda, operaciones de hackeo y filtración, y otras tácticas de manipulación para desestabilizar o influir en el entorno de información y política.

El factor determinante para considerar si algo puede ser considerado IMI no es el contenido falso o engañoso, sino el comportamiento engañoso o manipulativo.

Algoritmo[1]**:** Arquitectura digital que condiciona el comportamiento humano y se basa en conocimiento sobre lo que funciona con nosotros/as, con nuestro cerebro. Los algoritmos aprenden sobre lo que nos gusta recibir virtualmente, cuáles son los espacios donde se comparten nuestros gustos, conocimientos y opiniones políticas.

Bots: cuentas falsas en redes sociales.

Desinformación, en inglés *disinformation*: "todas las formas de información falsa, inexacta o engañosa diseñada, presentada y promovida para causar daño público intencionalmente o con fines de lucro" (CNECT, 2018, p. 7). Una pieza desinformativa[2] puede transmitirse a mayor velocidad y compartirse infinidad de veces más, debido a que es la noticia que nos gustaría oír, que calza con nuestros sesgos informativos y cognitivos y, porque para ser publicada, no requiere la aceptación y revisión de pares o editores/as, solo la habilidad de alguien para darle la apariencia de verosimilitud.

Fake Media o falsos medios digitales: la mayoría creados en Facebook para difundir información que carece de fuentes, a través de titulares llamativos con el objetivo de viralizar noticias muchas veces erróneas, fuera de contexto, con datos no verificados o falsas. Estos Fake Media generan mucha desinformación entre los electores teniendo efectos en las democracias.

Observables: son elementos concretos para comprender cómo se desarrolló un incidente IMI.

1 Noble, S.U. (2018). Algorithms of Oppression: How Search Engines Reinforce Racism. NYU Press.
2 MediaLab UNMSM (2021). ¿Puedes diferenciar entre Disinformation, misinformation y Mal Information? https://bit.ly/3Y2nXZE

4. FICHA PAÍS REPÚBLICA DOMINICANA

4.1 Datos generales

La República Dominicana fue **fundada el 27 de febrero de 1844, tras independizarse de Haití.** Es una **república democrática y soberana**, con un sistema político **presidencialista** en el que el presidente es el **jefe de Estado y de gobierno**. Su estructura política está basada en una **división de poderes entre el Ejecutivo, el Legislativo y el Judicial**. Tiene **58 años de democracia ininterrumpida,** desde 1966, cuando se estableció un gobierno democrático después de la Guerra Civil de 1965 y la intervención estadounidense.

La República Dominicana es un país situado en el Caribe, ocupa la parte oriental de la isla La Española, la cual comparte con Haití. La capital del país es la ciudad de Santo Domingo. Con una superficie de aproximadamente 48,442 km², la República Dominicana tiene una población de alrededor de 10.8 millones de habitantes (2023), lo que da una densidad poblacional de 225 habitantes por km².



REPÚBLICA DOMINICANA

CAPITAL: SANTO DOMINGO

48,442 KM2

225 HABITANTES POR KM2

ESPAÑOL, IDIOMA OFICIAL

PESO DOMINICANO (DOP)

El idioma oficial de la República Dominicana es español, y la moneda utilizada es el peso dominicano (DOP). En términos de composición étnica, la población dominicana se divide en mestizos (73%), afrodescendientes (16%) y blancos (11%).

La religión predominante en el país es el catolicismo romano (47%). Otras religiones presentes incluyen el protestantismo/evangelicalismo (21%), otras religiones cristianas (2%), y religiones afrocaribeñas, judías y musulmanas (2%). El 28% de la población se identifica como no religiosa.

ETNIA

73% MESTIZOS
16% AFRODESCENDIENTE
11% BLANCA/BLANCO

RELIGIÓN

CATOLICISMO **47%**
PROTESTANTISMO **21%**
OTRAS RELIGIONES CRISTIANAS **2%**
OTRAS RELIGIONES **2%**
SIN RELIGIÓN **28%**

CLIMA

TROPICAL,
CON TEMPORADA
DE LLUVIAS
DE MAYO A NOVIEMBRE.

4.2 Datos socioeconómicos de República Dominicana

El contexto socioeconómico de la República Dominicana se caracteriza por una economía diversificada y cifras destacadas en varios indicadores clave. El **Producto Interno Bruto (PIB) en el 2023 alcanzó aproximadamente $120,629 millones USD**, (Banco Central de la República Dominicana, 2023). **El PIB per cápita se situó en alrededor de $11,200 USD.**

Sostenido principalmente por el sector servicios, que contribuye con el 61% del PIB, seguido por el sector industrial con el 32%, y el sector agrícola con el 7% (MEPyD, 2023). Durante la última década, la economía dominicana ha experimentado un **crecimiento promedio anual de 5-6%**, respaldado por inversiones significativas tanto a nivel nacional como internacional. Este crecimiento ha sido crucial para la expansión y diversificación de sectores clave como el turismo, las zonas francas industriales y la agricultura. **La inflación se ha registrado en un promedio del 4-5% en los últimos tres años** (MEPyD, 2023).



En términos de distribución de ingresos, el **coeficiente de Gini se estima en 0.378 para 2023**, reflejando un nivel moderado de desigualdad económica en el país. La **pobreza monetaria afecta al 23% de la población** (MEPyD, 2023).

La población dominicana presenta una estructura demográfica joven, con una **edad media de aproximadamente 28 años y una esperanza de vida al nacer de 74.5 años.** La distribución por género muestra una ligera mayoría de mujeres, que representan el 51% de la población, mientras que los hombres constituyen el 49% restante (MEPyD, 2023).

El **43.4% de la población se encuentra en condiciones de pobreza extrema (ICV-I) y pobreza moderada (ICV-II)**, de acuerdo con los datos del Sistema Único de Beneficiarios (SIUBEN-2021). Según el Índice de Pobreza Multidimensional, IPM-RD, la **informalidad laboral afecta al 66.2% de la población económicamente activa, la brecha digital al 36.6%, y el acceso limitado a agua potable para el 61.7% de la población** (SIUBEN-2021).



4.3 División política administrativa de República Dominicana

La República Dominicana se divide políticamente en **un Distrito Nacional y 10 regiones, compuestas por 31 provincias, 157 municipios y 235 distritos municipales.** La ciudad de Santo Domingo de Guzmán es la capital de la República y sede del gobierno nacional, representa el Distrito Nacional. El **sistema político es presidencialista, bajo un Estado Social y Democrático de Derecho,** organizado en forma de **República unitaria, democrática y representativa**. **Todos los cargos de elección popular, Presidente, Senadores y Diputados del Congreso Nacional y autoridades municipales tienen un período de ejercicio de 4 años.**

El **Poder Legislativo se ejerce en nombre del pueblo por el Congreso Nacional, conformado por el Senado de la República y la Cámara de Diputados siendo cada uno**

de sus miembros elegidos por sufragio universal. El Senado de la República está integrado por 32 senadores y senadoras, elegidos por los habitantes de las 31 provincias y el Distrito Nacional que integran el país. La Cámara de Diputados está compuesta por 190 miembros (aproximadamente), cada provincia elige un número específico de diputados en función de su población, son elegidos mediante un sistema de representación proporcional por listas cerradas y bloqueadas, con escaños asignados según el porcentaje de votos obtenidos por cada partido político o coalición electoral en cada circunscripción electoral.
Cada provincia es gobernada por un Gobernador Civil, designado por el Presidente de la República, y administrada localmente por un Consejo Provincial. Los municipios, por su parte, son dirigidos por un Alcalde y un Concejo Municipal elegido por voto popular cada cuatro años. A su vez, los distritos municipales tienen una representación del poder ejecutivo y legislativo en el director de distrito, y vocales respectivamente.



4.4 Organización y justicia electoral

Autoridades y Órganos administrativos y jurisdiccionales en materia electoral:

I. **Junta Central Electoral (JCE):** máxima autoridad en materia de administración y organización de los procesos electorales. Órgano autónomo con personalidad jurídica e independencia técnica, administrativa, presupuestaria y financiera. Su finalidad principal es organizar y dirigir asambleas electorales para la celebración de elecciones y mecanismos de participación popular establecidos por la Constitución y las leyes. Administra y norma los Actos del Estado Civil.
Está integrada por un presidente y cuatro miembros y sus suplentes, elegidos por un periodo de cuatro años por el Senado de la República.

II. **Tribunal Superior Electoral (TSE):** es el órgano encargado de la justicia electoral y la máxima autoridad en asuntos contenciosos electorales, en concordancia con la Constitución y las leyes. Es una entidad autónoma con personalidad jurídica e independencia funcional, administrativa, presupuestaria y financiera, por lo tanto, no está subordinada a ninguna otra organización estatal. Tiene su sede en la ciudad de Santo Domingo de Guzmán, capital de la República Dominicana, y ejerce su jurisdicción en todo el territorio nacional. Su organización, funcionamiento y atribuciones están establecidos en la Constitución de la República, en los artículos 214 y 215, así como en su Ley Orgánica Número 29-11 del 20 de enero de 2011.

III. **Juntas Electorales:** son órganos de carácter permanente con funciones administrativas y contenciosas. En materia administrativa están subordinadas a la Junta Central Electoral; en lo contencioso, sus decisiones son recurribles ante el Tribunal Superior Electoral, de conformidad con la ley.
Operan en el Distrito Nacional y en 157 municipios, con la responsabilidad de organizar los procesos electorales en sus respectivas demarcaciones y conocen las protestas, impugnaciones y apelaciones sobre el proceso en los Colegios Electorales de sus jurisdicciones.

IV. **Oficinas de Coordinación de Logística Electoral en el Exterior (OCLEE):** La Junta Central Electoral (JCE) ha establecido las Oficinas de Coordinación de Logística Electoral en el Exterior (OCLEE) con el propósito de captar, reclutar, capacitar y seleccionar a las personas que conformarán los Colegios Electorales. Estas oficinas operan de acuerdo con las disposiciones y bajo la supervisión de la JCE.
En cada lugar de votación en el extranjero, se encuentra una OCLEE que realiza funciones similares a las Juntas Electorales. Tienen la autoridad para resolver situaciones relacionadas a objeciones presentadas en los Colegios Electorales en el extranjero, especialmente en lo que respecta a votos objetados y votos anulables. Cada OCLEE está compuesta por un presidente, un primer vocal, un segundo vocal y sus respectivos suplentes.
En el extranjero se llevan a cabo las elecciones para elegir al presidente o presidenta, vicepresidente o vicepresidenta de la República, así como siete diputados o diputadas de ultramar.

V. **Colegios Electorales:** Los Colegios Electorales son los espacios donde la Junta Central Electoral y las Juntas Electorales agrupan a los ciudadanos y ciudadanas según su lugar de residencia, con el objetivo de que puedan ejercer su derecho al voto en las Asambleas Electorales y otros mecanismos de participación popular, convocados de acuerdo con la Constitución y las leyes.
Estos colegios deben ser formados a más tardar 30 días antes de la fecha en que se llevarán a cabo las elecciones.

Para las elecciones generales ordinarias de 2024, se establecerán alrededor de 17,310 colegios electorales en 4,418 centros de votación.

VI. **Asambleas Electorales:** se refieren al conjunto de personas con el derecho de elegir y ser elegibles (Padrón Electoral) convocados en fechas establecidas, con el propósito de seleccionar los cargos establecidos por la Constitución.



AUTORIDADES Y ÓRGANOS ADMINISTRATIVOS Y JURISDICCIONALES EN MATERIA ELECTORAL

- JUNTA CENTRAL ELECTORAL (JCE)
- TRIBUNAL SUPERIOR ELECTORAL (TSE)
- JUNTAS ELECTORALES
- OFICINAS DE COORDINACIÓN EN EL EXTERIOR (OCLEE)
- COLEGIOS ELECTORALES
- ASAMBLEAS ELECTORALES

4.5 Situación política previa

La República Dominicana opera bajo un sistema democrático representativo, con elecciones regulares para elegir a sus representantes tanto a nivel nacional como local. Con 58 años de estabilidad democrática.

El **Instituto Freedom House ha posicionado a la República Dominicana (RD) en derechos civiles con una puntuación de 27/40 y en libertades con una puntuación de 41/60.** De acuerdo con el análisis de Freedom House, en este país se llevan a cabo elecciones relativamente libres, aunque en los últimos años han surgido controversias en torno a la implementación de un nuevo marco electoral.

La **participación y confianza en el gobierno local se mantiene en niveles medios** (40%), con una estabilidad relativa en los últimos años. Este nivel de confianza se asocia estrechamente con la **aprobación de la gestión presidencial, y sugiere una conexión entre lo local y lo nacional**, de acuerdo a datos de Latinobarómetro , 2023. Destaca que la **confianza interpersonal ha experimentado un ligero repunte en 2023: llega al 59%** y evidencia la importancia de las relaciones interpersonales en el entramado social y político.

En el 2023, Dominicana **ascendió tres puntos en el índice de percepción de la corrupción en el sector público**, alcanzando el puesto 108 de un total de 180 países, colocándose como el único país de la región que ha logrado avances significativos en la lucha contra la corrupción desde 2021, de acuerdo a la Organización Transparencia Internacional.

En cuanto a la **tolerancia política, se observa estabilidad en los niveles generales, pero con variaciones significativas** al considerar distintas situaciones. La República Dominicana se muestra comparativamente alta en los niveles de tolerancia hacia personas críticas del sistema político a postularse a cargos (34%) o dar un discurso (37%). Al mismo tiempo, la ciudadanía demuestra una menor tolerancia en el contexto de la participación cívica de personas gay (27%), una cifra baja en comparación con otros países. Estos hallazgos proporcionan una comprensión extensa de la participación ciudadana y la percepción democrática en la República Dominicana.

El contexto político dominicano en los últimos 5 años ha experimentado una serie de eventos significativos que han marcado la agenda nacional teniendo repercusiones tanto internas como externas.

A continuación, se desglosan los **principales hechos políticos desde el 2019 hasta la fecha** en cuatro aspectos: **Institucionalidad, Partidos políticos y competencia electoral, Sociedad civil y participación ciudadana y Relaciones Exteriores**.

1. **Institucionalidad:** el 17 de febrero de 2019 se aprobó la Ley Orgánica de Régimen Electoral No. 15-19. Esta ley introdujo varias reformas importantes al sistema electoral del país, como: la Regulación de Campañas Electorales, estableciendo normas más estrictas para la financiación de campañas electorales y la publicidad política; establecen normativas para la celebración de convenciones internas de los partidos políticos; se introduce un sistema de representación proporcional para las elecciones de senadores y diputados; incluye la posibilidad de que los ciudadanos puedan presentar propuestas de reforma a través de iniciativas populares.

   En el año 2020, la República Dominicana fue el primer país en celebrar elecciones en medio de la pandemia de COVID-19, (municipales, congresuales y presidenciales), OEA (2020). El 16 de febrero de 2020, previo a la cuarentena, estaba previsto celebrar las elecciones municipales, dicho evento estuvo marcado por un incidente particular: la suspensión repentina (el mismo día) después de que se detectaron fallos técnicos en el sistema de voto automatizado utilizado por la Junta Central Electoral (JCE). Este incidente llevó a la cancelación del proceso electoral en todo el país, provocando críticas generalizadas y un posterior reajuste en el calendario electoral.

2. **Partidos políticos y competencia electoral:** República Dominicana ha estado liderada principalmente por dos organizaciones: Partido de la Liberación Dominicana (PLD) y el Partido Revolucionario Dominicano desde el 2000 hasta el 2014. De estas organizaciones, debido a crisis internas, han surgido varias agrupaciones políticas siendo las más prominentes por resultados electorales el Partido Revolucionario

Moderno (actual partido de gobierno deriva del PRD tras crisis en el 2014), y el Partido Fuerza del Pueblo (deriva del PLD tras crisis en el 2019). En el año 2019, se produjeron eventos significativos relacionados con el Partido de la Liberación Dominicana (PLD) y su proceso interno de elecciones primarias. Leonel Fernández, expresidente y presidente del partido en ese momento fue uno de los principales contendientes en las elecciones primarias del partido. Durante este proceso, surgieron controversias y disputas sobre la transparencia y la integridad del proceso electoral interno. Fernández y su equipo denunciaron irregularidades y supuestas manipulaciones en el conteo de votos, lo que generó tensiones dentro del partido y entre sus seguidores y su posterior salida para fundar una nueva agrupación política.

En el 2020 en las elecciones presidenciales el partido revolucionario moderno gana los comicios, terminando con la larga dominación del partido de la liberación dominicana (16 años consecutivos).

En el 2024, en las elecciones de alcaldes y regidores que se celebraron en febrero, la representación de la mujer en elecciones municipales alcanzó el 42.84%, un avance positivo para el país, con 1,598 mujeres elegidas en los cargos de alcaldesa, vicealcaldesas, regidoras, directoras y vocales. En cuanto a representación política de alcaldes, el PRM (el partido de gobierno) y aliados, se alzó con 61.10%, respecto al partido de oposición PLD que obtuvo el 37.61%.

3. **Sociedad civil y participación ciudadana:** los movimientos de participación ciudadana se convirtieron en catalizadores de la lucha anticorrupción en los últimos 5 años. Liderando protestas masivas en demanda de transparencia y combate a la corrupción, especialmente tras el escándalo de los sobornos de Odebrecht que involucró a figuras políticas de alto nivel, jugaron un rol importante. El movimiento Marcha Verde, fundado en el 2017, logró movilizar a amplios sectores de la población y poner las preocupaciones sobre la corrupción y la transparencia en el centro del debate público en el contexto de las elecciones de 2020, influyendo en la agenda política y en los resultados electorales.

4. **Relaciones Exteriores:** el país mantiene relaciones diplomáticas estables con diversas naciones y es miembro activo de organizaciones regionales e internacionales como la OEA y la ONU. Las relaciones internacionales juegan un papel crucial en la política exterior dominicana, influenciada por intereses económicos, seguridad regional y colaboración en temas globales como el cambio climático y la migración. Algunas medidas migratorias como la gestión de relaciones con Haití han tensado por períodos las relaciones con Estados Unidos y otros actores internacionales, así como la participación en organismos regionales y globales.

La estabilidad política en la República Dominicana ha sido relativamente sólida en comparación con algunos de sus vecinos regionales. Según la Organización de Estados Americanos (OEA), el país ha mantenido un marco democrático funcional con procesos electorales regulares y pacíficos. Sin embargo, la República Dominicana enfrenta desafíos significativos que afectan su gobernanza y la percepción pública de su sistema político.

5. MARCO NORMATIVO BÁSICO DEL PROCESO DE OBSERVACIÓN

5.1 Constitución y legislación electoral

El marco jurídico del sistema electoral en la República Dominicana se sustenta en la **Constitución de la República y en las leyes que regulan los procesos electorales**. La Constitución, promulgada en 2010 y reformada posteriormente, establece en su artículo 211 las bases legales para la organización, dirección y supervisión de las elecciones, asignando a la Junta Central Electoral (JCE) la responsabilidad exclusiva de garantizar la libertad, transparencia, equidad y objetividad de los comicios, así como la administración del registro civil y del padrón electoral.

En consonancia con el mandato constitucional, la **Ley Orgánica del Régimen Electoral, Ley No. 15-19, promulgada en 2019, detalla las disposiciones específicas para la organización de los procesos electorales en el país.** Esta ley regula aspectos clave como la inscripción de candidatos, la organización de las votaciones, el escrutinio de votos y la proclamación de los resultados. Además, establece normativas sobre la financiación de los partidos políticos y la fiscalización de los recursos destinados a las campañas electorales, con el fin de asegurar un proceso electoral justo y transparente.

El marco legal también incluye la **Ley de Partidos, Agrupaciones y Movimientos Políticos, Ley No. 33-18, que regula la constitución, funcionamiento, derechos y obligaciones de los partidos políticos, fortaleciendo su institucionalidad y asegurando que sus actividades se desarrollen en consonancia con los principios democráticos establecidos en la Constitución**.

En conjunto, la Constitución de la República Dominicana y las leyes electorales proporcionan el sustento jurídico necesario para la organización de elecciones libres y transparentes, estableciendo los mecanismos y procedimientos que garantizan la participación ciudadana en los procesos electorales, conforme a los principios democráticos consagrados en la Carta Magna.

Respecto a las modificaciones introducidas por la Ley No. 15-19 en 2019, comparada con la Ley Electoral No. 275-97, destacan **cambios en la organización y supervisión electoral, el financiamiento de campañas, la implementación del voto preferencial y la transparencia en la publicidad de resultados.** Estas reformas reflejan un esfuerzo por modernizar el sistema electoral, adaptándolo a las realidades políticas y sociales contemporáneas.

5.1.1 Sistema y proceso electoral

Sistema electoral: se rige por la Constitución, las leyes números: 20-23, 33-18, 157-13, 176-07, 29-11, que establecen el marco legal en el cual interactúan la Junta Central Electoral, las Juntas Electorales, los Colegios Electorales, las organizaciones políticas y el Tribunal Superior Electoral.

El sistema electoral establece una mayoría absoluta para las elecciones del presidente y vicepresidente de la República. En las elecciones congresionales y municipales, se aplica un sistema de mayoría simple, específicamente para los senadores, alcaldes y directores de distritos municipales. En cuanto a la representación proporcional: en cada provincia, municipio, circunscripción electoral o distrito municipal, los partidos políticos o agrupaciones políticas independientes presentan candidatos para varios cargos incluyendo senadores,

diputados, diputados nacionales por acumulación de votos y representantes ante parlamentos internacionales, diputados y diputadas representantes de la comunidad dominicana en el exterior, alcaldes, vice alcaldes, regidores y suplentes de regidores, directores, subdirectores y vocales de distritos, ya sea a través de boletas conjuntas o separadas para cada nivel de elección. Para asignar los escaños de los representantes electos para la Cámara de Diputados, Concejos de Regidores y Juntas de Vocales, se implementa un sistema de voto preferencial a través de listas cerradas y desbloqueadas.

Paridad: la Ley Orgánica de Régimen Electoral (2019) establece que las nominaciones y propuestas de candidaturas a la Cámara de Diputados, a las Regidurías y vocales se regirán por el principio de equidad de género, por lo que éstas deberán estar integradas de acuerdo a lo establecido en la Ley de Partidos, por no menos de un 40% ni más de un 60% de hombres y mujeres de la propuesta nacional.

5.1.2 Leyes de medios de comunicación y acceso a la información

La **Constitución Dominicana** establece las siguientes disposiciones relacionadas con las leyes de medios de comunicación y el acceso a la información:

1. **Derecho a la información:** el Artículo 49 de la Constitución reconoce el derecho de todas las personas a buscar, recibir y difundir informaciones de todo tipo, en cualquier medio de comunicación, sin censura previa.
2. **Libertad de expresión:** el Artículo 49 también garantiza la libertad de expresión y opinión, así como la libertad de prensa, como derechos fundamentales de los ciudadanos.
3. **Regulación de los medios:** aunque la Constitución salvaguarda la libertad de expresión, también establece que el ejercicio de estos derechos debe realizarse dentro del marco de las leyes que regulen la materia. Es decir, los medios de comunicación están sujetos a regulaciones legales que buscan proteger otros derechos fundamentales y el interés público.
4. **Acceso a la información pública:** el Artículo 49 reconoce el derecho de acceso a la información pública, estableciendo que toda persona tiene derecho a acceder a los datos que obren en poder de las entidades públicas y a conocer el estado de los expedientes y documentos administrativos, salvo las excepciones que establezcan las leyes.
5. **Leyes y normativas:** además de la Constitución, existen leyes y normativas específicas que regulan los medios de comunicación y el acceso a la información en la República Dominicana, las cuales detallan los procedimientos para solicitar y obtener información pública, así como las responsabilidades y obligaciones de los medios de comunicación en el ejercicio de su labor.

En materia electoral, en la **Ley Orgánica de Régimen Electoral No. 15-19,** se establecen las normativas para la organización, administración y supervisión de los procesos electorales en el país, y cuenta con disposiciones específicas que regulan la participación de los medios de comunicación, en los siguientes aspectos:

1. **Cobertura electoral:** la ley establece que los medios de comunicación tienen la responsabilidad de informar de manera equitativa y objetiva sobre los procesos electorales. Esto implica brindar cobertura a todos los candidatos y partidos políticos de manera balanceada y no discriminatoria.
2. **Regulación de publicidad electoral:** la normativa regula la publicidad electoral, asegurando que sea transparente y respete los límites establecidos en cuanto a

tiempos y formas de difusión. Se establecen restricciones para evitar la saturación y el desequilibrio en la exposición de las campañas políticas en los medios.
3. **Acceso a los debates y foros electorales:** la ley también motiva el acceso equitativo de los candidatos y partidos a los debates y foros electorales organizados por los medios de comunicación, promoviendo así el intercambio de ideas y propuestas. Aunque no contempla la organización y/o participación como un deber dentro del proceso electoral.
4. **Supervisión y fiscalización:** la Junta Central Electoral (JCE) es la autoridad encargada de supervisar y fiscalizar el cumplimiento de estas disposiciones por parte de los medios de comunicación, asegurando que se respeten los principios de igualdad, imparcialidad y transparencia en la cobertura electoral.

5.1.3 Normativa internacional en materia de Derechos Humanos

La República Dominicana ha consolidado su compromiso con el Derecho Internacional de los Derechos Humanos mediante la ratificación de una serie de instrumentos clave. Estos tratados han sido fundamentales para integrar en la normativa interna del país los principios y obligaciones internacionales en materia de derechos humanos, fortaleciendo así el marco legal y promoviendo la protección de los derechos fundamentales de sus ciudadanos.

Entre los tratados internacionales más significativos ratificados por la República Dominicana se destacan:

1. **El Pacto Internacional de Derechos Civiles y Políticos (PIDCP)**, ratificado en 1977. Este pacto establece un conjunto de derechos esenciales, incluyendo la libertad de expresión, el derecho a un juicio justo, y la libertad de asociación. Estos derechos son fundamentales para garantizar la protección de las libertades civiles y políticas de los individuos dentro del territorio dominicano.
2. **El Pacto Internacional de Derechos Económicos, Sociales y Culturales (PIDESC)**, también fue ratificado en 1977. Este pacto se centra en la protección de derechos como el acceso a la educación, la salud y el trabajo digno. La inclusión de este tratado en la normativa interna ha permitido a la República Dominicana trabajar en la promoción de un nivel de vida adecuado para todos sus habitantes.
3. **La Convención sobre la Eliminación de todas las formas de Discriminación contra la Mujer (CEDAW)**, ratificada en 1982. Esta convención es un instrumento crucial en la lucha contra la discriminación de género, promoviendo la igualdad de derechos entre hombres y mujeres. La ratificación de la CEDAW ha impulsado la implementación de políticas públicas orientadas a garantizar la equidad de género en la República Dominicana.
4. **La Convención sobre los Derechos del Niño (CDN)**, ratificada en 1991. Esta convención protege los derechos fundamentales de los niños, asegurando su acceso a la educación, la salud, y la protección frente al abuso y la explotación. La CDN ha sido clave en la formulación de políticas que priorizan el bienestar y desarrollo integral de la niñez en el país.
5. **La Convención Internacional sobre la Eliminación de todas las formas de Discriminación Racial (CERD)**, ratificada en 1983. Esta convención aborda la erradicación de la discriminación racial en todas sus manifestaciones, promoviendo la igualdad y el respeto por la diversidad cultural. La ratificación de la CERD refuerza el compromiso del país con la lucha contra el racismo y la promoción de una sociedad inclusiva.
6. **La Convención contra la Tortura y otros tratos o Penas Crueles, Inhumanos o Degradantes**, ratificada en 1987. Este tratado prohíbe la tortura y otros tratos

inhumanos, asegurando que todas las personas sean tratadas con dignidad y respeto, independientemente de su situación.

7. **La Convención Americana sobre Derechos Humanos (Pacto de San José de Costa Rica)**, fue ratificada en 1978. Como instrumento regional, este pacto protege los derechos civiles y políticos en el ámbito de la Organización de los Estados Americanos (OEA). La inclusión de este tratado en el marco normativo dominicano refuerza el compromiso del país con la protección de los derechos humanos a nivel regional.
8. **La Convención sobre los Derechos de las Personas con Discapacidad (CDPD)**, fue ratificada en 2008. Este tratado promueve y protege los derechos y la dignidad de las personas con discapacidad, asegurando su inclusión y plena participación en la sociedad dominicana.

La ratificación de estos tratados internacionales demuestra el compromiso de la República Dominicana con el Derecho Internacional de los Derechos Humanos, constituyendo un marco legal robusto que respalda y promueve la protección de los derechos fundamentales de todos los ciudadanos, garantizando así el cumplimiento de las obligaciones internacionales en esta materia.

5.2 Marco normativo sobre desinformación electoral

5.2.1 Normas específicas sobre desinformación

Las **reglas concretas** que regulan la campaña electoral se enmarcan en unas **normas éticas** (art. 170 Ley electoral):

1) Las opiniones políticas de los demás partidos, agrupaciones o movimientos políticos y candidatos, de manera que las ideas se respondan con ideas, dentro de un marco de respeto y madurez:
2) La dignidad humana de los dirigentes y militantes de los partidos, agrupaciones o movimientos políticos, candidatos electorales y de la población en general;
3) El derecho de los partidos, agrupaciones o movimientos políticos y sus alianzas o coaliciones, inscritas para participar en las elecciones y de los candidatos admitidos, a realizar actividades lícitas en orden a la captación de sufragios; y
4) El derecho al buen nombre, la honra y reputación de las personas, por consiguiente, en ningún aviso o manifestación publicitaria, podrán utilizarse expresiones ofensivas en forma directa o indirecta hacia los demás participantes del proceso, y tampoco deben usarse calificativos insultantes, ni referencias degradantes a la persona, al nombre o apellidos de los candidatos y miembros de otras organizaciones políticas.

Para el correcto desarrollo de las campañas electorales la Ley electoral prevé, en otras medidas:

- Prohibición de actos y medios de propaganda anónimos (art. 171)
- Derecho de rectificación (art. 175)
- Prohibición de propaganda electoral fuera del periodo electoral o durante la veda electoral (art. 179)

El art. 200.3 de la Ley electoral permite a la Junta Central Electoral:

“Sancionar durante la campaña electoral a toda persona, candidato, partido, agrupación o movimiento político que usare frases y emitiere conceptos, por cualquier medio de difusión,

contrarios a la decencia, al decoro y a la dignidad de los candidatos, partidos, agrupaciones o movimientos políticos adversos. A estos fines, la Junta Central Electoral queda investida de la facultad para hacer amonestaciones a los partidos, agrupaciones o movimientos políticos que violen esta norma de propaganda, con derecho a requerir de la persona o empresa de divulgación o comunicación de masas la identificación de la entidad política o su representante que autorizó a efectuar tal publicación, y publicar el desagravio o desmentido correspondiente según la Ley núm.6132, del 15 de diciembre de 1972, de Expresión y Difusión del Pensamiento."

La Ley electoral describe las infracciones administrativas y los delitos electorales. Corresponde a la Junta Central Electoral establecer sanciones de carácter administrativo, en aquellos casos que se produzcan faltas administrativas. Conforme al artículo 306, "Constituirán **infracciones administrativas**, las cuales serán castigadas con el pago de compensaciones pecuniarias en base a salarios mínimos, aquellas **violaciones que cometan ciudadanos, ciudadanas o instituciones de cualquier naturaleza, al no cumplir las disposiciones de esta ley en lo que respecta al desempeño de las funciones que les fueren asignadas o los que violentaren los procedimientos establecidos en esta ley**". El artículo 308 detalla las faltas administrativas y las sanciones correspondientes. Destacan, por su relación con la campaña, los numerales 8 (prohibición de actos y uno de medios anónimos), 12 (violentar u obstaculizar la propaganda de otros partidos, agrupaciones o movimientos políticos, candidatos o candidatas) y 13 (difusión de propaganda electoral durante la veda electoral). Todas estas infracciones están previstas únicamente para los partidos, agrupaciones o movimientos políticos, candidatos o candidatas. Es decir, no se prevé que la infracción sea cometida por un particular ajeno a la contienda electoral.

En cuanto a los **delitos electorales**, cuyo conocimiento corresponde a los tribunales penales ordinarios, se encuentran descritos en los artículos 310 y siguientes. Entre las conductas tipificadas no se encuentra ninguna que se refiera concretamente a la desinformación o a actividades que pongan en peligro la integridad electoral. No obstante, hay dos apartados que con carácter genérico podrían servir de base para incluir otras conductas no expresamente tipificadas:

Art. 310. 6): Los que violaren cualquiera de las resoluciones que en atribuciones reglamentarias dicte la Junta Central Electoral.

Art. 311. 6): Los que cometieren algún hecho que infringiere esta ley que no esté penado de otro modo por ella.

Además, el art. 317 regula los **crímenes contra la integridad de las elecciones**, aunque limitados a la utilización de cualquier mecanismo que **impida la celebración de las elecciones en las fechas previstas** por la Constitución, o que ejecuten acciones tendentes a dicho propósito. Si las acciones se hicieren utilizando sistemas informáticos, electrónicos, telemáticos o de telecomunicaciones, se impondrá a los autores la pena prevista para el **sabotaje** en la Ley núm.53-07, del 23 de abril de 2007, sobre Crímenes y Delitos de Alta Tecnología.

Precisamente la **Ley sobre Crímenes y Delitos de Alta Tecnología** ofrece un marco legal adecuado para afrontar los peligros de ciberataques y reforzar la ciberseguridad en la gestión de los procesos electorales. Además, permite castigar la **difamación y la injuria pública cuando se cometan a través de medios electrónicos**, informáticos, telemáticos, de telecomunicaciones o audiovisuales (arts. 21-22). También habilita al Ministerio Público para ordenar el suministro de información a los proveedores de servicios y **secuestrar o eliminar**

contenidos de un sistema de información (art. 54 d), e) y h)).

Asimismo, resulta muy relevante la previsión específica de delitos de violencia política contra las mujeres en razón de género (art. 316. 21):

a) Ejerza cualquier tipo de violencia, contra una mujer, que afecte el ejercicio de sus derechos políticos y electorales, o el desempeño de un cargo público;
b) Amenace o intimide a una mujer, directa o indirectamente, con el objeto de inducir u obligar a presentar su renuncia a una precandidatura o candidatura de elección popular;
c) Amenace o intimide a una mujer, directa o indirectamente, con el objeto de inducir u obligar a presentar su renuncia al cargo para el que haya sido electa o designada;
d) Limite o niegue a una mujer el otorgamiento, ejercicio de recursos o prerrogativas, en términos de ley, para el desempeño de sus funciones, empleo, cargo, comisión, o con la finalidad de limitar el ejercicio de sus derechos políticos y electorales;
e) Realice o distribuya propaganda político electoral que degrade o denigre a una mujer, basándose en estereotipos de género, con el objetivo de menoscabar su imagen pública o limitar sus derechos políticos y electorales.

Por último, también hay que tener en cuenta las previsiones de la **Ley 33-18 de Partidos, Agrupaciones y Movimientos Políticos**, que **prohíbe** a los partidos, agrupaciones y movimientos políticos (art. 25. 1), 3) y 4):

1) Realizar toda actividad que tienda o tenga por resultado **suprimir, desconocer o disminuir los derechos humanos o las libertades,** derechos o garantías individuales y sociales que consagran la Constitución y las leyes.
2) Promover o propiciar la alteración del orden público
3) Influir por **medio de violencia, amenazas, coacciones, engaños, desinformación, sobornos o dádivas** sobre los ciudadanos para obtener votos a favor de sus candidatos o en contra de determinados candidatos internos o de otros partidos, o para provocar la abstención electoral de los mismos.

Dichas conductas, cuando fueran realizadas por los partidos, serán sancionadas con multas de diversa cuantía conforme al art. 78.1 Ley de Partidos. Cuando fueran efectuadas por **personas físicas o jurídicas** que no sean partidos serán sancionadas también con multas, conforme al artículo 80 de la Ley de Partidos.

5.2.2 Disposiciones específicas sobre competencia de los órganos electorales

Sobre las competencias de los órganos electorales es necesario distinguir dos vías de actuación de las Juntas electorales. La imposición de sanciones administrativas se efectúa de acuerdo con el **procedimiento administrativo sancionador**, previsto en el Reglamento correspondiente[3]. Se aplica a las infracciones recogidas en los arts. 305 a 308 de la Ley electoral y en los arts. 72 y 78.2 de la ley de partidos. Para instruir los procedimientos se crea la **Unidad de Atención, Seguimiento y Mecanismos de ejecución de sanciones**. Entre sus atribuciones se encuentran las de dar curso a las denuncias, recabar pruebas y realizar recomendaciones a la Junta Central Electoral mediante dictamen para la aplicación de medidas cautelares y sanciones.

[3] Reglamento que crea el procedimiento administrativo sancionador y pone en funcionamiento la Unidad de Atención, Seguimiento y Mecanismos de ejecución de sanciones con ocasión de infracciones administrativas electorales y medidas cautelares que establecen las leyes 20-23 orgánica de régimen electoral y 33-18 de partidos, agrupaciones y movimientos políticos, de 2023.

El **procedimiento sancionador** puede iniciarse de oficio o mediante denuncia de parte. La Unidad encargada decidirá sobre su admisión a trámite. Tras la notificación de la denuncia o del pliego de cargos, en caso de iniciación de oficio, la parte denunciada dispone de 10 días para presentar las alegaciones. La Unidad encargada emitirá el dictamen correspondiente en diez días y el Pleno de la JCE en cinco días, dictará la resolución correspondiente. Dicha resolución puede ser objeto de recurso de reconsideración ante la misma JCE o de recurso ante el Tribunal Superior Electoral.

El reglamento también prevé la adopción de **medidas cautelares** (arts. 11-20) que permiten al JCE la ejecución de una acción rápida y oportuna que permita suspender una omisión, acción o actuación realizada por cualquier actor electoral o por particulares y hacer cesar algún tipo de perturbación que afecte, de forma ilegal, manifiesta o evidente el normal funcionamiento del sistema electoral y que esté prevista como infracción administrativa. Las medidas pueden acordarse incluso antes de la iniciación del procedimiento sancionador. Pueden adoptarse de oficio por el Pleno de la JCE o a instancia de parte o de la Unidad encargada, que trasladará un dictamen al Pleno.

En sus **funciones contenciosas**, la Junta Central Electoral, las Juntas electorales y las OCLEE actúan como Tribunal electoral de primer orden en la llamada **acción de amparo electoral**, cuya finalidad es la tutela del derecho al sufragio activo y pasivo, competencia circunscrita sólo al día en que se reúnan las asambleas electorales. Además, también pueden dictar **medidas cautelares** para garantizar la protección del derecho al sufragio de uno o más ciudadanos.

Los procedimientos están descritos en el **Reglamento de procedimientos contenciosos electorales.** Con carácter general se inician por instancia motivada (art. 26). Una vez recibida, se fija una audiencia en un plazo de entre uno y tres días. Sin embargo, dependiendo de la urgencia o de la naturaleza del proceso, a apreciación del presidente del órgano apoderado o por solicitud de parte, ésta podrá ser fijada de día a día o de hora a hora.

En todo caso, una vez emitida la proclama de apertura del período electoral por la Junta Central Electoral, de manera excepcional, los plazos serán determinados a discreción del presidente del órgano contencioso electoral correspondiente, mediante decisión motivada, salvo disposición expresa por la ley y observando el debido proceso y garantizando los derechos del sujeto destinatario de la notificación.

Se prevé la posibilidad de intervención voluntaria en los procesos para toda persona física o jurídica con interés legítimo.

La **acción de amparo electoral** puede interponerse ante el **Tribunal Superior Electoral** o ante las Juntas Electorales y las OCLEE (arts. 130 y siguientes). Es admisible contra todo acto u omisión de autoridad pública o de cualquier particular, que en forma actual o inminente y con arbitrariedad o ilegalidad manifiesta lesione, restrinja, altere o amenace los derechos fundamentales político-electorales (TSE) o el derecho fundamental al sufragio activo o pasivo (Juntas Electorales y OCLEE).

Posee legitimación activa toda persona física o moral que reclame protección o restauración inmediata de su derecho fundamental de sufragio activo o pasivo. También está legitimado el Defensor del Pueblo.

En cuanto al procedimiento, la acción de amparo electoral se iniciará de forma verbal o mediante escrito dirigido a la autoridad electoral. Una vez el asunto quede en estado de fallo, el órgano contencioso electoral correspondiente deberá rendir su decisión el mismo día de la audiencia en dispositivo, disponiendo de un plazo de hasta cinco días hábiles para motivarla.

La decisión que concede el amparo electoral deberá contener:

1) Mención de la persona en cuyo favor se concede el amparo electoral;
2) Identificación de la persona física o moral, pública o privada, órgano, ente o agente de la administración pública contra cuyo acto u omisión se concede el amparo electoral;
3) Determinación precisa de lo ordenado a cumplirse, de lo que debe o no hacerse, con las especificaciones necesarias para su ejecución;
4) Plazo para cumplir lo decidido;
5) Sanción prevista en caso de incumplimiento.

Todas las sentencias dictadas por las Juntas Electorales y la OCLEE pueden ser recurridas en revisión ante el Tribunal Constitucional.

Respecto a las **medidas cautelares**, su solicitud podrá ser planteada en la misma instancia de la demanda principal o en otra separada o solicitarlas en la audiencia. Los órganos contenciosos electorales pueden adoptar las medidas cautelares cuando concurran los siguientes presupuestos:

1) Cuando se acredite de forma fehaciente la **verosimilitud del derecho** invocado por el peticionante de la medida cautelar;
2) Cuando se verifique un **perjuicio o daño inminente de difícil o imposible reparación** que impidiere o dificultare la efectividad de la tutela que pudiera otorgarse en la sentencia definitiva;
3) Cuando se verifique la **identidad** entre el objeto de la pretensión cautelar y la acción de fondo.

La decisión sobre las medidas cautelares dictada por las Juntas Electorales y las OCLEE puede ser apelada ante el Tribunal Superior Electoral en un plazo de cinco días.

El Tribunal Superior Electoral, como máximo órgano de la justicia electoral, tiene competencia para conocer de las impugnaciones contra los actos electorales o actos administrativos de contenido electoral dictadas por la Junta Central Electoral (arts. 118 y siguientes).

La impugnación se presentará por escrito en un plazo de 30 días a partir de la notificación del acto atacado, del día de su publicación oficial o cuando el agraviado haya tomado conocimiento del acto o la omisión de la Junta Central Electoral, siempre que la ley no disponga un plazo distinto.

Recibida la instancia, en un plazo no mayor de cuarenta y ocho horas se emplazará al interesado a una audiencia. La impugnación será decidida por el Tribunal Superior Electoral en un plazo de cinco días hábiles y su motivación ha de producirse en los cinco días subsiguientes.

5.2.3 Desarrollo reglamentario por parte de los organismos electorales

No nos consta la adopción de la JCE de disposiciones normativas específicas sobre la desinformación electoral.

6. ANTECEDENTES

6.1 Antecedentes sobre desórdenes informativos en procesos electorales

El riesgo ante desórdenes desinformativos es latente para la República Dominicana. Desde las elecciones internas de los partidos políticos del 2019, hasta las recientes elecciones municipales de febrero de 2024, se han identificado diversas narrativas desinformativas.

Dentro de los contenidos registrados para esta investigación, la narrativa más frecuente es de "Fraude" en el proceso electoral con 5 de 7 publicaciones vinculadas, detalladas en el siguiente recuadro:

NARRATIVA	FECHA	NOTA DESINFORMATIVA	NOTA/RESPUESTA OFICIAL
FRAUDE/ATAQUES EXTERNOS	7 DE OCTUBRE **2019**	https://www.europapress.es/internacional/noticia-leonel-fernandez-denuncia-fraude-primarias-republica-dominicana-20191007114906.html https://proceso.com.do/2019/10/06/leonel-fernandez-denuncia-fraude-y-se-declara-ganador-de-las-primarias-del-pld/	https://www.diariolibre.com/actualidad/jce-defiende-voto-automatizado-ante-las-denuncias-de-leonel-fernandez-EJ14593896
FRAUDE/ DENUNCIA EXPERIENCIA ELECTORAL	13 DE JULIO **2020**	IVÁN LORENZO DENUNCIA IRREGULARIDADES EN EL RECUENTO DE LOS VOTOS https://www.diariolibre.com/actualidad/politica/ivan-lorenzo-denuncia-irregularidades-en-el-recuento-de-los-votos-KD20106480	
REGLAS/ PROTOCOLO PARA VOTAR	28 DE DICIEMBRE **2023**	NO SE PUEDE VOTAR EN ROLOS O PANTALÓN CORTO https://x.com/josepeguero/status/1740338088486801530?s=20	https://x.com/DiarioLibre/status/1740504209806495850?s=20
PADRÓN ELECTORAL	17 DE FEBRERO **2024**	JUNTA TIENE OPERATIVO DE DECLARACIÓN TARDÍA> https://deultimominuto.net/jce-desmiente-informacion-circulada-a-traves-de-whatsapp/	
FRAUDE/ATAQUES A LA LEGITIMIDAD DEL ÓRGANO	15 DE FEBRERO **2024**	SUPUESTA ORQUESTACIÓN DE FRAUDE POR PARTE DE UN FUNCIONARIO DEL DNI https://www.youtube.com/watch?v=pNCsCUIb-es	Presidente de la JCE sobre hackeo del PLD: "Nadie ha hackeado nada" https://www.diariolibre.com/actualidad/politica/2024/01/31/la-respuesta-de-la-jce-a-la-denuncia-de-hackeo-del-pld/2593249

FRAUDE/ ATAQUES EXTERNOS	13 DE MARZO **2024**	JCE CENTRAL ELECTORAL SABÍA Y SABE LO QUE SUCEDIÓ EN FEBRERO https://www.youtube.com/watch?v=O_loFq9ZXxM https://www.elcaribe.com.do/panorama/politica/pgr-investiga-la-denuncia-de-supuesto-sabotaje-a-elecciones/	
FRAUDE/ DENUNCIA EXPERIENCIA ELECTORAL	18 DE FEBRERO **2024**	DENUNCIA COMPRA Y VENTA DE VOTOS CON FOTOGRAFÍAS COMO EVIDENCIAS EN ELECCIONES MUNICIPALES https://www.diariolibre.com/actualidad/politica/2024/02/18/elecciones-municipales-pc-denuncia-compra-de-votos-con-pruebas/2617749	

En las elecciones municipales, previas a las presidenciales, la desinformación estuvo presente, desde cómo se debía ir vestido o peinado al centro electoral, hasta las denuncias de compra de votos y fraude.

En el caso de la República Dominicana podemos decir que el grado de peligro de las declaraciones de fraude es bajo, ya que la confianza en el gobierno local está vinculada a factores socioeconómicos, políticos y sociales, como la aprobación presidencial, y tomando en cuenta los resultados electorales de las elecciones municipales de febrero, la abrumadora victoria del partido de gobierno está relacionada a la aprobación del ejecutivo.

6.2 Antecedentes sobre el organismo electoral. (miembros, valoración general, pacto ético, acuerdos con plataformas

- El pleno actual de la Junta Central Electoral (JCE) de la República Dominicana, fue elegido en noviembre de 2020, está compuesto por cinco miembros titulares y cuatro miembros suplentes. Este es el primer pleno escogido con perfiles variados no exclusivamente juristas. Fue seleccionado en un contexto de crisis de confianza tras la suspensión de las elecciones municipales de febrero de 2020 debido a fallos técnicos en el sistema de voto automatizado, lo que subrayó la necesidad de fortalecer la gestión tecnológica y la transparencia electoral.

Miembros Titulares del Pleno de la Junta Central Electoral:

1. **Román Jáquez Liranzo - Presidente**: Abogado, académico con amplia experiencia en justicia electoral. Fue presidente del Tribunal Superior Electoral (TSE) y ha liderado misiones de observación electoral internacional. Su enfoque está en la integridad y modernización del sistema electoral.
   Su elección como presidente fue vista como una oportunidad para restaurar la confianza en la JCE después de la crisis de 2020, dado su historial en la promoción de reformas judiciales y electorales.

2. **Rafael Armando Vallejo Santelises**: Abogado con una larga trayectoria en la práctica legal y en la dirección de organizaciones gremiales. Ha sido miembro de la JCE en el pasado, lo que le proporciona un conocimiento profundo del sistema electoral dominicano. Su experiencia fue un aval de continuidad al pleno, especialmente en un momento en que la JCE necesitaba reforzar su credibilidad.

3. **Samir Chami Isa**: Administrador público con experiencia en Gestión y Políticas Públicas. Ha ocupado cargos importantes en la administración pública, enfocados en la reforma y modernización de la justicia. Su inclusión fue considerada como

oportunidad debido a la necesidad de un enfoque administrativo sólido para mejorar la eficiencia y transparencia del proceso electoral.

4. **Dolores Fernández Sánchez**: Académica y experta en Derecho, con una carrera enfocada en la investigación y enseñanza del derecho. Su perfil técnico y académico fue valorado como una perspectiva de equilibrio en la toma de decisiones dentro de la JCE.

5. **Patricia Lorenzo Paniagua**: Ingeniera en Sistemas, primera persona no abogada en ser miembro de la JCE. Su experiencia en tecnología y sistemas ha sido crucial para abordar los desafíos de modernización y seguridad cibernética en los procesos electorales. Su elección respondió directamente a la necesidad de fortalecer la gestión tecnológica de la JCE, especialmente tras los problemas técnicos que afectaron las elecciones de 2020.

También, son parte del pleno 5 miembros adicionales en calidad de suplentes: **Vanahí Bello Dote**, Miembro Suplente del presidente; **Prado López Cornielle,** Miembro Suplente; **Freddy Ángel Castro Díaz,** Miembro Suplente: **Anibelca Rosario Rosario,** Miembro Suplente**; Hirayda Fernández Guzmán** Miembro Suplente

En la evolución del sistema electoral de la República Dominicana, el órgano electoral ha desempeñado un papel crucial en la adaptación y modernización de los procesos de votación. A lo largo de los años, se han implementado diversas modalidades de voto, cada una con implicaciones significativas para la transparencia y la confianza en el proceso electoral. La transición hacia el voto automatizado, las adaptaciones para el voto asistido, voto en casa y la inclusión piloto del voto penitenciario, novedades de los comicios del 2024, han sido aspectos fundamentales en la evolución del sistema electoral dominicano. Otro aspecto novedoso de la Junta Central Electoral, en específico sobre el pleno que preside esta gestión 2020-2024 es la inclusión de perfiles no jurídicos, para integrar una mirada transversal del funcionamiento del sistema electoral a la instancia de toma de decisión. Así pues, en esta ocasión está incluida la mirada administrativa pública y cibernética.

En un rol complementario como garante de la justicia electoral, el **Tribunal Superior Electoral (TSE)**, ha desempeñado un papel relevante para los avances del sistema electoral. Aunque este es un órgano de carácter autónomo con personalidad jurídica e independencia funcional, administrativa, presupuestaria y financiera de la Junta Central Electoral, el desarrollo de jurisprudencia ha sido clave para orientar y regular la conducta electoral en el país.

De conformidad con la Constitución dominicana, en su artículo 212, 213, 214, el TSE tiene a su cargo:

- Juzgar y decidir con carácter definitivo sobre los asuntos contenciosos electorales y estatuir sobre los diferendos que surjan a lo interno de los partidos, agrupaciones y movimientos políticos o entre estos.
- Dentro del período electoral, conocer de los recursos de apelación contra las decisiones adoptadas por las juntas electorales, así como de las impugnaciones y recusaciones de los miembros de estas.
- Ordenar la celebración de nuevas elecciones cuando hubieren sido anuladas, de conformidad con la ley.
- Conocer y decidir de los amparos electorales conforme a las reglas constitucionales y legales y sobre las rectificaciones de Actas del Estado Civil que tengan un carácter judicial.

El Tribunal está conformado por cinco jueces electorales, cada uno con su respectivo suplente, quienes son designados por el Consejo Nacional de la Magistratura (CNM). Este órgano es responsable, además, de la designación del presidente del Tribunal. Los jueces son nombrados por un período de cuatro años, con posibilidad de reelección.

Para el período de gestión 2021-2025, el Pleno del Tribunal Superior Electoral está compuesto por Ygnacio Pascual Camacho Hidalgo, quien ocupa el cargo de Juez Presidente, junto con los jueces titulares Hermenegilda del Rosario Fondeur Ramírez, Rosa Pérez de García, Pedro Pablo Permenos Forastieri y Fernando Fernández Cruz.

Adicionalmente, los suplentes que completan el pleno son Juan Cuevas, Hermenegilda del Rosario Fondeur Ramírez, Juan Manuel Garrido Campillo, Lourdes Teresa Salazar Rodríguez y Francisco Eugenio Cabrera Matos.

Sobre el voto Automatizado:

El voto automatizado fue **introducido en la República Dominicana en 2010,** con su primera implementación en las elecciones de diputados en el exterior (JCE, 2010). Posteriormente, en las elecciones generales de 2016, se amplió el uso de máquinas de votación a gran parte del territorio para las elecciones presidenciales y legislativas (JCE, 2016). Sin embargo, durante estos comicios, surgieron problemas técnicos significativos, incluyendo fallos en el software y hardware de las máquinas, lo que suscitó dudas sobre la eficacia del sistema automatizado (Oppenheimer, 2016).

La eliminación del voto automatizado facilitó la propagación de desinformación y teorías de conspiración. Los problemas técnicos durante las elecciones de 2016 y 2020 se convirtieron en el centro de rumores sobre manipulación y fraude electoral. La falta de transparencia en la gestión de estos problemas, junto con la insuficiencia de información clara sobre las medidas correctivas, contribuyó al vacío informativo, que fue ocupado por fuentes no confiables (Pérez, 2020).

La desinformación afectó la percepción pública sobre la legitimidad del sistema electoral, intensificando la desconfianza hacia la JCE y el proceso de votación. **La propagación de noticias falsas y especulaciones en un contexto de inestabilidad tecnológica y administrativa debilitó la confianza en la capacidad de la JCE** para manejar un proceso electoral transparente y justo (Pérez, 2020; García, 2020).

En el proceso electoral de 2024, objeto de esta Observación, la ausencia de voto automatizado se presenta como una medida para evitar los problemas técnicos y las controversias asociadas con las elecciones anteriores. La decisión de regresar al conteo manual de votos busca restaurar y fortalecer la confianza pública en el sistema electoral, reduciendo el impacto de la desinformación y las especulaciones (JCE, 2024).

Sobre el Voto Penitenciario:

El voto penitenciario en la República Dominicana ha habido un enfoque continuo en mejorar la accesibilidad y la administración del proceso. La Constitución y la legislación electoral dominicana reconocen el **derecho de los reclusos a participar en las elecciones, estableciendo mecanismos para permitir su voto en circunstancias controladas** (Ley No. 15-19, Código Electoral de la República Dominicana). Sin embargo, la implementación práctica de estas disposiciones ha enfrentado una serie de desafíos logísticos y administrativos.

En las elecciones de **2024**, la Misión electoral de la **OEA calificó como un "avance", el voto inclusivo en el sector carcelario, las mesas auxiliares para votantes con dificultades motrices y aumentar los colegios electorales** ubicados en el primer piso de los recintos electorales.

Sobre el voto asistido, voto en casa:

El voto en casa manual es una modalidad implementada **piloto**, por la Junta Central Electoral (JCE) de la República Dominicana para **permitir a los ciudadanos que no pueden desplazarse a un centro de votación, como personas con discapacidades graves, mayores de edad con movilidad reducida o enfermos, participar en el proceso electoral desde su hogar.**

Para acceder a este servicio, los interesados deben solicitarlo a la JCE con antelación, presentando la documentación necesaria para justificar su situación. Una vez aprobada la solicitud, la JCE organiza el envío de una comisión electoral, que incluye personal de la JCE y, en algunos casos, representantes de los partidos políticos, a la residencia del votante. Esta comisión lleva consigo la documentación electoral, como las papeletas y urnas, y asiste al votante en el proceso de emisión de su voto.

El voto en casa manual presenta varios desafíos, entre ellos la logística de organizar y coordinar las visitas a domicilio, asegurar la confidencialidad e integridad del voto, y garantizar que el proceso se lleve a cabo de manera transparente.

6.3 Antecedentes de decisiones jurisdiccionales vinculadas a desórdenes informativos

No se han identificado decisiones jurisprudenciales referidas específicamente a la desinformación u otros desórdenes o actividades realizadas en el entorno de las redes sociales que puedan poner en peligro la integridad electoral. No obstante, conviene tener presente la postura del Tribunal Constitucional de la República Dominicana sobre la libertad de expresión en contextos electorales cuando resolvió la acción directa de inconstitucionalidad contra los apartados 4 y 6 y el párrafo III del artículo 44 de la Ley 33-18 de partidos, Agrupaciones y Movimientos Políticos (Sentencias TC/0092/19 y TC/0441/19).

Dicha norma establecía, en relación con la propaganda en el período de precampaña o campaña interna, que quedaba prohibido:

[…]

4) Toda propaganda política que se fundamente, haga referencia o pueda percibirse de manera negativa, irrespetuosa o contraria a los principios, costumbres y valores culturales de la comunidad local, regional o nacional, en el orden religioso, racial, de preferencia sexual, o de cualquier otra naturaleza que contravenga las buenas costumbres.
6) La difusión de mensajes negativos a través de las redes sociales que empañen la imagen de los candidatos será sancionada conforme a los artículos 21 y 22 de la Ley No. 53-07, sobre Crímenes y Delitos de Alta Tecnología.
   Párrafo III: Las violaciones al presente artículo serán sancionadas con la retención de los fondos públicos que aporta el Estado a los partidos, agrupaciones y movimientos políticos conforme a la ley.

En la Sentencia TC/0092/19, de 21 de mayo de 2019, el Tribunal Constitucional declara no ser conforme a la Constitución (artículo 49) el apartado 6 del artículo 44 y en su argumentación señala:

> "gg. Las redes sociales se han convertido en los únicos espacios accesibles para que una masa significativa de ciudadanos y ciudadanas pueda exteriorizar su pensamiento, comunicarse, recibir e intercambiar opiniones e informaciones de manera global, instantánea y a un costo razonable respecto de los asuntos concernientes a todos y todas. El discurso público ha dejado de ser dirigido exclusivamente por el Estado o por los profesionales de la comunicación a través de los medios tradicionales, provocando una deliberación verdaderamente pública, plural y abierta sobre los asuntos de interés. De ahí *la importancia de que el uso de la libertad de expresión por estos medios se mantenga libre del temor a represalias innecesarias y desproporcionadas que obstaculicen la construcción de una ciudadanía plena, participativa y consciente*.
> hh. La protección del honor, reputación o imagen de un candidato a una función pública a través del derecho penal, que, en este caso concreto, corresponden a las penas de tres (3) meses a un (1) año de prisión y multa de cinco (5) a quinientas (500) veces el salario mínimo (…), *no compensa el sacrificio y peligro que supone para el ejercicio del derecho a la libertad de expresión de la ciudadanía*. Sobre todo, porque no se trata de aspectos concernientes a la vida privada e íntima de los mismos, ya que, en ese hipotético caso, como bien expresó el Tribunal Constitucional, en su precedente TC/0075/16 ya citado, corresponde otorgar la misma protección que a los particulares frente al uso abusivo de la libertad de expresión" (cursiva nuestra)

En la Sentencia TC/0441/19 el Tribunal declaró inconstitucional el apartado 4 y el párrafo II del artículo 44, por ser contrarios al artículo 49 de la Constitución. Señala el Tribunal Constitucional:

> "12.4.5. (…) para determinar si la opinión o el pensamiento difundido a través de estos medios masivos de comunicación se traduce en una afectación a los derechos fundamentales de cualquier persona –ya sea física o jurídica– que se considere afectada por el mismo, debe partirse de un margen de *razonabilidad objetiva* que permita separar las impresiones personales e interpretaciones que se puedan tener sobre tales publicaciones. Entonces, solo así es que podrían advertirse los límites a que se encuentra ceñido el ejercicio de este novedoso y creciente derecho"
>
> Y añade, " 12.4.8. (…) En este sentido, la percepción no se basa en supuestos objetivos, pues no son constitucionalmente válidas las prohibiciones relativas a la difusión del pensamiento al margen de las limitaciones que la propia Constitución y las demás normas del bloque de constitucionalidad establecen para preservar los derechos al honor o la reputación, a la intimidad, a la dignidad y a la moral de las personas, así como a la seguridad nacional, al orden público, a la salud y a la moral pública, ya que, fuera de esos casos, la expresión y difusión del pensamiento debe ser ejercida con libertad y sin censura previa" (cursiva nuestra).

En la misma sentencia se declara inconstitucional el párrafo III porque no respeta las exigencias de razonabilidad y personalidad de la pena.

De estos pronunciamientos cabe concluir que las limitaciones a la libertad de expresión, especialmente a través de las redes sociales, deben responder a una finalidad legítima que esté expresamente prevista en el ordenamiento constitucional. Además, debe basarse en

una razonabilidad objetiva y no en percepciones subjetivas. Las limitaciones y las sanciones por su incumplimiento deben ser adecuadas, necesarias y proporcionadas, de modo que el castigo penal debería ser excepcional. En todo caso, las sanciones deben quedar delimitadas taxativamente.

6.4 Antecedentes en materia de ciberseguridad

La República Dominicana ocupa la posición 66 en el ***Global Cybersecurity Index*** **de 2020**[4], con una puntuación de 75 sobre 100. Ello nos indica el estado de madurez del país en las distintas facetas que allí se miden. Una de las debilidades que apunta este índice es la relativa a las medidas legales. No obstante, se denota un trabajo en este sentido desde ese año hasta la actualidad, como podremos comprobar en este apartado del diagnóstico.

Dominican Republic



Development Level:
Developing Country, Small Island Developing States (SIDS)

Area(s) of Relative Strength
Organizational Measures
Area(s) of Potential Growth
Capacity Development Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
75.07	16.38	18.42	18.52	9.94	11.81

Source: ITU Global Cybersecurity Index v4, 2020

6.4.1 Estrategias nacionales de ciberseguridad de la República Dominicana

- Parte de la Estrategia interamericana integral para combatir las amenazas a la seguridad cibernética: un enfoque multidimensionales y multidisciplinario para la creación de una cultura de seguridad cibernética, de 2004[5].
- Estrategia nacional de ciberseguridad 2018-2021, Decreto 230-18[6].
- Estrategia nacional de ciberseguridad 2021-2030, Decreto 313-22[7].

Se aprueba con el objeto de fortalecer el marco nacional de ciberseguridad, fomentando la concientización y creación de entornos digitales seguros, confiables y resilientes, que

4 Global Cybersecurity Index de 2020 del ITU, disponible en: https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E/
5 Estrategia interamericana integral para combatir las amenazas a la seguridad cibernética: un enfoque multidimensionales y multidisciplinario para la creación de una cultura de seguridad cibernética, disponible en: https://www.oas.org/en/citel/infocitel/julio-04/ult-ciberseguridad_e.asp
6 Estrategia nacional de ciberseguridad 2018-2021, Decreto 230-18. Disponible en: https://cncs.gob.do/decreto-230-18/
7 Estrategia nacional de ciberseguridad 2021-2030, Decreto 313-22. Disponible en: https://cncs.gob.do/decreto-313-22/

promuevan una sociedad digital dentro de un esquema de inclusión y de respeto a los derechos fundamentales. La Estrategia Nacional de Ciberseguridad 2030 tiene como misión establecer los mecanismos adecuados de ciberseguridad que protejan al Estado, los sectores productivos y los ciudadanos, para garantizar un ecosistema de ciberseguridad favorable para el desarrollo nacional, y sobre un ciberespacio seguro, resiliente y confiable. Se estructura bajo los principios de: colaboración, prevención de actividades ilícitas, intercambio de información, protección de los derechos fundamentales y de las infraestructuras críticas, solicitud de asistencia, cadena de suministro y divulgación responsable de las vulnerabilidades.

- Decreto de notificación obligatorio de incidentes e intercambio de inteligencia de amenazas, Decreto 685-22[8].

Los ciberataques son el segundo factor de riesgo, situado inmediatamente después de los desastres naturales según datos del Foro Económico Mundial de 2022[9]. Para la consultora KPMG las amenazas cibernéticas forman parte de nuestro día a día y en el caso de Latinoamérica sólo el 19% de las instituciones cumplen con el 50% de los controles necesarios en ciberseguridad[10].

Latinoamérica ocupa el segundo lugar en cantidad de ciberataques por institución y es el tercero en crecimiento interanual a nivel global según el Informe Ciberataques a la logística y la infraestructura crítica en América Latina y el Caribe de Naciones Unidas y CEPAL de 2023 que recoge datos de Checkpoint de 2022[11]:

Cuadro 4
Cantidad de ataques semanales por región

Región	Ataques por semana	Cambio Interanual
ANZ	904	72%
América del Norte	849	47%
América Latina	1 572	32%
Europa	896	22%
Asia	1 778	21%
África	1 549	-6%

Fuente: Checkpoint, 2022.

En suma, los ataques se centran en las administraciones públicas: educación e investigación, gobierno y militar, salud, comunicaciones, como se muestra en el gráfico:

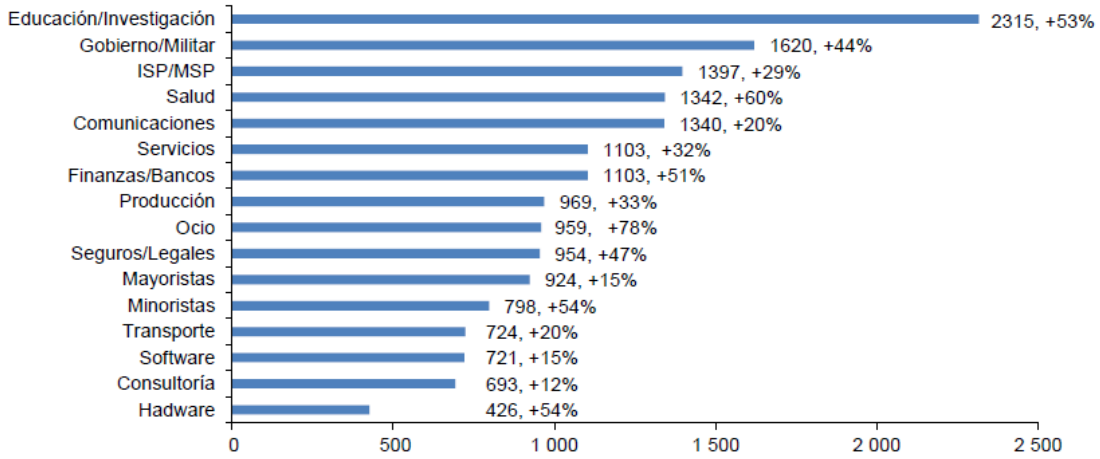
[8] Decreto de notificación obligatorio de incidentes e intercambio de inteligencia de amenazas, Decreto 685-22. Disponible en: https://cncs.gob.do/Decreto-685-22

9 Más información disponible en: https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf

10 KPMG. (2022), Una triple amenaza en las américas. Obtenido de https://home.kpmg/ar/es/home/insights/2022/01/kpmg-fraud-outlook-survey-spanish.html

11 Informe Ciberataques a la logística y la infraestructura crítica en América Latina y el Caribe de Naciones Unidas y CEPAL 2023, disponible en: https://www.cepal.org/es/publicaciones/49086-ciberataques-la-logistica-la-infraestructura-critica-america-latina-caribe

Grafico 6
Promedio semanal por organización por industria – global tercer trimestre 2022



Fuente: Checkpoint, 2022.

República Dominicana recibió en torno a 470 millones de intentos de ciberataques en el primer semestre de 2023. Los sectores más afectados fueron el financiero, el gubernamental y el de servicios, de acuerdo con el informe Panorama GLobl de Amenazas, de FortiGuard Labs de Fortinet. Es cierto que esta cifra es menor que en anualidades anteriores, debido a la inversión que se está haciendo en el país. Es importante señalar que FortiGuard Labs, Fortinet, sostiene que **hay menos cantidad de ataques, pero son diseñados para objetivos específicos, lo que los vuelve más sofisticados y con mayor posibilidad de éxito si las organizaciones no cuentan con defensas de ciberseguridad integradas, automatizadas y actualizadas.**

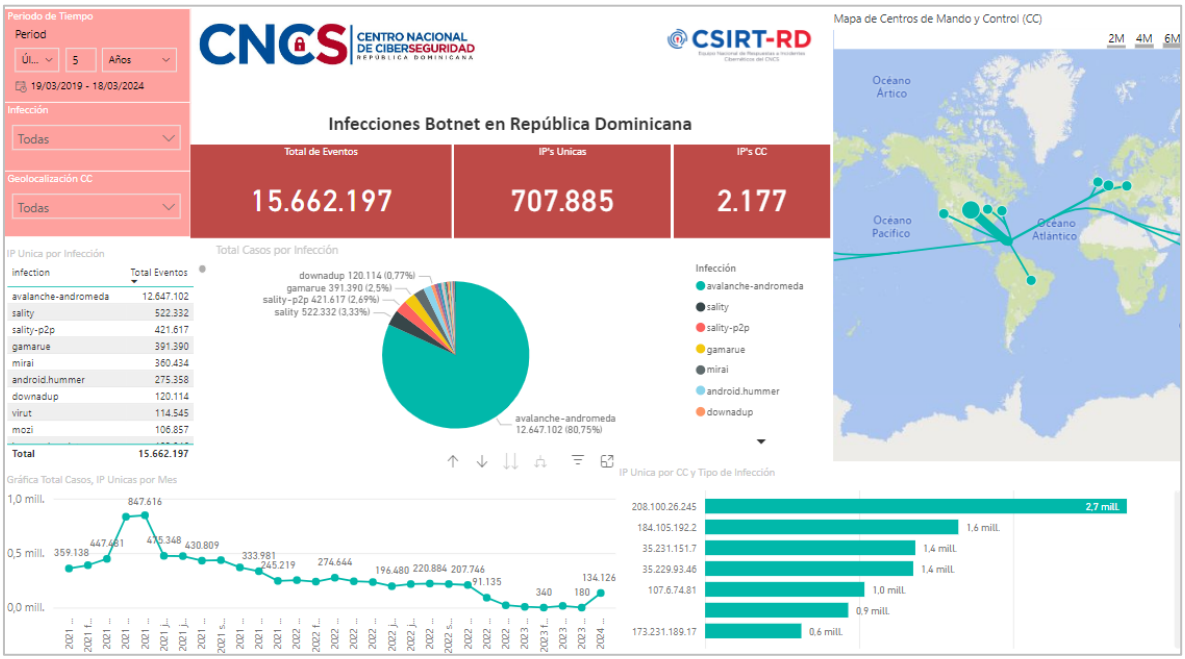
Además, los ciberataques en Latinoamérica crecieron un 24% durante el último año, que se tradujo en más de 728 millones de intentos de infección en la región –promedio de 35 ataques por segundo-. Si observamos los datos de los primeros ocho meses de 2022 frente a los primeros ocho meses de 2021, vemos que ha habido una explosión de ataques de phishing en toda la región. Guatemala es uno de los países con mayor crecimiento en esta amenaza (188%) y le siguen Perú (157%), República Dominicana (129%) y Colombia (127%), tal y como afirma uno de los responsables de Kasepersky[12].

Junto a estos datos el Informe Ciberataques a la logística y la infraestructura crítica en América Latina y el Caribe de Naciones Unidas y CEPAL de 2023[13] señala que entre 2020 y 2022 se han producido 82 incidentes en la región.

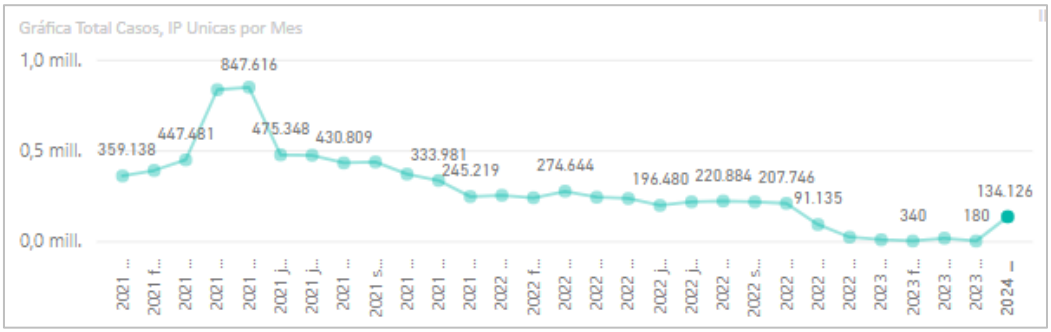
Una fotografía en modo evolutivo de la situación del Estado la encontramos en el observatorio de su CSIRT:

12 Mas información disponible en su web: https://latam.kaspersky.com/blog/panorama-amenazas-latam-2022/25509/

13 Informe Ciberataques a la logística y la infraestructura crítica en América Latina y el Caribe de Naciones Unidas y CEPAL 2023, disponible en: https://www.cepal.org/es/publicaciones/49086-ciberataques-la-logistica-la-infraestructura-critica-america-latina-caribe



Es importante prestar atención al pico de incidentes que se está empezando a dar en el año 2024, que se asemejan a los de 2022:



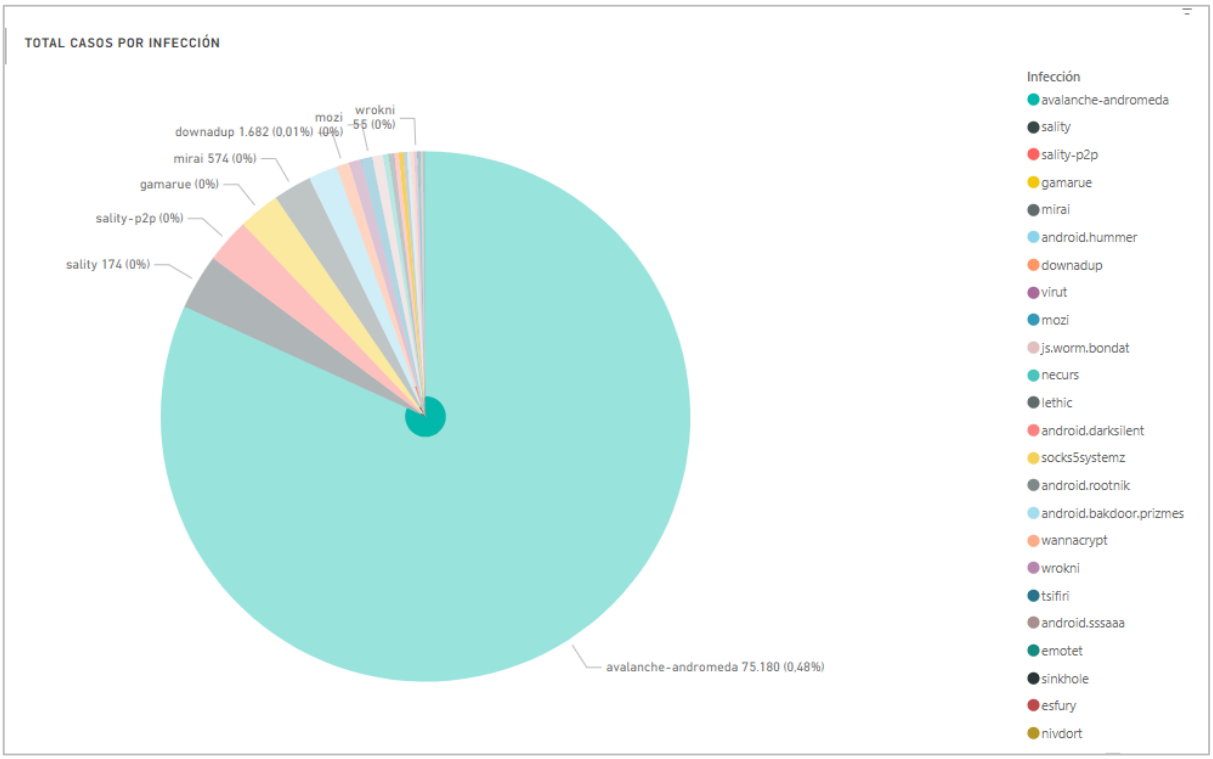
Centrándonos en el mes de enero de 2024, último del que se arrojan datos podemos observar los siguientes datos:

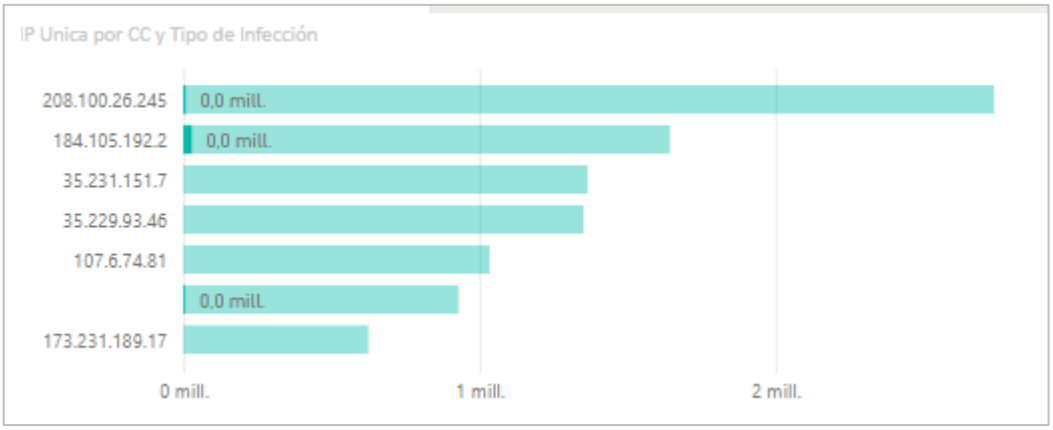
Infecciones Botnet en República Dominicana

Total de Eventos	IP's Unicas	IP's CC
134.126	707.885	368

Volver al informe | **IP UNICA POR INFECCIÓN**

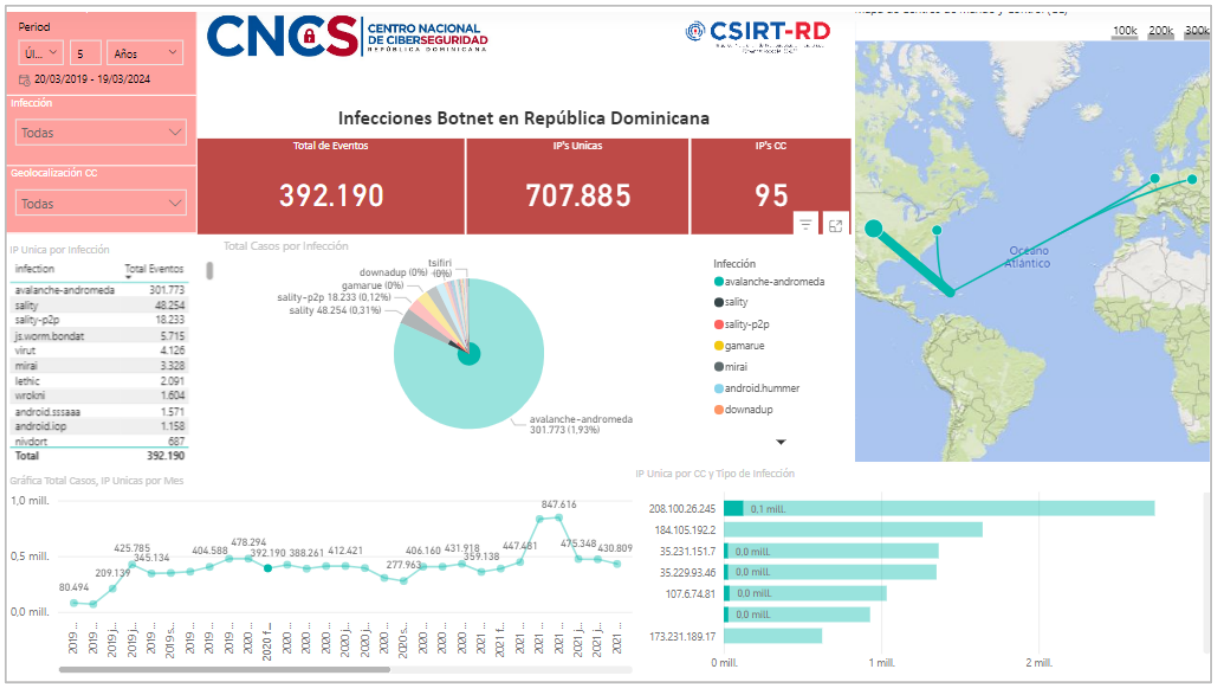
infection	Total Eventos
avalanche-andromeda	75.180
socks5systemz	39.900
adload	9.381
pseudomanuscrypt	3.603
downadup	1.682
vipersoftx	609
android.hummer	599
mirai	574
js.worm.bondat	522
necurs	262
sinkhole	215
sality	174
android.bakdoor.prizmes	157
tsifiri	128
cutwail	120
m0yv	110
expiro	92
qsnatch	82
avalanche-matsnu	79
sharkbot	73
trickbot-fallback-c2	68
avalanche-ranbyus	65
wrokni	55
avalanche-nymaim	48
likely-rat-warzone	38
android.rootnik	35
suppobox	35
flubot	32
nivdort	31
likely-rat-adwind	29
Total	**134.126**

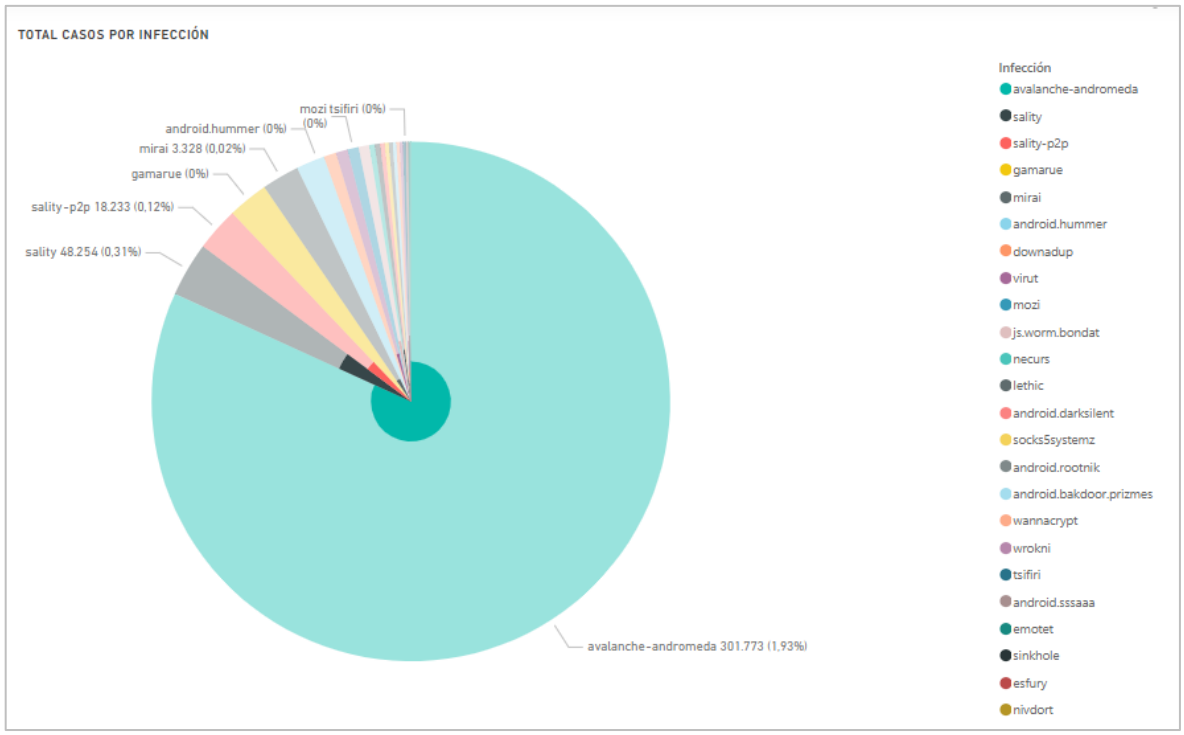

TOTAL CASOS POR INFECCIÓN
downadup 1.682 (0,01%)
mozi (0%)
wrokni 55 (0%)
mirai 574 (0%)
gamarue (0%)
sality-p2p (0%)
sality 174 (0%)
avalanche-andromeda 75.180 (0,48%)
Infección
avalanche-andromeda
sality
sality-p2p
gamarue
mirai
android.hummer
downadup
virut
mozi
js.worm.bondat
necurs
lethic
android.darksilent
socks5systemz
android.rootnik
android.bakdoor.prizmes
wannacrypt
wrokni
tsifiri
android.sssaaa
emotet
sinkhole
esfury
nivdort


IP Unica por CC y Tipo de Infección
208.100.26.245
184.105.192.2
35.231.151.7
35.229.93.46
107.6.74.81
173.231.189.17
0,0 mill.
0,0 mill.
0,0 mill.
0 mill.
1 mill.
2 mill.



La situación previamente descrita para 2024 podemos compararla con la sufrida en febrero del año 2020, en el momento electoral, donde podemos observar una diferencia de 258,064 más de infecciones de botnet en 2020.


Period
Últ... 5 Años
20/03/2019 - 19/03/2024
Infección
Todas
Geolocalización CC
Todas
CNCS CENTRO NACIONAL DE CIBERSEGURIDAD REPÚBLICA DOMINICANA
CSIRT-RD
Infecciones Botnet en República Dominicana
Total de Eventos
392.190
IP's Unicas
707.885
IP's CC
95
IP Unica por Infección
infection Total Eventos
avalanche-andromeda 301.773
sality 48.254
sality-p2p 18.233
js.worm.bondat 5.715
virut 4.126
mirai 3.328
lethic 2.091
wrokni 1.604
android.sssaaa 1.571
android.iop 1.158
nivdort 687
Total 392.190
Total Casos por Infección
tsifiri (0%)
downadup (0%)
gamarue (0%)
sality-p2p 18.233 (0,12%)
sality 48.254 (0,31%)
avalanche-andromeda 301.773 (1,93%)
Infección
avalanche-andromeda
sality
sality-p2p
gamarue
mirai
android.hummer
downadup
100k 200k 300k
Océano Atlántico
Gráfica Total Casos, IP Unicas por Mes
1,0 mill.
0,5 mill.
0,0 mill.
80.494
209.139
425.785
345.134
404.588
478.294
392.190
388.261
412.421
277.963
406.160
431.918
359.138
447.481
847.616
475.348
430.809
IP Unica por CC y Tipo de Infección
208.100.26.245 0.1 mill.
184.105.192.2
35.231.151.7 0.0 mill.
35.229.93.46 0.0 mill.
107.6.74.81 0.0 mill.
173.231.189.17
0 mill.
1 mill.
2 mill.


TOTAL CASOS POR INFECCIÓN
mozi tsifiri (0%) (0%)
android.hummer (0%)
mirai 3.328 (0,02%)
gamarue (0%)
sality-p2p 18.233 (0,12%)
sality 48.254 (0,31%)
avalanche-andromeda 301.773 (1,93%)
Infección
avalanche-andromeda
sality
sality-p2p
gamarue
mirai
android.hummer
downadup
virut
mozi
js.worm.bondat
necurs
lethic
android.darksilent
socks5systemz
android.rootnik
android.bakdoor.prizmes
wannacrypt
wrokni
tsifiri
android.sssaaa
emotet
sinkhole
esfury
nivdort

6.4.2 Ciberataques sufridos en República Dominicana

En el Informe Ciberataques a la logística y la infraestructura crítica en América Latina y el Caribe de Naciones Unidas y CEPAL 2023[14] se recogen algunos de los incidentes más relevantes acaecidos en la región, siendo aquí mostrados los relativos a República Dominicana:

A. Eventos destacados en logística e infraestructuras críticas

A través de la investigación de escritorio realizada, se ha podido documentar un total de 82 incidentes que afectaron a los diez países investigados en el presente informe y que se detallan en el cuadro 1. En el se visualiza los siguientes datos estadísticos ocurridos entre 2020 y 2022.

Cuadro 1
Cantidad de incidentes encontrados por país

País	Cantidad	Porcentaje
Brasil	27	19
Colombia	20	14
Argentina	19	13
Chile	16	11
México	15	10
Perú	11	8
Uruguay	11	8
Ecuador	10	7
República Dominicana	8	6
Panamá	7	5

Fuente: Elaboración propia.

14 Informe Ciberataques a la logística y la infraestructura crítica en América Latina y el Caribe de Naciones Unidas y CEPAL 2023, disponible en: https://www.cepal.org/es/publicaciones/49086-ciberataques-la-logistica-la-infraestructura-critica-america-latina-caribe

Tipo de actividad	Argentina	Brasil	Chile	Colombia	Ecuador	México	Panamá	Perú	Rep. Dominicana	Uruguay	Organización afectada	Descripción de la actividad	Impacto D	Impacto C	Impacto I	Tipo de incidente	Fecha de referencia del incidente	Descripción del incidente	Impacto Cualitativo	Impacto Cuantitativo	Días impacto	Costo en dólares	Resolución	Fuente
Logística							X				Aeropost, Inc.	Empresa de comercio electrónico y logística que opera el sitio web Aeropost.com		X		Violación de datos de los clientes	24/4/2022	La empresa confirmó que hubo una brecha de datos de corta duración en la plataforma tecnológica operada por Aeropost, lo que resultó en que algunas tarjetas de crédito de los clientes se vieran comprometidas	Evidencia de fallos en los niveles de seguridad de datos y de la *tokenización* de todas las tarjetas	Indeterminado por las características del ataque			La empresa comunica a sus clientes que cancele las operaciones realizadas a través de las respectivas entidades emisoras	https://www.jdsupra.com/legalnews/aeropost-com-asks-customers-to-delete-4835917/
Estado								X			Ministerio de Transportes y Comunicaciones	Organo que busca lograr un racional ordenamiento territorial vinculado a las áreas de recursos, producción y mercados		X	X	Secuestro de la cuenta de Twitter	29/3/2022	La cuenta de Twitter del Ministerio ha sido secuestrada y rebautizada como MTC.ETH	Se presume que pudo haber quedado expuesta información personal de ciudadanos que, por una gestión, pudieron compartir números de documentos y teléfonos	La cuenta tiene aproximadamente 260 mil seguidores	1		No informado	https://rpp.pe/tecnologia/redes-sociales/twitter-cuenta-secuestrada-del-mtc-luce-un-bored-ape-como-avatar-noticia-1396019
Estado								X			Dirección General de Inteligencia del Ministerio del Interior-Digimin	La Dirección General de Inteligencia del Ministerio del Interior DIGIMIN coordina y centraliza la inteligencia relacionada al orden interno, seguridad pública, seguridad ciudadana, crimen organizado y nuevas amenazas transnacionales, que produce la Dirección de Inteligencia de la Policía Nacional	X	X		Ransomware-grupo Conti-Secuestro de información sensible	28/4/2022	El atacante asegura haber penetrado en los servidores de la Digimin y secuestrados documentos secretos de una oficina que es estratégica para la seguridad nacional. Exigen dinero al Estado peruano a cambio de no publicar la información	Información altamente sensible del organismo	No se publicó el volumen de los datos afectados			No informado	https://sudaca.pe/noticia/informes/hackers-rusos-en-los-servidores-de-inteligencia-del-mininter/
Estado									X		Contraloría General de la República Dominicana	Organo Rector del Sistema Nacional de Control Interno de la República Dominicana	X			Defacement-Bloqueo de la página Web	6/2/2022	Un supuesto grupo paquistaní hackeó la mañana de este domingo la página virtual de la Contraloría General de la República Dominicana, por lo que las personas no pueden acceder a la misma ni visualizar nada de la institución	Bloqueo total del acceso a la información	No se ha informado el volumen de los datos afectados			No informado	https://encontexto.com.do/hackean-pagina-de-la-contraloria-general-de-la-republica-dominicana/
Estado									X		Consejo Estatal del Azúcar	Organismo que administra los ingenios y la producción de azúcar en la República Dominicana bajo la Dirección General de Bienes Nacionales	X			Defacement - Bloqueo de la página Web	6/2/2022	Desconfiguración de la estructura web	Bloqueo total del acceso a la información	No se ha informado el volumen de los datos afectados			No informado	https://www.gadgetdominicana.com/2022/02/14-sitios-web-del-estado-dominicano-hackeados-estn-en-peligro-los-datos-de-los-ciudadanos/
										X	Usuarios	La propia de	X	X	X	Ransomware-	1/12/2020	Es parte de una estafa en línea	Intenta convencer a	Variable según			No aplica	https://www.enigmas

Tipo de actividad	Argentina	Brasil	Chile	Colombia	Ecuador	México	Panamá	Perú	Rep. Dominicana	Uruguay	Organización afectada	Descripción de la actividad	Impacto D	Impacto C	Impacto I	Tipo de incidente	Fecha de referencia del incidente	Descripción del incidente	Impacto Cualitativo	Impacto Cuantitativo	Días impacto	Costo en dólares	Resolución	Fuente
Tecnología			X			X					SolarWinds Corporation	Empresa estadounidense que desarrolla software para ayudar a las empresas a administrar sus redes, sistemas e infraestructura de tecnología de la información		X		Filtración de datos (puerta trasera)-Sunburst	13/12/2020	El ciberataque infectó a las actualizaciones de su software de monitoreo de redes Orion	SolarWinds solicitó, ese mismo día, a sus clientes actualizar Orion inmediatamente a su versión 2020. 2.1 HF 1	Se estima que fueron afectadas aproximadamente 18.000 empresas en todo el mundo	4		Aplicar una nueva actualización de emergencia, la que reemplazará el componente comprometido y agregará nuevas funcionalidades de seguridad	https://www.csirt.gob.cl/media/2020/12/10CND20-00045-01.pdf
Tecnología	X					X					Kaseya Limited	Servicios de TI	X	X		Ransomware-Revil	2/7/2021	Ataque contra el servicio VSA (software de gestión de IT) el ataque se llevó a cabo mediante la explotación de una vulnerabilidad zero-day (CVE-2021-30116)	Cerraron los servidores SaaS y notificaron el problema a los clientes para que apagaran los servidores VSA	Se estima que fueron afectadas aproximadamente 1500 empresas	4		La empresa desarrolló un parche de solución	https://www.xataka.com/seguridad/kaseya-su-espeluznante-ataque-ransomware-esto-todo-que-sabemos-momento
Tecnología				X				X			Securitas	Firma de vigilancia, seguridad y gestión de riesgos corporativos		X	X	Filtración de información reservada	31/1/2022	Uno de los tres buckets Amazon Simple Storage Service (AS3) de la firma estaba completamente expuesto en línea	La información expuesta incluye identificación personal de los empleados y detalles de las instalaciones de al menos cuatro aeropuertos	Filtración de más de 1 millón de archivos confidenciales, equivalentes a 3TB			No informado	https://noticiasseguridad.com/hacking-incidentes/filtran-informacion-personal-y-fotos-de-los-empleados-en-aeropuertos-de-colombia-y-peru/
Tecnología		X		X	X						Operadores de telecomunicaciones	Persona física o jurídica que explota redes públicas de telecomunicaciones o presta servicios de telecomunicaciones disponibles al público		X	X	Ransomware-LightBasin	Año 2021	El tráfico del malware emuló los servidores que manejan las conexiones GPRS, lo que le permitió enviar y recibir datos entre los sistemas infectados y los servidores de comando y control sin alertar al firewall	El procedimiento de los ataques fue el mismo: captura de la base de datos, un DDoS y pedido de rescate que debe ser depositado en billeteras virtuales	En octubre de 2021 fue anunciado, que las redes de 13 operadores globales de telefonía móvil fueron infiltradas	120	5000000	No informada	https://enperspectiva.uy/enperspectiva-netgente-y-empresas/empresas-de-telecomunicaciones-recibieron-un-tercio-de-los-ata ques-ciberneticos-perpetrados-en-2021/
Tecnología		X		X	X						Por las características del ataque afectó a distintas entidades bancarias	Bancos comerciales y de servicios financieros		X	X	Troyano bancario-Qbot	8/1/2021	Distribución por correo electrónico del malware Qbot, con la finalidad de robar datos sensibles de las redes empresariales infectadas	No fue difundido por los distintos usuarios afectados	1.500 usuarios afectados en distintos países	90		El 22 de marzo, Microsoft anunció que en el 92% de los servidores in situ de Microsoft Exchange, los efectos del hackeo habían sido corregidos o mitigados	https://portalinnova.cl/nueva-ola-de-correos-maliciosos-propaga-el-malware-qbot-advierte-kaspersky/
Logística						X		X	X		Expeditors International	Empresa estadounidense de logística y transporte de carga con filiales en distintos países del mundo. Sus servicios incluyen la cadena de suministro, el almacenamiento y la distribución, el transporte, las aduanas y el cumplimiento		X	X	Ransomware	20/2/2022	La compañía de logística y transporte de mercancías debió cerrar la mayor parte de sus operaciones en todo el mundo para mantener "la seguridad de su entorno global de sistemas"	Los impactos en curso del ciberataque tuvieron un efecto material adverso en su negocio, ingresos, gastos, resultados de las operaciones, flujos de efectivo y reputación. En un principio, la empresa no puede estimar las repercusiones financieras directas e indirectas definitivas de este ciberataque	La empresa tiene 350 sucursales y más de 18.000 empleados en todo el mundo			Se aplicaron soluciones de contingencia de acuerdo a cada filial y disponibilidad de recursos	https://www.baenegocios.com/negocios/Un-ciberataque-obligo-a-un-gigante-logistico-a-cerrar-sus-operaciones-mundiales-20220221-0120.html

Tipo de actividad	Argentina	Brasil	Chile	Colombia	Ecuador	México	Panamá	Perú	Rep. Dominicana	Uruguay	Organización afectada	Descripción de la actividad	Impacto D	Impacto C	Impacto I	Tipo de incidente	Fecha de referencia del incidente	Descripción del incidente	Impacto Cualitativo	Impacto Cuantitativo	Impacto Días Impacto	Impacto Costo en dólares	Resolución	Fuente
Energía		X	X	X							Empresas petroleras y mineras	Empresas de extracción y refinado		X	X	Filtración de correos electrónicos y publicación de la información en la plataforma web DDo Secrets.com	3/8/2022	La información proviene de correos electrónicos de firmas de Colombia, Brasil y Chile. De la que se recabó mayor cantidad de datos fue de la empresa minera chilena Quiborax. Revelaron casos de derrames y denuncias de corrupción	Las distintas empresas fueron afectadas de diversas formas, según su materia específica de actividad	Se difundió más de 1TB de información			No informada	https://www.rionegro.com.ar/energia/hackers-filtraron-mas-de-1tb-de-informacion-sobre-petroleras-y-mineras-de-latinoamerica-2427530/
Comercio	X		X	X				X			Cencosud-Supermercados: Easy, Jumbo, Vea y Blainstein	Cadenas de supermercados de venta minorista	X	X		Ransomware-Egregor	17/11/2020	El ataque secuestró las bases de datos con la información de los clientes de las empresas, las que fueron usadas para la extorsión del atacante	Durante la operación ordinaria diaria, las máquinas registradoras imprimieron tickets sin freno con un mensaje en inglés: "Si no pagan, publicaremos toda la información de sus clientes". Preventivamente la empresa cerró sus locales por algunas horas y puso en standby sus sitios web	Inactividad total con el consecuente lucro cesante	1		Se presume que la empresa pagó el rescate pedido	https://www.memo.com.ar/economia/que-hubo-detras-del-ciberataque-a-easy-jumbo-y-vea-en-argentina/
Estado			X	X		X		X			Fuerzas armadas	Defensa militar		X		Fuerza bruta	30/9/2022	Robo de información reservada, principalmente de correo electrónico a través de una brecha de seguridad del servicio Exchange	No informado, debido a la confidencialidad de la información relacionada con la seguridad de cada país	No informado, debido a la confidencialidad de la información relacionada con la seguridad de cada país	No informado debido a la confidencialidad de la información relacionada con la seguridad de cada país		No informado, debido a la confidencialidad de la información relacionada con la seguridad de cada país	https://www.bbc.com/mundo/noticias-america-latina-63167331
Logística	X	X	X		X	X	X	X	X	X	Hellmann Worldwide Logistics	Hellmann Worldwide Logistics SE & Co. KG es una empresa alemana de servicios logísticos con sede en Osnabrück, Alemania. Con sucursales en 56 países	X	X		Ransomware-filtración de datos	9/12/2022	Ataque Ransomware y filtración de datos, esta se produjo con anterioridad al secuestro de datos, como primera parte del plan de ataque	Como consecuencia de este ataque ransomware, los clientes de Hellmann están experimentando llamadas y correos electrónicos fraudulentos, según indica la propia compañía en su web. Esta puede ser una de las consecuencias derivadas del ataque. Ya que, si los atacantes no monetizan el incidente a través del cobro del secuestro de datos, lo hacen a través de los datos obtenidos, mediante estafa	Fueron afectados 70.64 GB de datos comprimidos. Estos archivos contienen información como los nombres de clientes, el ID de usuario, correos electrónicos y contraseñas	No especificados, se estima que varias semanas		Se aplicaron soluciones de contingencia de acuerdo con el cada filial y disponibilidad de recursos	https://unaaldia.hispasec.com/2021/12/lata que-ransomware-y-filtracion-de-datos-de-hellmann.html

Tipo de actividad	Argentina	Brasil	Chile	Colombia	Ecuador	México	Panamá	Perú	Rep. Dominicana	Uruguay	Organización afectada	Descripción de la actividad	Impacto D	Impacto C	Impacto I	Tipo de incidente	Fecha de referencia del incidente	Descripción del incidente	Impacto Cualitativo	Impacto Cuantitativo	Impacto Días Impacto	Impacto Costo en dólares	Resolución	Fuente
Tecnología	X	X	X	X	X	X	X	X	X	X	Por las características del ataque afectó a cualquier tipo de organizaciones	Por las características del ataque afectó a cualquier tipo de actividad		X		Acceso a cuentas y contraseñas de servidores de correo Microsoft	8/1/2021	Filtración de datos en sus servidores in situ de Microsoft Exchange Server	Los atacantes obtuvieron privilegios de administrador en los servidores afectados, acceso a los correos electrónicos y contraseñas de los usuarios y también a los dispositivos conectados a la misma red	250.000 servidores en todo el mundo	90		El 22 de marzo, Microsoft anunció que en el 92% de los servidores in situ de Microsoft Exchange, los efectos del hackeo habían sido corregidos o mitigados	https://blog.malfence.com/es/analisis-del-hackeo-a-microsoft-exchange-server/
Tecnología	X	X	X	X	X	X	X	X	X	X	Usuarios de Facebook	Utilidades de la aplicación		X	X	Robo y publicación de datos de usuarios de la aplicación	1/3/2021	El ataque dejó expuesta la información personal de millones de usuarios que ha sido publicada en un foro de piratería. Se trata de los correos electrónicos, teléfonos, fechas de nacimiento, biografías, ubicaciones, estado sentimental y biografía	Exposición de información privada	533.000.000 de usuarios afectados	Dadas las características de los datos expuestos a afectación producida por el ataque perduró en el tiempo, sin poder determinar su duración		No informado	https://www.channelpartner.es/seguridad/noticias/11298590025 02/siete-ciberataques-han-marcado-ano-2021.1.html
Finanzas	X	X	X	X	X	X	X	X	X	X	Bancos comerciales/ clientes	Organizaciones cuya actividad económica es la intermediación financiera. Es decir, capta depósitos del público, dirigiendo esos recursos al otorgamiento de créditos, con el objetivo de obtener un beneficio		X	X	Phishing-ingeniería social	19/3/2022	Los clientes de los bancos son víctimas, de ingeniería social como phishing. Estos ciberataques se realizan a través de los correos electrónicos de los usuarios financieros, con el objeto de tratar de capturar o robar información confidencial de los clientes, tales como sus usuarios y contraseñas, números de tarjetas de créditos, entre otras informaciones, para que la víctima voluntariamente revele dichas informaciones mediante técnicas de manipulación y el engaño	Estos crímenes han conllevado, a que los bancos tengan que invertir importantes recursos en realizar campañas de concientización para advertir y educar a los clientes. Asimismo, los bancos deben invertir en programas y herramientas robustas de ciberseguridad para protegerse ante los diferentes ataques cibernéticos	Variable según las víctimas afectadas			La implementada por cada entidad	https://www.diariolibre.com/actualidad/nacional/2022/03/19/victimas-de-fraudes-bancarios-son-por-robo-de-identidad/1716145
Comercio	X	X	X	X	X	X	X	X	X	X	Pequeñas y medianas empresas y comercios	Actividades varias	X	X	X	Troyano_PGW - ataques de internet-ataques al Protocolo de Escritorio Remoto	Periodo años 2021-2022	De acuerdo con el tipo de ataque en cada caso	De acuerdo con el tipo de ataque en cada caso	De acuerdo con el tipo de ataque en cada caso		155 000	De acuerdo con el tipo de ataque en cada caso	https://latam.kaspersky.com/blog/pymes-latam-enfrentan-creciente-numero-ciberataques/24950

6.4.3 Algunas medidas generales aplicables al contexto electoral que se están aplicando y/o se prevén en los distintos documentos:

Plan Estratégico Institucional 2020-2024. Junta Central Electoral

- Profesionalización y actualización de los colaboradores internos de la JCE. Adiestrar y capacitar al personal de la JCE en sus respectivas funciones y responsabilidades.
- Capacitación del personal relativa al manejo y presencia de redes sociales. El tema de las redes sociales no deja de ser un gran desafío, el rol que juegan, con poca regulación, y sobre todo lo que tiene que ver con las noticias falsas y campañas negativas, publicidad engañosa y la propaganda perversa que sobre el proceso electoral y los órganos electorales se ponen en marcha en los distintos medios que forman parte de las redes sociales.
- Especificación del organigrama según roles y funciones. Organizar a nivel interno la institución en términos de organigrama, para dignificar a los servidores, según su capacidad y competencia.
- Vinculación con los sectores externos (CSIRTs, partidos, etc.).

Objetivos estratégicos:

1. Fortalecimiento de la gestión y dirección institucional

   1.1. **Optimizar la infraestructura** de la institución.
   1.2. Implementar un **modelo de gestión de calidad.**
   1.3. **Fortalecer la confianza** de nuestros usuarios.
   1.4. **Gestionar efectivamente la estructura organizacional** y todos los procesos de **recursos humanos**.
   1.5. Desarrollar una **política** efectiva y dinámica de **comunicación y coordinación interna**.
   1.6. **Propiciar el uso de las herramientas tecnológicas como eje transversal.**
      1.6.1. **Obtener la certificación del Data Center**. Producto: Data Center debidamente certificado en TIER-3.
      1.6.2. **Diseñar plan de recuperación ante desastres.** Producto: Plan de recuperación de desastre debidamente formulado y documentado, aprobado por el Pleno.
      1.6.3. **Actualizar las redes de telecomunicaciones**. Producto: Contar con un sistema de redes actualizadas y que dispongan de los recursos tecnológicos de última generación. [TA1]
      1.6.4. **Instalar centro de monitoreo.** Producto: Centro de monitoreo del Data Center funcionando y operando de manera permanente y ofreciendo los reportes correspondientes.
      1.6.5. **Realizar levantamiento de workflows para la automatización de los componentes de los procesos que establezca un orden y una jerarquización.** Producto: Procesos del nivel tecnológico integrados entre sí disponibles en las distintas áreas de trabajo que se hayan contemplado en el alcance.

2. **Consolidar la modernización del Registro Civil y garantizar la identidad ciudadana:** disponer de una base de datos documental que facilite el acceso a los actos registrales de las personas, con un servicio más rápido y eficiente. Esto, a su vez, se traducirá en que los datos contenidos en el documento de identidad de los ciudadanos serán más fiables, y contarán con el debido respaldo del Registro Civil.

2.1. **Actualizar y depurar los registros de los Actos del Estado Civil.**
  2.1.1. **Completar el proceso de digitalización de los actos del Estado Civil.** Productos: Libros escaneados e indexados. Libros digitales impresos.
2.2. Mejorar de manera continua los **registros oportunos de nacimiento y defunciones**.
2.3. Establecer la **integración de la cedulación con el registro civil.**
  2.3.1. **Unificar las bases de datos del Registro Civil y Cedulación**. Producto: Disponer de una base de datos de cedulación unificada con los Actos del Registro Civil que permita la interacción entre ambos sistemas y elimine el requerimiento de documentos expedidos por las propias Oficialías del Estado Civil.
2.4. **Implementar la identidad digital.**
  2.4.1. **Definir el tipo de identidad digital a implementar**. Producto: Modelo de implementación de la identidad digital definida.
  2.4.2. **Implementar plan piloto de la identidad digital.** Producto: Componentes de la identidad digital definidos e implementados con lo cual se facilitará a los ciudadanos la obtención de servicios públicos y privados.
2.5. **Innovar y mejorar continuamente los servicios al público.** [TA2]
  2.5.1. **Proveer de plataformas alternativas a la ciudadanía para la obtención de los servicios.** Producto: Plataformas de comunicación alternativos (Call Center, Internet, minimensajes, correo) disponibles y puestos en funcionamiento.
  2.5.2. **Crear unidad de seguimiento de la calidad de los servicios**. Producto: Unidad de monitoreo y mejoras continúas instaladas y en funcionamiento operacional, de la cual se recibirán reportes permanentes para la aplicación de mejoras en los servicios.

3. **Procesos electorales eficientes, confiables y transparentes:** actualización de los procedimientos y la implementación de mejoras a los subprocesos existentes, incorporando nuevas propuestas para el mejoramiento de las estructuras electorales operacionales, así como otros mecanismos que generen la confianza de los distintos actores externos en los procesos electorales, actuando con eficiencia y transparencia para ofrecer resultados creíbles. Mejora el acceso a personas con discapacidad.

3.1. Investigar y dar seguimiento a las **infracciones electorales-administrativas**.
3.2. **Fortalecer la organización del voto en el exterior.**
3.3. Facilitar **la accesibilidad al ejercicio del voto** de personas con discapacidad, adultos mayores e internos en recintos penitenciarios.
  3.3.1. **Facilitar el ejercicio del sufragio de personas que por condiciones especiales de salud no pueden trasladarse a los centros de votación.** Producto: Reimplementado el proyecto piloto del “voto en casa”.
3.4. **Fortalecer las Juntas y Colegios Electorales.**
3.5. Impulsar **acciones para mejorar la gestión y organización electoral**.
  3.5.1. **Readecuación y fortalecimiento del programa educativo electoral a los funcionarios de los colegios electorales.** Producto: Un programa de capacitación electoral actualizado, adecuado y con disponibilidad de herramientas tecnológicas para los funcionarios que intervienen en el proceso electoral.
  3.5.2. **Modernizar los procesos de la logística electoral.** Producto: Contar con procesos de logística electoral estandarizados, documentados y automatizados.

4. **Contribución al fortalecimiento institucional de las organizaciones políticas:** Promover el fortalecimiento del sistema de partidos, **cooperando** con los mismos.

   4.1. Apoyar el **desarrollo de capacidades y habilidades** para la gerencia interna de las organizaciones políticas.
   4.2. **Promover la formación en buenas prácticas** de la militancia partidaria.

5. **Confianza institucional y sociedad participativa:** Propiciar una relación de confianza con la ciudadanía respecto a los procesos electorales.

   5.1. **Aumentar la confianza de la sociedad** en los procesos electorales.
   5.2. **Difundir las informaciones** de manera oportuna y transparente.

Medidas generales derivadas de la Estrategia de Ciberseguridad vigente

De la Estrategia de Ciberseguridad vigente es reseñable destacar algunos de los objetivos estratégicos en que se trabaja a nivel general con el CSIRT del Estado, por cuanto va a tener un impacto en la Junta Central Electoral:

1. **Objetivo estratégico de fortalecimiento de la capacidad institucional: se trata de fortalecer las capacidades de las entidades y organismos especializados de apoyo, para mejorar la prevención, detección, respuesta y recuperación en materia de ciberseguridad. Asimismo, contribuir al fortalecimiento de las instituciones del Estado, en todo el contexto de la ciberseguridad. Para lo cual se han determinado distintos objetivos específicos con unas líneas de actuación concretas:**

   1.1. Objetivo específico de **fortalecimiento integral de las entidades y organismos especializados de apoyo en el ámbito de la gestión y seguimiento de ciberseguridad**.

      1.1.1. Línea de acción encaminada a fortalecer las entidades y organismos especializados de apoyo en la gestión, seguimiento, monitoreo y evaluación de ciberseguridad, a nivel de recursos tecnológicos, financieros, humanos, entre otros.
      1.1.2. Línea de acción tendente a fortalecer la gobernanza de las entidades y organismos especializados de apoyo y de las instituciones de investigación y persecución del ciberdelito.
      1.1.3. Línea de acción encargada de desarrollar planes de formación, capacitación y sensibilización para funcionarios y servidores en materia de ciberseguridad.
      1.1.4. Línea de acción tendente a crear mecanismos seguros y ágiles para reportes y denuncias de forma presencial y digital, así como también simplificar dichos trámites.

   1.2. Objetivo específico de **fortalecimiento de las instituciones del Estado en materia de ciberseguridad a nivel de estructuras, formación, estándares y lineamientos para el fortalecimiento de la seguridad de la información.**

      1.2.1. Línea de acción para articular **la revisión de las estructuras actuales de tecnologías de la información (TI) de las instituciones del Estado para establecer una estructura independiente, enfocada en la ciberseguridad, conforme a las buenas prácticas internacionales, con fines de priorizar los**

pilares fundamentales de la seguridad de la información en las instituciones del Estado.

1.2.2. Línea de acción encargada de diseñar un **plan de formación, capacitación y sensibilización en ciberseguridad para personal responsable de la seguridad de la información en las instituciones del Estado.**

1.2.3. Línea de acción tendente a **elaborar, definir y garantizar cumplimiento de los estándares para la seguridad** de las Tecnologías de la Información y Comunicación (TIC) en el Estado.

2. Objetivo estratégico de protección y resiliencia de infraestructuras: tendente a asegurar el continuo funcionamiento de las infraestructuras críticas nacionales y las infraestructuras de tecnologías de la información (TI) del Estado.

2.1. Objetivo específico para **fortalecer la protección de las infraestructuras críticas nacionales y las de tecnologías de la información (TI) del Estado.**

2.1.1. Línea de acción para elaborar y establecer un **plan nacional de respuesta a incidentes de ciberseguridad, y contingencias a riesgos**, que procure la adecuada actuación en la gestión de incidentes cibernéticos, riesgos de emergencia y crisis nacional.

2.1.2. Línea de acción tendente a **identificar y apoyar los organismos principales en el área de respuesta a incidentes** que puedan proporcionar soporte a las infraestructuras críticas nacionales y a las infraestructuras tecnologías de la información (TI) del Estado y del sector privado en función al Plan Nacional de Respuesta a Incidentes de Ciberseguridad.

2.1.3. Línea de acción encargada de **desarrollar y establecer los protocolos de activación y acción** para los organismos de respuesta, y todo el ciclo de gestión de los incidentes.

2.1.4. Línea de acción para elaborar y establecer un plan nacional de comunicación e intercambio de información ante crisis de incidentes de seguridad cibernética.

2.1.5. Línea de acción que trata de fortalecer los Equipos Sectoriales de Respuestas a Incidentes Cibernéticos (CSIRT) y promover el establecimiento de los mismos en los sectores críticos nacionales.

2.1.6. Línea de acción que pretende **diseñar, establecer y poner en marcha un plan de ejercicios de simulación de incidentes cibernéticos** para las infraestructuras críticas nacionales y las instituciones del Estado.

2.2. Objetivo específico para **fortalecer la gestión de riesgos, identificar las infraestructuras** críticas nacionales y las infraestructuras de tecnologías de la información (TI) relevantes del Estado y **efectuar un análisis de riesgo**.

2.2.1. Línea de acción encargada de **establecer una metodología común para la gestión de los riesgos cibernéticos**, y sus lineamientos, así como los mecanismos de gobernabilidad, para la **supervisión, evaluación y medición periódica de implementación y cumplimiento de las políticas de tecnologías de información**, los planes de riesgos y de continuidad operativa, en conformidad con las **mejores prácticas**, y alineada a los **estándares y metodologías internacionales para las infraestructuras críticas nacionales** y de las instituciones del Estado, y promover su adopción en el sector privado.

2.2.2. Línea de acción tendente a **establecer los criterios que determinan el grado de criticidad de una infraestructura,** basado en los estándares internacionales en la materia.

2.2.3. Línea de acción para **catalogar las infraestructuras** críticas nacionales e infraestructuras tecnologías de la información (TI) relevantes del Estado de acuerdo con los criterios que determinan su grado de criticidad, incluyendo los

servicios colaterales que las soportan.

2.2.4. Línea de acción tendente a **efectuar análisis de riesgo sobre las infraestructuras críticas** nacionales e infraestructuras tecnologías de la información (TI) relevantes del Estado y **determinar su nivel de vulnerabilidad**, contemplando la inclusión de los perfiles de riesgos sectoriales más críticos para la sociedad y la economía nacional.

2.3. Objetivo específico para **elaborar los reglamentos, normas, estándares y lineamientos para el fortalecimiento de la coordinación y respuesta a incidentes de ciberseguridad en las infraestructuras críticas nacionales y de tecnologías de la información (TI) del Estado.**

2.3.1. Línea de acción para **evaluar las normas y reglamentaciones emitidas por reguladores sectoriales** para someter propuestas de **actualizaciones** a estos órganos, atendiendo a **estándares internacionales.**

2.3.2. Línea de acción tendente a apoyar la **elaboración y el establecimiento de reglamentos sectoriales y en el diseño del modelo de gobernanza del sector.**

2.3.3. Línea de acción encargada de **elaborar y establecer los protocolos de intercambio de información entre los Equipos Sectoriales de Respuestas a Incidentes Cibernéticos (CSIRT), las instituciones del Estado, las infraestructuras críticas y el Equipo Nacional de Respuesta a Incidentes Cibernéticos (CSIRT-RD),** para la gestión de los incidentes de ciberseguridad.

3. Objetivo estratégico de educación y cultura: trata de promover y fortalecer la educación, sensibilización y cultura nacional de ciberseguridad.

3.1. Objetivo específico para **fomentar la inclusión de la formación y sensibilización en ciberseguridad en todos los niveles del sistema educativo**.

3.2. Objetivo específico tendente a **impulsar una cultura nacional de ciberseguridad en todo el país enfocada a las diferentes poblaciones vulnerables.**

3.2.1. Línea de acción dedicada a desarrollar un **programa general de concientización para sensibilizar y fortalecer el entendimiento de ciberseguridad**, conocer los riesgos, amenazas y forma de abordarlos estos temas, para niños, adolescentes, adultos mayores, mipymes, el **sector público** y privado, entre otros.

3.2.2. Línea de acción para **desarrollar campañas de sensibilización**, en medios tradicionales y digitales, **con el apoyo del sector público, privado**, la academia, organizaciones de medios y las organizaciones de la sociedad civil para fortalecer la cultura de ciberseguridad, promover la protección en línea de la información personal, y buenas prácticas en el uso de plataformas en línea y redes sociales.

3.2.3. Línea de acción 3.2.3 tendente a implementar programas de reconocimiento para diversos sectores en apoyo a la cooperación en los esfuerzos de concientización y cultura de ciberseguridad a la población.

4. Objetivo estratégico para realizar alianzas públicas y privadas nacionales e internacionales

4.1. Objetivo específico para realizar alianzas nacionales e internacionales **para fortalecer la cooperación.**

4.1.1. Línea de acción tendente a establecer **acuerdos marcos de cooperación** técnica, operativa y de capacitación para el fortalecimiento de la ciberseguridad.

4.1.2. Línea de acción para fortalecer las **alianzas con el sector privado**,

organizaciones de la sociedad civil y la **academia** para reafirmar la confianza ciudadana en la seguridad cibernética.

4.1.3. Línea de acción dedicada a fomentar la **relación con organismos e instituciones internacionales** para facilitar la cooperación transfronteriza.

4.1.4. Línea de acción para asegurar la participación de la República Dominicana en los foros internacionales.

4.1.5. Línea de acción para monitorear y evaluar el nivel de cumplimiento del país con los acuerdos y gobernanza del ciberespacio a nivel internacional.

5. **Objetivo estratégico y específico tendente a fomentar la investigación, el desarrollo y la innovación de la ciberseguridad y su entorno.**

6. **Objetivo estratégico tendente a fortalecer el marco normativo:** trata de fortalecer el marco normativo y regulatorio que incide en los temas relacionados con la ciberseguridad.

6.1. Objetivo específico para **fortalecer y garantizar el cumplimiento de las normativas legales, técnicas y regulatorias** de ciberseguridad al margen del contexto actual del país y el entorno.

6.1.1. Línea de acción para **monitorear, revisar y analizar el marco legal y normativo** vinculado a la ciberseguridad, ciberdefensa, ciberterrorismo y ciberdelito, y proponer un plan de actualización que garanticen un ecosistema nacional seguro, frente al contexto de nuevas amenazas y riesgos cibernéticos producto de las tecnologías emergentes, velando por la protección de los derechos humanos en línea, la niñez y el consumidor en línea, la protección de datos personales, las prioridades nacionales y los estándares internacionales relevantes.

6.1.2. Línea de acción tendente a **elaborar las normativas y los estándares técnicos** aplicables a la ciberseguridad y promover su adopción.

6.1.3. Línea de acción dedicada a **impulsar el cumplimiento** de las normativas en materia de ciberseguridad por parte de los **organismos de la administración** pública.

7. OBSERVACIÓN DE LOS DESÓRDENES INFORMATIVOS

7.1 Observación de los desórdenes informativos durante la campaña

7.1.1 Criterios de selección de la muestra

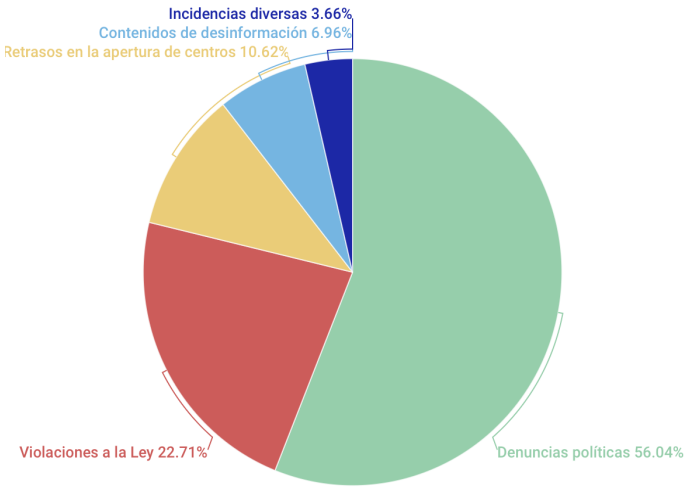
Se ha analizado el inventario de incidencias registrado por la dirección de comunicación de la Junta Central Electoral. En la muestra de **341 incidentes se recogen todos los contenidos vinculados a denuncias sobre el proceso, acusaciones a los miembros del pleno de la Junta Central Electoral.**

Esta muestra fue puesta a disposición de la Pontificia Universidad Católica Madre y Maestra, algunos estudiantes participaron en la etapa inicial del proceso de analizar la información.

El equipo de trabajo del Observatorio realizó dos procesos de análisis de la muestra: análogo y con el protocolo FIMI utilizando el Software *cyberelections* de Maldita.es , para este último se escogió una muestra de 34 casos del inventario, equivalente al 10% del total de incidencia registradas, priorizando las que fueron etiquetadas como desinformación por el Órgano Electoral y algunos casos en los que hubo respuesta, aunque debido a la ausencia de contraparte certificada, este último análisis no se pudo concluir.

7.1.2 Análisis de incidentes y recopilación de evidencia

Se identificaron 341 incidencias digitales. De estas incidencias, 19 estuvieron directamente relacionadas con desinformación. Las categorías más frecuentes de las 341 incidencias fueron las siguientes: 153 denuncias de distinta índole, 62 violaciones de la Ley Electoral como la compra y venta de cédulas en algunos centros de acopio a favor de los candidatos congresuales oficialistas, se reportaron 29 retrasos en la apertura de los centros de votación y se recogieron 19 desinformación. Asimismo, se publicaron 11 contenidos relacionados con encuestas y el resto de las publicaciones con menos de 10 incidencias.



Fuente: Elaboración propia

El equipo de comunicaciones de la Junta Central Electoral clasificó de la siguiente manera:

- **Abstención:** referidas a la acción de no ejercer el derecho al voto en una elección.
- **Boleta electoral:** problemas con la boleta electoral que es el documento en el que los votantes marcan su elección durante una elección. Contiene los nombres de los candidatos y las opciones disponibles para que los votantes elijan.
- **Cédulas:** las cédulas son documentos de identificación personal que se utilizan para verificar la identidad de los votantes durante las elecciones. Los votantes deben presentar su cédula para poder ejercer su derecho al voto. Los extranjeros no tienen derecho a votar. Los contenidos sobre estas publicaciones alegan la compra de cédulas para afectar el resultado electoral y la entrega de cédulas a haitianos para votar a favor de una tendencia política.
- **Certificado Primer Voto:** el Certificado Primer Voto es un documento que se emite a los ciudadanos que emiten su primer voto en una elección. Sirve como un reconocimiento y puede ser requerido en algunos casos. Varias personas se quejaron por no recibir su certificado de primer voto.
- **Colegio Electoral:** el lugar donde los ciudadanos votan directamente por los candidatos. Están presididos por funcionarios/delegados electorales. En algunos casos las denuncias son por la partidización de los funcionarios.
- **Delegados:** los delegados son representantes designados para coordinar el proceso de votación.
- **Denuncias:** las denuncias son informes o acusaciones informales hechas en las plataformas sobre posibles irregularidades o violaciones de la ley electoral durante el proceso electoral. Hay varias denuncias de personas ubicadas cerca de los recintos electorales haciendo proselitismo.
- **Empadronamiento:** es el proceso de registro de los ciudadanos en el padrón electoral, que es la lista de personas elegibles para votar en un colegio electoral. Los ciudadanos deben empadronarse para poder ejercer su derecho al voto en RD o fuera del país. Muchas personas no lo hicieron, por lo que se quejaron de que no aparecieron en el padrón electoral.
- **Encuestas:** las encuestas pueden ayudar a predecir resultados electorales y comprender las preferencias y tendencias de los votantes. Varias encuestadoras no inscritas ante la JCE publicaron resultados.
- **Escrutinio:** es el proceso de contar y verificar los votos emitidos durante una elección. Algunas denuncias tienen que ver con este proceso.
- **Fallos en el sistema:** se refieren a problemas técnicos o errores que pueden ocurrir durante el proceso de transmisión de los resultados.
- **Incidentes de violencia o intimidación:** situaciones en las que se produce violencia física o amenazas hacia los actores involucrados en el proceso electoral, como candidatos, votantes o funcionarios electorales. Estos incidentes pueden tener como objetivo influir en los resultados electorales o coartar la participación democrática.
- **Padrón:** el padrón electoral es la lista oficial de todos los ciudadanos registrados y elegibles para votar en una elección. Contiene la información personal de los votantes, como nombres, direcciones y números de cédula.
- **Pagos a colaboradores:** se refieren a la compensación económica de funcionarios públicos.
- **Problemas de conectividad:** se refieren a dificultades técnicas relacionadas con la conexión a internet o la comunicación entre los diferentes sistemas utilizados durante el proceso electoral. Estos problemas pueden afectar la transmisión de resultados.
- **Queja:** insatisfacción o descontento presentada por un votante o una parte interesada en relación con el proceso electoral. Las quejas pueden estar relacionadas con posibles irregularidades, violaciones de la ley electoral o cualquier otro problema

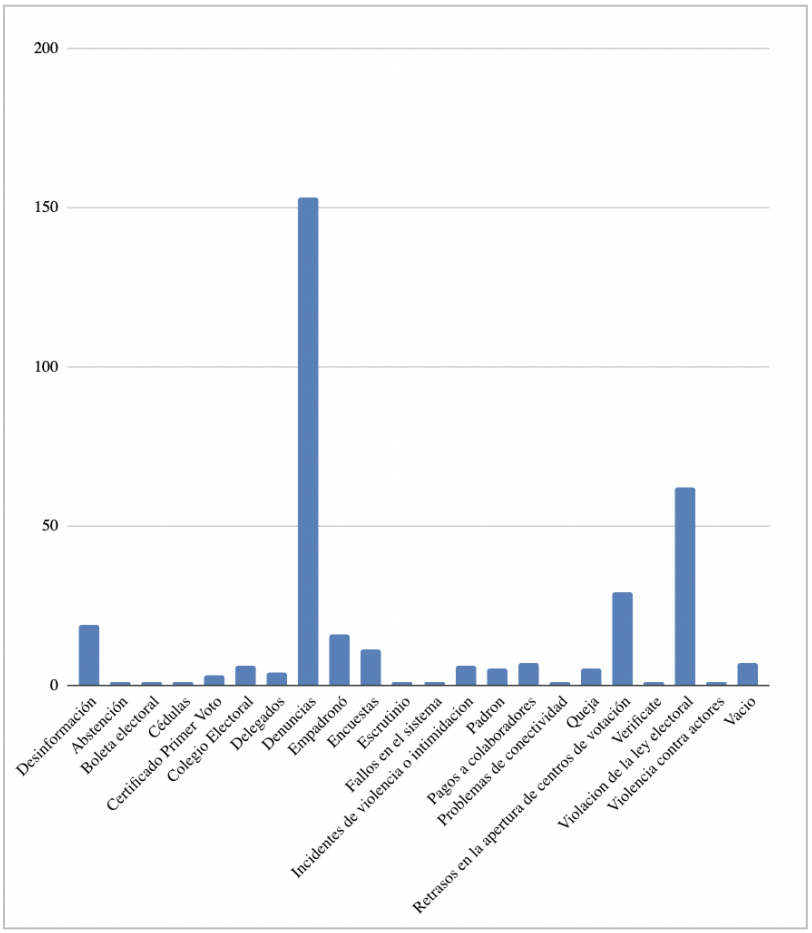
percibido durante el proceso electoral.

- **Retrasos en la apertura de centros de votación:** estos retrasos pueden deberse a problemas logísticos, falta de personal o cualquier otra circunstancia que impida la apertura puntual de los centros de votación.
- **Verifícate:** "Verifícate" portal oficial para conocer el colegio electoral donde le toca al ciudadano votar.
- **Violación de la ley electoral:** acción o comportamiento que infrinja las normas y regulaciones establecidas en la legislación electoral. Esto puede incluir acciones como la compra de votos, el uso indebido de recursos públicos, campaña en veda, la difusión de desinformación o cualquier otra actividad ilegal relacionada con el proceso electoral.
- **Violencia contra actores:** estos actos de violencia pueden tener como objetivo influir en los resultados electorales o coartar la participación democrática.
- **Vacío:** se refiere a una situación en la que no existe una regulación o normativa específica que aborde un aspecto particular del proceso electoral. Puede referirse a un vacío legal o a una falta de directrices claras sobre cómo abordar ciertos problemas o situaciones durante el proceso electoral.

7.1.3 Narrativas y metanarrativas detectadas

Al hacer un primer ejercicio de análisis de las narrativas de modo análogo, sin el uso de la herramienta de Maldita, se identificaron varios aspectos relevantes. En primer lugar, se encontró la narrativa que afirma la parcialización de la Junta Central Electoral a favor del partido oficial de gobierno, el Partido Revolucionario Moderno (PRM). Además, se mencionó el uso de fondos públicos y compra de votos en el proceso electoral, denunciando la inacción por parte de la JCE.

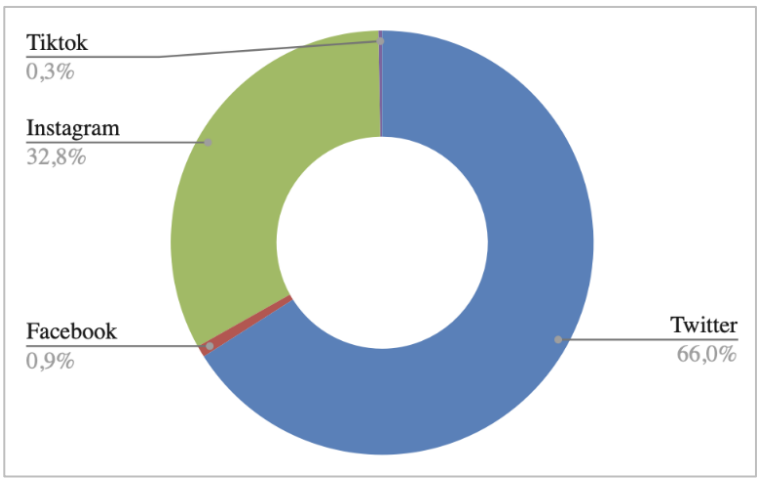
Cabe subrayar que, al revisar el tipo de denuncias recibidas, coincide con las desinformaciones, y la mayoría estuvo relacionada con el uso de recursos del estado, campañas durante la veda electoral y violaciones a la ley electoral durante el proceso de votación. Sin embargo, entendemos que al **no existir un procedimiento legal que norme el tratamiento de estas denuncias, no se siguió un proceso administrativo de investigación por parte de la Justicia Electoral, solo el levantamiento por parte del equipo de monitoreo sin resolución**. A continuación, se muestra el gráfico correspondiente.



Fuente: Elaboración propia

En cuanto a los canales más utilizados para denunciar y difundir desinformación electoral, se destaca **Twitter como el principal canal, con 225 incidencias reportadas.** Le sigue **Instagram con 112 incidencias**, Facebook con 3 y TikTok con 1.

Dado el amplio alcance y la facilidad con la que se replica entre los usuarios el contenido en estos medios, se resalta la importancia de hacer frente a la desinformación y así garantizar la imparcialidad en el proceso electoral. Para ello, es fundamental que se promueva la transparencia y se tomen medidas para investigar y sancionar las irregularidades detectadas.



Fuente: Elaboración propia

7.2 Análisis de las bibliotecas de anuncios disponibles durante el periodo de la campaña electoral

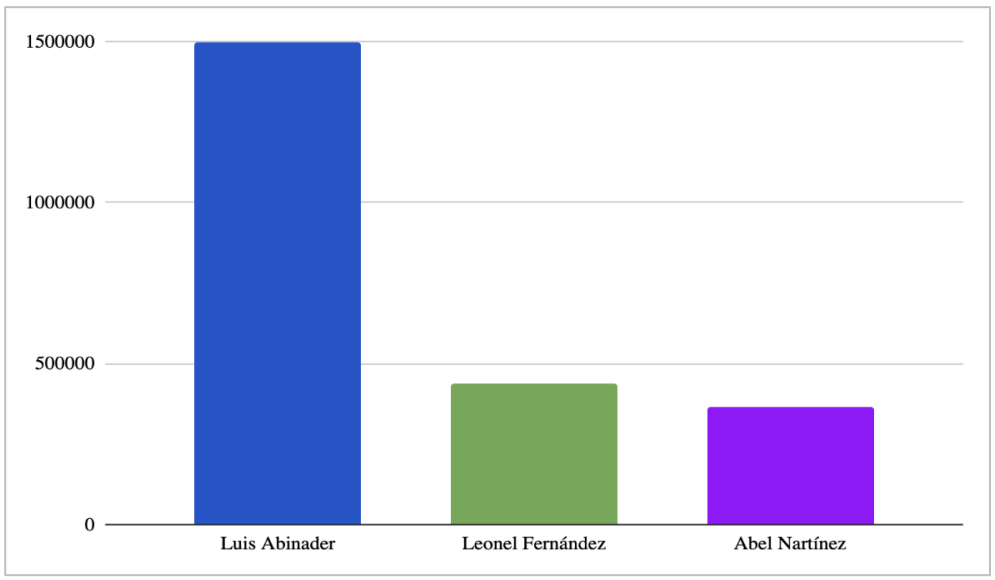
7.2.1 Actores (oficial, órganos electorales, partidos y candidatos, terceros)

Para el presente análisis, solo se encontró disponible la biblioteca de META (Facebook, Instagram y WhatsApp). En esta, los anuncios eran principalmente de candidatos, el Órgano Electoral y una mínima incidencia de contenidos 'Orgánicos", ninguno de estos con contenidos que comprometieron la integridad del proceso electoral.

En el caso de los Ads de Google (YouTube, Google Ads) uno de los principales canales digitales por donde se emite publicidad política, la biblioteca de publicidad política no está para República Dominicana. Solo está disponible en México, Argentina, Chile y Brasil. En el caso de Twitter, plataforma que ahora permite los Ads de índole política, tampoco su biblioteca es pública. Ya se ha mencionado que no hay un marco jurídico que regule la campaña en la dimensión digital, esto sumado a la imposibilidad de acceder a los datos de inversión de publicidad política en las principales plataformas de difusión de estas, da espacio al uso discrecional de estos canales, contribuyendo a competencia desigual, y en muchos casos a la alteración de los espacios de silencio/veda electoral.

7.2.2 Importe total e importes más destacados

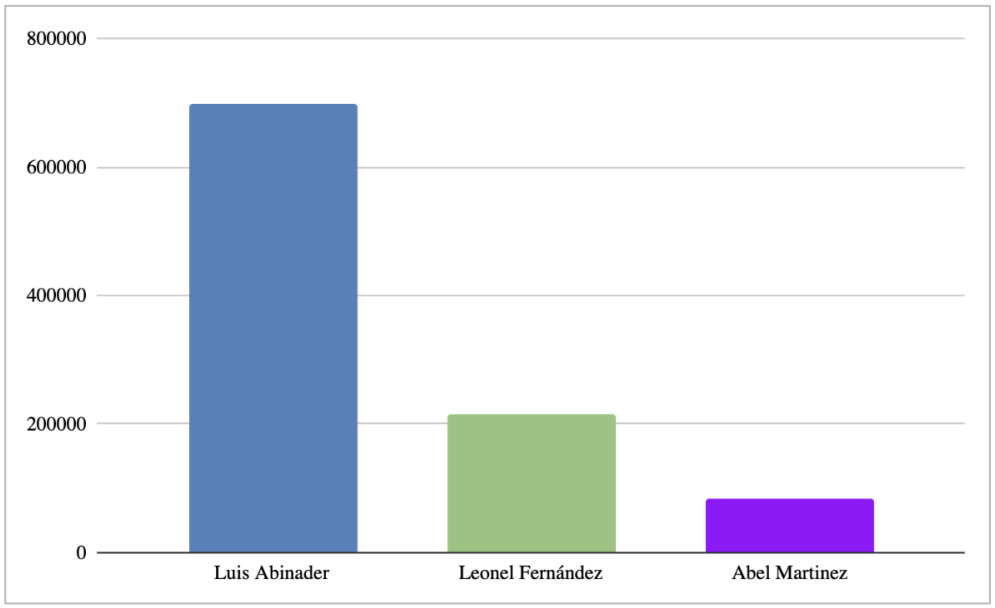
Hoy día el ámbito digital no es meramente un complemento de las estrategias tradicionales, sino un terreno crucial en la contienda política moderna. Un alto número de las campañas provinciales y nacionales que se realizan, tienen un gran enfoque en lo digital, aumentando la competitividad en ese entorno. Desde una perspectiva analítica, este territorio digital se convirtió en un espacio clave para la interacción política, la inversión que se hizo durante las campañas electorales en las distintas plataformas. De acuerdo con los datos del analista digital dominicano, Pavel de Camps[15], Luis Abinader se destacó como el candidato con el mayor crecimiento en las redes sociales, con Instagram liderando la contienda al obtener +115,326 nuevos seguidores, seguido por X con +52,918, YouTube con +9,300, Facebook con +6,000 y TikTok con +5,300.



Instagram

[15] Fuente: Pavel de Camps , @PaveldeCamps

Fuente: Elaboración propia



Fuente: Elaboración propia

Al investigar los gastos en publicidad digital, según los datos de la librería de anuncios de META, **Luis Abinader fue el candidato que más invirtió en redes sociales** con un total de **USD $426,053** a través de 2 páginas principales: Luis Abinader y Luis 24. El **segundo candidato que más invirtió en publicidad digital fue Abel Martínez**, con un gasto de **USD $187,346** dólares en anuncios. Sin embargo, Martínez fue el tercer candidato que más creció en redes sociales, siendo Instagram el medio donde más seguidores obtuvo con +22,226. Por otro lado, en X (Twitter) experimentó una disminución abrupta de -107,519 seguidores. En FB, al igual que Abinader, obtuvo +6,000 seguidores, +9,400 en TikTok y +600 en YouTube.

En el caso de **Leonel Fernández**, de los tres principales candidatos a la presidencia, **fue el que invirtió menos en publicidad digital**, con un gasto de **USD $16,515**. Sin embargo, fue el segundo candidato que más creció en Instagram, obteniendo +79,531 seguidores. También tuvo un crecimiento destacado en TikTok con +22,900 seguidores, en YouTube con 8,400 y en Facebook con +1,000.



Luis Abinader

Facebook	Instagram	X (Twitter)	TikTok	Youtube
698.000	1.500.000	1.000.000	178.600	58.000
Crecimiento	*Crecimiento*	*Crecimiento*	*Crecimiento*	*Crecimiento*
+ 6.000	*+ 115.326*	*+ 52.918*	*+ 5.300*	*+ 9.300*
704.000	1.615.326	1.052.918	183.900	67.300



Leonel Fernández

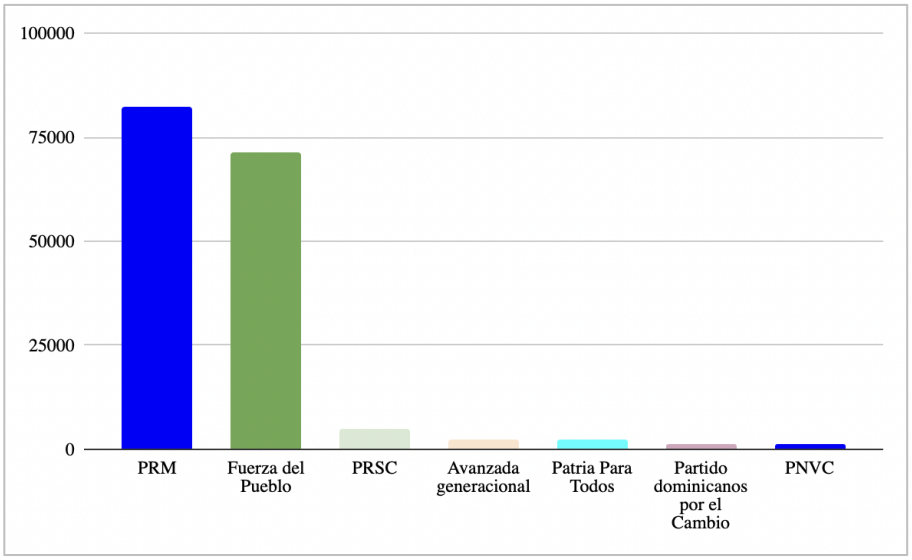
Facebook	Instagram	X (Twitter)	TikTok	Youtube
215.000	438.900	598.300	81.000	50.400
Crecimiento	*Crecimiento*	*Crecimiento*	*Crecimiento*	*Crecimiento*
+ 1.000	*+ 79.531*	*+ 5.351*	*+ 22.900*	*+ 8.400*
216.000	518.431	603.651	103.900	58.800



Abel Martínez

Facebook	Instagram	X (Twitter)	TikTok	Youtube
83.000	363.600	363.600	43.100	10.600
Crecimiento	*Crecimiento*	*Disminución*	*Crecimiento*	*Crecimiento*
+ 6.000	*+ 22.216*	*- 107.519*	*+ 9.400*	*+ 600*
89.000	385.816	256.081	52.500	11.200

En cuanto a los partidos, el **Partido Revolucionario Moderno (PRM) gastó USD $82,298** en publicidad digital, mientras que la **Fuerza del Pueblo invirtió USD $71,486**. En el caso del candidato presidencial Luis Abinader, es evidente que contó con un mayor presupuesto, más páginas de FB para distribuir recursos y además fue el portaaviones de los candidatos congresuales y senadores a nivel nacional, lo que le dio una ventaja en cuanto a su presencia en redes sociales. La inversión del PRM y la FDP fue superior a la del resto de los partidos políticos. El PLD no invirtió como partido.



Fuente: Elaboración propia

En la campaña nacional, el partido oficial tuvo más recursos, cosa que se reflejó en los resultados electorales a excepción de la contienda digital por la senaduría del Distrito Nacional, aunque **Guillermo Moreno gastó USD $45,436 en 118 anuncios, Omar Fernández logró un impacto significativo invirtiendo USD $43,141 en 45 anuncios estratégicos.**

En el caso de los Ads de Google, compañía dueña de YouTube, uno de los principales canales digitales por donde circuló publicidad electoral durante el proceso electoral, la biblioteca de Ads no está disponible para República Dominicana. Solo está disponible en México, Argentina, Chile y Brasil. En el caso de Twitter, plataforma que ahora permite los

Ads de índole política, tampoco tiene su biblioteca disponible para países de América Latina solo Europa. Cabe destacar que en ambos canales: YouTube como X (Twitter) la campaña durante la veda se incrementó.

A continuación, los datos de las compras publicitarias de los últimos 90 días previos a las elecciones de campaña de la librería de META de la República Dominicana:

Page ID	Page name	Disclaimer	Amount spent (USD)	Number of ads in Library
115301876826105	Luis24	Luis24	232252	220
253635411315081	Luis Abinader	Luis Abinader	193801	69
734071116605879	Abel Martínez	abelmartinezsectorexterno@gmail.com	187346	38
822022737837699	Partido Revolucionario Moderno PRM	Partido Revolucionario Moderno PRM	86298	111
493878640989577	Fuerza del Pueblo	La Fuerza del Pueblo	71486	126
31119393145	Guillermo Moreno	Guillermo Moreno	45436	118
703104329777124	Omar L. Fernández	Omar Fernandez	43141	45
111522395020384	Miguel Vargas	Miguel Vargas	36998	361
101581852174318	Fuerza Digital	Fuerza del Pueblo	36188	212
254168731109667	No mires para atras	No mires para atras	25107	60
321083414699132	Antonio Taveras Guzmán	Antonio Taveras	23911	186
106007344367029	anibaldiaz1	anibaldiaz1	22308	27
107838249029709	Sector Externo Con Abel 2024	Sector Externo Con Abel 2024	19954	15
734071116605879	Abel Martínez	Abel Martínez	19176	7
272221675964586	Leonel es Progreso	Leonel es Progreso	16515	10
1704086439631141	Liz Mieses	Liz Mieses	15015	681
339085486274571	Alexis Victoria Yeb	Alexis Victoria Yeb	11071	131
102316904801735	Roque Espaillat	Roque Espaillat	9319	13
111173542011822	Opinión RD	Opinión RD	8216	77
108587379178593	miprd	Partido Revolucionario Dominicano	7919	52
2198866780362264	Cacante	DataSRL	7885	12
243327488855022	Daniel Rivera	Daniel Rivera	7237	42
123397997671209	Listín Diario	Editora Listín Diario	7217	37
111484585277355	La Voz del Caribe	La Voz del Caribe	5730	53
104563872691724	Haydée Fadul	Haydee Fadul	5519	21
113006361873042	Jorge Leonardo Tavárez Valdez	Jorge Leonardo Tavárez Valdez	5217	46
857158420968826	Dr. Jhonny Medina Diputado	Dr. Jhonny Medina Diputado	5141	72
108067467411782	Raymond Diputado	Sub25	5036	73
162856027062762	(PRSC) Partido Reformista Social Cristiano	(PRSC) Partido Reformista Social Cristiano	4749	21
430008757208257	Dr. Iván Silva	Dr. Iván Silva	4281	202

Fuente: Librería de META

109134650449031	Gustavo Lara Salazar	Gustavo Lara Salazar	4072	68
182233498939275	País Posible	Pais Posible	3972	37
123489104473618	María Teresa Cabrera	María Teresa Cabrera	3845	19
332956889895735	Seguimos Unidos con Luis	Seguimos Unidos con Luis	3735	10
277609805587079	Pelegrin Castillo	Pelegrin Castillo	3449	13
151065776084	Leonardo Paniagua	Leonardo Paniagua	3416	59
894514950669625	Eugenio Cedeño	Eugenio Cedeño	3415	67
118031244729786	Robert E. Martínez	Robert E. Martínez	3188	63
260622983808957	Cholitin El Senador	Cholitin El Senador	3154	51
100710379656333	Movimiento Más Luis	Movimiento Más Luis	3066	68
253604491651072	Alfredo Pacheco Diputado	Alfredo Pacheco Diputado	2998	9
1477738419177340	Carlos Peña RD	Carlos Peña RD	2928	18
1889025001371004	Construyendo Con Cholitín	Construyendo Con Cholitín	2833	120
2385260388419056	Rafael Paz RD	Rafael Paz RD	2780	46
203663416156222	Virginia Antares Rodríguez	Virginia Antares Rodríguez	2766	43
309556172977925	Ing. Alexander perez	Ing. Alexander perez	2750	142
270444976151104	Silvia González Diputada	Equisoft SRL	2722	14
527516837662072	Vicente Sánchez	Vicente Sánchez	2701	25
2508132585868824	Candidatos RD	Candidatos RD	2687	51
110034781942381	Justicia Social	Justicia Social	2652	5
723068364502894	Rafael Duluc Cholitín	Rafael Duluc Cholitín	2628	18
105672461149444	Mateo Espaillat	Mateo Espaillat	2601	33
1555723231415892	Avanzada Generacional	Avanzada Generacional	2584	16
104246757869061	Raquel Peña	Raquel Peña	2495	7
163688327520908	Moisés Ayala	Moisés Ayala	2453	39
215329308339485	Fulgencio Severino	Partido Patria Para Todos y Todas	2446	7
170095596188700	Luis en Primera	Luis en Primera	2245	23
186000167929607	ANCLA	ANCLA SOCIAL 24	2230	42
241405362385750	BaniLejos al día	BANILEJOS AL DÍA	2164	26
261267053732815	Robinson Santos Diputado	Robinson Santos Diputado	2145	23
101252495067542	maria_laurabg	maria_laurabg	2126	51

Fuente: Librería de META

111692511830494	Jose Tavarez	Jose Tavarez	2087	15
364302183618093	Periódico Hoy	Digo Network	2065	7
292993744383759	Zoraima Cuello	Zoraima Cuello	1970	47
319648605292	Francisca Jáquez Diputada.	Francisca Jáquez Diputada.	1964	12
102559905972362	Raúl Lara	Raúl Lara	1962	32
510463889001499	Dr. Franklin Peña	Dr. Franklin Peña	1929	56
535680466801440	Yuri Enrique Rodríguez	Yuri Enrique Rodríguez	1914	13
266580736530346	Jose Del Castillo	José Del Castillo	1873	11
891945740901626	Emilio Doñe	Emilio Doñe	1862	48
179684385964003	Trajano Santana	Trajano Santana	1841	41
106379462553309	Jose Caraballo - Diputado	Jose Caraballo - Diputado	1827	22
287251521128170	Vanessa Hernández Diputada	Vanessa Hernández Diputada	1791	41
109525171809236	Republica Dominicana Elige - Encuestas Radio	República Dominicana Opina RCC	1768	27
101721332857262	Juan Carlos Echavarría	Juan Carlos Echavarría	1687	23
394443600887769	Emely Taveras	Emely Taveras	1682	9
220505164488044	Erredé Rap y Dembow	Opinión RD	1656	14
118091328056209	AbiVa2024	Abiva2024	1640	2
108337467605153	Ing. Ogando El Diputado Amigo	Ing. Ogando El Diputado Amigo	1639	6
112415850401253	Mi Familia con El Cambio	Mi Familia con El Cambio	1607	10
103597119509691	Monchy Diputado	Monchy Diputado	1599	15
107513408152399	Felipe Gavilán M	Felipe Gavilán M	1596	8
400067456731288	Francisco Luciano Alcalde	Francisco Luciano Alcalde	1595	10
106065020788412	Edison Garcia Diputado	Edison Garcia Diputado	1560	25
199479176794405	Partido Revolucionario Social Demócrata - PRSD	Partido Revolucionario Social Demócrata - PRSD	1500	25
229343182382010	Amable Cordones	Amable Cordones	1493	37
187684561105490	RD Sports	Opinión RD	1489	12
102328036043056	Juan Carlos Echavarria	Juan Carlos Echavarria	1486	21
275224596177335	Grupo SID	Grupo SID	1475	2
103185334455740	Hillary Diputada	Fior Daliza Peguero	1474	43
130992710099968	Claudia Rita Abreu	Claudia Rita Abreu	1468	19
117887798077086	Ariel Medos Diputado	Ariel Medos Diputado	1460	46
113200106043814	Nurca Nieves Luciano Jimenez	Nurca Nieves Luciano Jimenez	1455	7

Fuente: Librería de META

7.2.3 Tipos de anuncios (partidista, integridad electoral)

Los anuncios en las bibliotecas eran partidistas, sobre los candidatos, y educativos/informativos del proceso electoral promovidos por la Junta Central Electoral. No se evidenció publicidad contra la integridad del proceso electoral.

7.3 Incidencias reportadas en materia de ciberseguridad

La auditoría se realizó en dos fases: del 28 de noviembre al 8 de diciembre de 2023 y que durante este periodo el equipo de auditores tuvo la oportunidad de revisar y evaluar la solución tecnológica; y del 10 al 19 de enero de 2024, se entregaron las unidades EDET, ambientes y accesos requeridos con la nueva versión del software y mejoras de ambiente.

En esta auditoría, se comprobó que, de un total de 24 recomendaciones, 19 fueron cumplidas, 2 están parcialmente cumplidas y subsanadas con medidas compensatorias verificadas y comprobadas, al igual que las tres restantes.

Se hizo de conocimiento de los observadores que **los equipos de transmisión de resultados electorales** constan de varios componentes (laptop, impresora, módem, ups-backup, servidor) que se **comprueban previamente a iniciarse la jornada y que están auditados**, y que se cuenta con un 8% de equipos de respaldo por cada junta electoral a una hora u hora y media de distancia de los centros de votación aproximadamente. **Estos sistemas se han auditado y probado al menos tres veces** lo que asegura que los errores sean los mínimos. Un ejemplo de ello es que en febrero sólo hubo 30 incidencias.

Los equipos los instala un grupo de personas que tiene a su cargo cuatro colegios: hay un técnico que instala y presta la asistencia técnica (instala, prueba, hace el encendido de equipos, etc.). Según los datos proporcionados por la JCE, se trata de aproximadamente 8000 técnicos en el interior y exterior del país.

En aras a **evitar uno de los ataques más probables, Ddos,** la Junta Central Electoral tomó medidas preventivas, tales como hacer que la ciudadanía consulte las webs y redes sociales oficiales de la JCE de resultados y no a la web principal, así como se facilita la información a los medios de comunicación. Ello **evitó la congestión de la web principal** y que se produjese un error en los servicios. En todo caso la **JCE tenía en su poder un comunicado para responder ante ese posible escenario** desde el plano comunicativo.

La cuenta de la Red social X del presidente de República Dominicana, Luis Abinader, fue hackeada y posteriormente recuperada el sábado 18 de mayo, en la jornada de reflexión, según informó el Gobierno del país. Este ataque recuerda al sufrido por el presidente francés Emmanuel Macron en 2017, y que pone de manifiesto la imposibilidad de los candidatos de defenderse públicamente al estar en tiempo de veda electoral, y se produce en un momento de máxima sensibilidad.

Por ello, destaca la importancia de concienciar a los partidos políticos y candidatos sobre la seguridad de la información: se recomienda que se les haga entrega de la “Guía de ciberseguridad” que les hicimos llegar en la primera etapa de nuestra consultoría.

Además, conviene tener preparada una respuesta comunicacional ante este tipo de eventos en la cual se llame –y se subraye– a la responsabilidad ciudadana para no compartir informaciones, desinformación, que pudiese provenir de las cuentas de los candidatos en esas horas previas, en la jornada de reflexión.

8. REACCIONES Y MEDIDAS ADOPTADAS

8.1 Medidas adoptadas por organismos electorales

La normativa legal vigente no contempla mecanismos para levantar procedimientos administrativos frente a las desinformaciones como denuncias de violaciones de la ley electoral en la publicidad en redes sociales. A pesar de que el equipo de monitoreo realizó un seguimiento de las incidencias, **ninguna fue reportada a las plataformas correspondientes para solicitar su colaboración en la eliminación o suspensión del contenido, a pesar de tener al menos un contacto explícito para ello en una de las empresas de tecnología.** La falta de envío de solicitudes a las plataformas no dejó evidencia sobre su apoyo o falta de respuesta en el proceso.

En este análisis, queremos destacar cómo **la ausencia de mecanismos legales para abordar la desinformación en el contexto de la publicidad en redes sociales durante el proceso electoral o de violación a la ley electoral genera un vacío que puede dar ventajismo electoral a una facción y puede afectar la cognición de la ciudadanía.**

Por ello, se considera necesario establecer mecanismos jurídicos y procedimientos claros para reportar y abordar la desinformación, así como la necesidad de colaboración con las plataformas para garantizar la integridad del proceso electoral, para entender el grado de denuncia, y si hay evidencias o irregularidades en el proceso electoral que contengan elementos que impliquen una sanción frente a la violación de la normativa legal.

En ausencia de recursos jurídicos para el combate de la desinformación, la comunicación jugó un papel activo para estos fines, durante el proceso electoral. Su plan de comunicación fue amplio, ambicioso e innovador explorando nuevos formatos para llegar a todas las audiencias cuya valoración es positiva por el amplio trabajo que realizaron. Estuvo centrado en 4 pilares: información proactiva y oportuna, educación continua a la ciudadanía sobre el sistema electoral, motivación al voto y contrarrestar la desinformación. Este plan cumplió con los requisitos de divulgación de información sobre el proceso electoral, alfabetización de voto y concientización sobre la desinformación:

- Canal de YouTube: más de 31.5K suscriptores y 664 contenidos publicados
- JCE El Podcast en la plataforma de Spotify: 12 programas.
- Portal web actualizado
- Canal de Telegram
- Boletín digital informativo cada 2 semanas: 9400 suscriptores.
- Página de las elecciones: Elecciones 2024, landing page dentro de la web de la JCE. Allí está el Verificate.do
- Centro de Divulgación transmitido a través de YouTube
- Redes Sociales: Twitter, Instagram, Facebook, TikTok.
- Uso de Influencers para motivar al voto

Además, se destaca la existencia de un **Plan de comunicación proactivo con los medios de comunicación**, una política de comunicación abierta para la prensa:

- Encuentros constantes con los medios de comunicación
- Programa de TV Orientación Electoral: transmitido por el medio CDE en alianza con la JCE. Programa semanal, transmitido los domingos.
- Simulacros de votación en medios de comunicación

- Simulacros en estaciones del Metro
- Videos con líderes de opinión en diferentes medios y programas: noticieros, opinión, eventos, entrevistas, entre otros.
- Vinculación de figuras públicas, líderes de opinión, líderes de la iglesia evangélica y artistas para motivar al voto.
- Campaña publicitaria paga en los medios de comunicación dividida en dos etapas: educativa y motivacional.

En materia de desinformación, la JCE elaboró piezas comunicacionales para redes sociales y medios de comunicación, que exhortaron a la concientización ciudadana como denuncia. Asimismo, desarrolló una guía ABC para combatir la desinformación, pero esta no fue difundida en los canales digitales.

Para las elecciones Presidenciales y Congresuales, el equipo de Comunicaciones de la JCE realizó un levantamiento de las informaciones en las plataformas de redes sociales, incluyendo Twitter, Instagram, Facebook, LinkedIn y TikTok.

De modo preventivo, la Junta Central Electoral realizó un programa para intentar identificar, y contrarrestar la desinformación del proceso electoral, realizamos una análisis de las medidas implementadas en diferentes áreas en el Programa para Combatir la Desinformación.

8.2 Medidas adoptadas por las plataformas

8.2.1 Contenido orgánico

En ausencia de regulación de la campaña digital, las plataformas no tenían un marco jurídico local que les orientara a tomar medidas en los contenidos orgánicos. Sobre las incidencias recogidas (341), no hay registro de acciones o medidas desde las plataformas, aunque varios contenidos reportados ya no están disponibles.

8.2.2 Publicidad

Aunque la publicidad política digital durante el periodo electoral no está regulada, incluido el periodo de veda electoral, la JCE solicitó apoyo al equipo de META para desactivar la publicidad de un total de 431 anuncios publicitarios que se identificaron en Facebook e Instagram, pertenecientes a partidos políticos y candidatos a diputados y senadores. A pesar de que META accedió a suspenderlos, para el día de las elecciones aún se encontraban activos 68 de ellos.

8.2.2.1 ¿Han admitido compras fuera del proceso electoral (precampañas y veda)?

A pesar de que la ley contempla la regulación de los medios de comunicación masivos durante la veda electoral, actualmente no existe una regulación explícita sobre las campañas en redes sociales, muchos candidatos aprovecharon el vacío legal para invertir una gran cantidad de recursos durante la veda electoral, para aumentar su presencia en redes sociales durante el período de reflexión previo a las elecciones, **llegando incluso a aumentar la puja (precio) de los anuncios publicitarios**. Así, **durante la veda electoral, se identificaron un total de 431 anuncios publicitarios en Facebook e Instagram** pertenecientes a partidos políticos y candidatos a diputados y senadores. **Se solicitó apoyo al equipo de META desactivar la publicidad de estos contenidos durante la veda, a la cual accedieron; sin embargo, para el día de las elecciones, aún se encontraban activos**

68 de ellos. Asimismo, en Google, a través de los anuncios de YouTube, también se continuó con la publicidad de candidatos a diputados y senadores durante la veda electoral, pero a diferencia de META, con estas plataformas el órgano electoral no tiene ninguna relación.

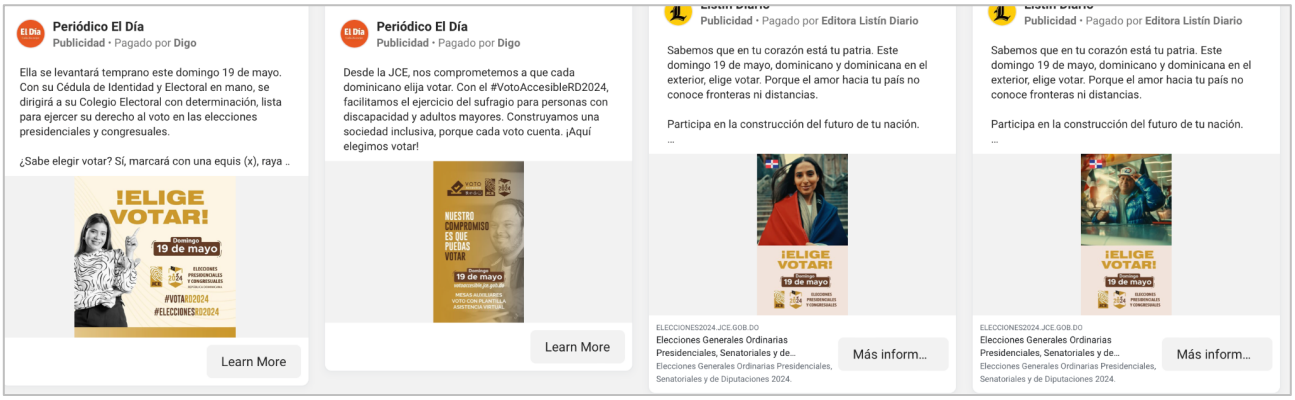
En el caso de Twitter, incluso la campaña electoral se extendió más allá de los candidatos, con la aparición de encuestas de boca de urna que intentaban predecir resultados. Destacamos especialmente el caso de @sincrimenrd con pauta sobre encuestas, la cual estaba fuera del plazo legal de difusión y no contaban con la acreditación de la JCE.

8.2.2.2 ¿Han admitido campañas contra la integridad electoral?

No observamos la admisión de compra de publicidad en contra de la integridad del proceso electoral. Ni campañas desinformativas articuladas para este fin.

8.2.2.3 ¿Han admitido campañas de terceros?

Adicionalmente a la Junta Central Electoral, los Partidos y candidatos en la Biblioteca de META se pueden verificar algunos anunciantes como medios de comunicación y cuentas de terceros (personales). Sin embargo, la publicidad de medios de comunicación sobre el proceso electoral redirecciona a la web del órgano electoral, evidenciado que esto es parte de la campaña digital articulada desde la dirección de comunicación de la Junta Central Electoral.



Fuente: Biblioteca anuncios META

8.2.3 Respuesta de las plataformas a las solicitudes de los organismos electorales

De los casos presentados META actuó en consecuencia. Frente a esta problemática, META alega lo siguiente:

1. En el caso de contenido orgánico, META no puede eliminarlo, ya que esto se consideraría una violación de la libertad de expresión.
2. Se eliminará el contenido desinformativo pagado si se proporcionan pruebas a META de que dicho contenido es falso o engañoso.
3. Se eliminará el contenido si se demuestra claramente que ha sido alterado utilizando IA, siempre y cuando se envíe a META tanto el video original como el video manipulado.
4. En la última fase, durante la veda electoral, sí hubo una mayor colaboración por parte de META para bajar los contenidos pagados que infringieron la ley.

En el caso de otras plataformas como X (anteriormente Twitter), TikTok y YouTube, no existe un puente de colaboración que permitiera este trabajo conjunto contra la desinformación.

8.3 Medidas adoptadas por los verificadores

La República Dominicana carece de un servicio dedicado a la verificación de datos, o "Fact Checker", así como de una plataforma que se enfoque de manera parcial en esta tarea. Esta carencia representa una valiosa oportunidad para la Junta Central Electoral (JCE) de cara a futuros comicios. Ejemplos como el del Tribunal Electoral de Panamá, que implementó la plataforma "Verificado", o el Instituto Nacional Electoral (INE) de México, que también cuenta con “Verificado MX”, una herramienta institucional de verificación de noticias, destacan la importancia y las bondades de este tipo de iniciativas.

Implementar una plataforma de fact-checking permitiría a la JCE reforzar la transparencia y la confianza en el proceso electoral, combatiendo la desinformación y garantizando que el electorado tenga acceso a información veraz y oportuna.

Además, una herramienta de este tipo no solo beneficiaría la integridad del proceso electoral, sino que también contribuiría a elevar el nivel del debate público, fomentando un entorno de comunicación basado en hechos comprobables. Esta iniciativa posicionaría a la República Dominicana a la vanguardia en la región en términos de innovación electoral, alineándose con las mejores prácticas internacionales.

9. EVALUACIÓN FINAL Y LECCIONES APRENDIDAS

9.1 Evaluación

A nivel general, existen oportunidades de mejora en las acciones implementadas para combatir la desinformación. En cuanto a la respuesta comunicacional, esta fue proactiva, innovadora y amplia. Sin embargo, en materia de desinformación, aunque contaron con piezas comunicacionales de concientización, como de denuncia, no profundizaban del todo ni en los mecanismos de verificación ni de denuncia. Por otro lado, si bien el equipo de comunicaciones de la JCE tomó previsiones y logró responder de manera efectiva a ciertos incidentes de desinformación que surgieron y afectaron la credibilidad de la institución, encontramos que **una de las principales áreas de mejora para dar respuesta a la desinformación, radica en la necesidad de una normativa legal clara que regule las campañas digitales y los fenómenos de desinformación en el ecosistema digital en República Dominicana**.

El equipo de comunicaciones de la JCE estuvo monitoreando de manera proactiva las redes sociales y atento a las tendencias, incidencias y denuncias reportadas en las diferentes plataformas, **pero la ausencia de procedimientos normativos claros limitó las respuestas a los mismos al ámbito comunicativo, disminuyendo la eficacia a la hora de solicitar el apoyo a las plataformas como para dar seguimiento a los casos de denuncia.**

Se pueden concentrar mayores esfuerzos para una adecuada pedagogía y sensibilización, específica y estratégica, sobre la desinformación electoral.

A nivel de ciberseguridad, podemos valorar positivamente las medidas implementadas en el Sistema de Gestión de Seguridad de la Información por cuanto no constan incidentes que afectasen al normal funcionamiento de la JCE. Ello se debe a que se llevaron a cabo auditorías de tecnologías y sistemas. No obstante, se ha de poner de relieve la necesidad de continuar revisando el Sistema de Gestión de Seguridad de la Información de forma periódica, pues permite adaptarnos a riesgos y amenazas acordes a las circunstancias actuales.

Se ha podido comprobar que **existe cierta debilidad en la concienciación en seguridad de la información que afecta a candidatos**, muestra de ello el hackeo a la cuenta personal del candidato Abinader. Por lo que se hace necesario trabajar en esta línea en la capacitación de estos y del conjunto de los empleados de la JCE. Había sido recomendable incidir en las recomendaciones que contenía la Guía de Ciberseguridad que se les entregó y que puede ser una buena herramienta para próximas ocasiones.

9.2 Lecciones aprendidas

9.2.1 Jurídicas

1. **Ampliar la regulación sobre campañas digitales en la normativa legal. En primer lugar, es importante ampliar la regulación existente en la normativa legal para abordar de manera más precisa y exhaustiva las campañas digitales durante los procesos electorales. Esto implica establecer reglas claras sobre el uso de redes sociales, plataformas en línea y herramientas digitales para promover la transparencia y la equidad en las campañas políticas.**

La JCE puede "reglamentar la propaganda política y electoral en los medios de comunicación social y de cualquier otra naturaleza" (art. 20 de la Ley Orgánica de Régimen Electoral), de modo que sería posible incluir disposiciones concretas referidas a las campañas digitales

Algunos aspectos que se podrían considerar en esta regulación son: establecer límites en el gasto de publicidad en línea; exigir la verificación de identidad de los responsables de las campañas digitales; establecer sanciones claras para las violaciones de las normas entre ellas las de veda electoral, acoso o violencia de género y difamación de información; y, finalmente, promover la transparencia en la divulgación de información sobre financiamiento de campañas digitales.

La previsión de nuevas infracciones administrativas o incluso de delitos requiere su regulación por Ley, de modo que sería necesario modificar la ley electoral para incluir estos nuevos ilícitos, salvo que se acogiera a la previsión legal (muy genérica) contenida en el Art. 310. 6) de la Ley Orgánica de Régimen Electoral "Los que violaren cualesquiera de las resoluciones que en atribuciones reglamentarias dicte la Junta Central Electoral".

2. **Ampliar la normativa legal para regular los fenómenos de desinformación. En segundo lugar, es necesario ampliar la normativa legal para abordar de manera efectiva los fenómenos de desinformación durante los procesos electorales. La desinformación puede tener un impacto significativo en la opinión pública y en la toma de decisiones de los votantes, por lo que es crucial establecer mecanismos para prevenirla, detectarla y combatirla.**

Algunas medidas que se podrían considerar en la ampliación de la normativa legal para regular la desinformación son: definir y tipificar la desinformación electoral como una infracción administrativa o como un delito; establecer mecanismos de monitoreo y verificación de información durante las campañas electorales; fomentar la educación cívica y digital para promover el pensamiento crítico entre los votantes; y promover la colaboración entre las autoridades electorales, las plataformas en línea y los medios de comunicación para abordar de manera conjunta la desinformación.

Además de las necesarias reformas legales, en caso de contemplar infracciones o sanciones, se podría dictar una reglamentación de la JCE abordando esta materia.

Junto a ello, las medidas concretas podrían implementarse con base al art. 20 de la Ley Orgánica de Régimen Electoral (numerales 20 y 22) que atribuye a la JCE la competencia para:

a) **Disponer las medidas que considere apropiadas para asegurar** el libre ejercicio de los derechos de tránsito, libre reunión, igualdad de acceso a los medios de comunicación, tanto estatales como privados, así como de todos **los derechos y obligaciones relacionados con la campaña electoral previstos en esta ley;**

b) **Disponer cuantas medidas considere necesarias para resolver cualquier dificultad** que se presente en el desarrollo del proceso electoral, y dictar, dentro de las atribuciones que le confiere la ley, todas las instrucciones que juzgue necesarias y convenientes, a fin de **rodear el sufragio de las mayores garantía**s y de ofrecer las mejores facilidades a todos los ciudadanos aptos para ejercer el derecho al voto. Dichas medidas tendrán carácter transitorio y sólo podrán ser dictadas y surtir efectos durante el período electoral de las elecciones de que se trate".

Todas estas previsiones normativas contribuirán a dotar de mayor seguridad jurídica al proceso electoral y reforzarán las atribuciones de la JCE, propiciando una respuesta más previsible y eficaz.

9.2.2 Comunicacionales

En el ámbito de la comunicación se podrían desarrollar mejoras en los siguientes ámbitos:

1. **Fact checker propio:** ante la inexistencia de un fact checker de garantías en la sociedad civil cabe la alternativa de que los organismos electorales desarrollen uno propio a través de una página web con un equipo o departamento encargado de verificar la veracidad de la información, especialmente en el contexto de las noticias y la desinformación relacionados con el proceso y los organismos electorales. Su función principal es analizar y contrastar la información para determinar su precisión y autenticidad, proporcionando así a la audiencia información verificada y confiable.

2. **WhatsApp / Chatbot:** implementación de un sistema de mensajería, vía WhatsApp, o un chatbot, específicamente diseñado para responder dudas relacionadas con desinformación, irregularidades electorales u otros problemas relacionados con el proceso electoral. Este canal permite a los ciudadanos comunicar de manera rápida y sencilla posibles violaciones o situaciones que requieran atención por parte de las autoridades electorales y recibir respuestas rápidas y automatizadas.

3. **Establecer canales y un procedimiento para las denuncias:** es necesario mantener canales y un procedimiento para las denuncias. Esto implica crear mecanismos claros y accesibles a través de los cuales los ciudadanos puedan reportar posibles casos de desinformación, irregularidades electorales u otros problemas relacionados con el proceso electoral que se les pueda dar seguimiento a través de la Justicia Electoral. Estos canales pueden incluir líneas telefónicas, formularios en línea, direcciones de correo electrónico o aplicaciones específicas, y el procedimiento debe garantizar la recepción, revisión y seguimiento adecuado de las denuncias recibidas.

4. **Red para combatir la desinformación**: una alianza organizativa que reúne a diversos actores de la sociedad civil: universidades, agencias, medios, corresponsales, etc., para combatir la desinformación es una estructura de verificación de hechos, para que los medios de comunicación procuren una divulgación de noticias más limpia, con el propósito de coordinar esfuerzos para identificar, desacreditar y contrarrestar la desinformación durante el proceso electoral. Esta red puede colaborar en la verificación de hechos, la difusión de información veraz y la sensibilización sobre la importancia de la verificación de la información.

5. **Negociación con las plataformas para la bajada de contenidos falsos o que violen la ley electoral de RD:** esto implica establecer acuerdos y mecanismos de cooperación con las plataformas, especialmente con META, como otras redes sociales y servicios de mensajería, para identificar, revisar y eliminar contenidos que sean falsos o que infrinjan la legislación electoral del país. Estos acuerdos buscan promover la eliminación rápida y efectiva de contenidos perjudiciales para el proceso electoral. No se puede dejar esto para el momento de la elección, es algo que se debe trabajar con mucho tiempo de antelación con META. Además, es necesario cultivar con tiempo la relación con el resto de las plataformas sociales con las que no

ha habido una relación efectiva durante el presente proceso electoral.

6. **Acuerdos con las plataformas de telefonía celular:** con el fin de establecer convenios y colaboraciones con los proveedores de servicios de telefonía móvil para difundir información verificada, promover la educación cívica y alertar sobre posibles casos de desinformación a través de mensajes de texto, notificaciones o campañas de concienciación dirigidas a los usuarios de telefonía celular.

7. **Plan de comunicación permanente para combatir la desinformación**: combatir la desinformación requiere de un conjunto de estrategias y acciones diseñadas para enseñar a los ciudadanos como verificar la información, promover la alfabetización mediática, sensibilizar sobre los riesgos de la desinformación y fomentar el pensamiento crítico entre la población. La experiencia previa demuestra que el plan no puede limitarse a los meses anteriores a la elección, sino que tiene que convertirse, en la línea de organismos electorales de todo el mundo, en una forma de acción permanente de la Junta. Este plan puede incluir campañas de concienciación, material educativo, colaboraciones con medios de comunicación y el uso de plataformas digitales para difundir mensajes veraces.

8. **Formación a periodistas e influenciadores para combatir la desinformación**: es clave para combatir la desinformación a través de recursos y herramientas profesionales para que puedan identificar, verificar y contrarrestar la desinformación. Esta formación puede incluir talleres, seminarios, guías de buenas prácticas y acceso a fuentes confiables de verificación de hechos.

9.2.3 Organizativas

Respecto a las oportunidades en la organización, se pudiera incluir:

1. Un protocolo que permita a todas las áreas conocer el proceso y canales de tratamiento de dudas y contenidos desinformativos.

2. Mesa con **los diferentes equipos de comunicaciones, monitoreo digital, organización electoral, jurídica**, y contraparte de las plataformas digitales. Esto es esencial para el abordaje transversal de incidencias.

9.2.4 Educativas

1. Incluir en los programas para universitarios una línea de sensibilización sobre desórdenes informativos.

2. Incluir en el programa de simulación electoral para adolescentes en las escuelas, contenido de manera lúdica para abordar el tema de la desinformación y sus efectos negativos en los procesos electorales.

3. Programa de sensibilización para sociedad civil, población en general.

4. Añadir prevención de desinformación como contenido en la materia de Comunicación Política y Marketing Electoral de la maestría de Gerencia de Partidos Políticos y en la maestría de Derecho Electoral junto al Tribunal.

5. Desarrollar una materia transversal o un programa exclusivo sobre desinformación,

que puede realizarse en colaboración con alguna universidad, y que pase a formar parte de la oferta formativa de la Junta.

9.2.5 Relaciones interinstitucionales con las plataformas

En cuanto a las plataformas, **se recomienda establecer un canal oficial para una comunicación fluida y constante con ellas, y establecer un acuerdo aprobado por ambas partes en cuanto al proceso para la eliminación de contenidos que violen las normas electorales.** Ante el desacato de las plataformas, para poder combatir la desinformación electoral recomendamos:

1. **Establecer acuerdos claros y aprobados por ambas partes con las plataformas para la eliminación de contenidos que violen las normas electorales.**

2. Promover una mayor coordinación y cooperación entre las plataformas y las instituciones electorales para garantizar la integridad del proceso electoral.

3. Implementar mecanismos que permitan la identificación y eliminación eficaz de la desinformación, respetando al mismo tiempo la libertad de expresión.

4. Fomentar la transparencia y la responsabilidad por parte de las plataformas en la gestión de contenidos electorales, evitando así el ventajismo electoral y protegiendo el espacio de reflexión durante la veda electoral.

9.2.6 Ciberseguridad

1. **Revisión periódica del Sistema de seguridad de la información:** la revisión constante del Sistema de seguridad de la información es crucial para determinar el estado actual de la institución y para prevenir, mitigar y responder de manera eficaz y eficiente a los diversos eventos de ciberseguridad.

2. **Actualización de la información sobre auditorías realizadas en la web:** la práctica de actualizar regularmente la información sobre auditorías en la web puede mejorar la imagen de la institución y fomentar la confianza pública al permitir un control transparente sobre las auditorías realizadas. Esta transparencia demuestra el compromiso de la Junta Central Electoral con la ciberseguridad.

3. **Mejora de la visibilidad de las certificaciones ISO:** incrementar la visibilidad de las certificaciones ISO obtenidas refuerza la confianza en la institución, ya que demuestra el cumplimiento de estándares internacionales y la acreditación por parte de autoridades independientes y externas a la Junta Central Electoral.

4. Se recomienda revisar periódicamente el Sistema de seguridad de la información implementado para asegurar su actualización y protección frente a amenazas nuevas y renovadas. Además, es esencial actualizar la información sobre auditorías realizadas en la web y mejorar la visibilidad de las certificaciones ISO obtenidas, con el fin de fortalecer la confianza en la institución.