Instituto Nacional Electoral

CURSO INTERNACIONAL ESPECIALIZADO

EL USO DE LAS PLATAFORMAS DIGITALES EN LOS PROCESOS ELECTORALES Y SUS PRINCIPALES DESAFÍOS

INFORME FINAL

Ciudad de México del 6 al 10 de noviembre, 2023

CONTENIDO

Curso Internacional Especializado “El uso de las plataformas digitales en los procesos electorales y sus principales desafíos”

Del 6 al 10 de noviembre, 2023

Países representados: 9 países y 29 estados de la República.
Países: Bolivia (TSE), Ecuador (CNE y TCE), El Salvador (TSE), Honduras (CNE), Instituto Interamericano de Derechos Humanos (IIDH), (TE) Panamá; (TSJE) Paraguay, (ONPE y RENIEC) Perú y (JCE) República Dominicana.
Estados de la República: Aguascalientes, Baja California, Baja California Sur, Campeche, Chihuahua, Chiapas, Ciudad de México, Coahuila, Colima, Durango, Estado de México, Guerrero, Jalisco, Michoacán, Morelos, Nuevo León, Querétaro, Quintana Roo, San Luis Potosí, Sinaloa, Sonora, Tabasco, Tlaxcala, Yucatán, Zacatecas.

Instituciones colaboradoras: IDEA Internacional, IFES, Centro Nacional de Ciberseguridad de República Dominicana (CNCS), TSE de Costa Rica, TE de Panamá.

***Participantes*:** 120 personas funcionarias de organismos electorales de América Latina y de Organismos Públicos Locales Electorales de México y 47 personas funcionarias del INE.

Objetivo: Analizar los desafíos que representarán las plataformas digitales a los organismos electorales en la organización y desarrollo de los procesos electorales desde diferentes perspectivas: desde el empleo por parte de las y los candidatos y de los partidos políticos de las redes sociales, las plataformas y las aplicaciones en las campañas, tanto para informar e influenciar el voto como sus costos económicos. Desde el ámbito de las autoridades electorales, la regulación en materia de fiscalización de recursos y las posibles restricciones para la utilización de las TIC’s en términos de facilitación de la gestión electoral. Los retos que representará para las autoridades electorales combatir la desinformación y la protección de plataformas como la lista electoral, el voto electrónico y de resultados electorales frente a ciberataques que, mediante la ingeniería social pueden impedir el acceso a las plataformas; o bien, profundizan la polarización y minar la confianza en la integridad de las elecciones y la democracia.

Asimismo, las personas funcionarias de los organismos electorales y expertas brindaron una visión general sobre la utilización de la inteligencia artificial (IA) en el ámbito electoral, analizando tanto los beneficios potenciales como los riesgos asociados. Resalta la importancia de la supervisión humana y la necesidad de establecer principios éticos claros para guiar su implementación. En particular, se subraya la importancia de la ciberseguridad en los procesos electorales, así como la necesidad de una preparación y colaboración constantes para proteger la integridad del sistema electoral.

Entre las principales conclusiones que se incluyen en el informe, se destaca la relevancia de adoptar un enfoque integral y colaborativo para enfrentar los desafíos digitales en los procesos electorales. Este enfoque busca promover una participación democrática informada y responsable, asegurando así que los procesos electorales sean justos y seguros.

LUNES 6 DE NOVIEMBRE

1. Introducción

En la era digital que estamos viviendo, las plataformas digitales han transformado radicalmente la forma en que se desarrollan y se comunican los procesos electorales en todo el mundo. Las herramientas tecnológicas han revolucionado la manera en que las y los candidatos, y los partidos políticos se vinculan con los votantes, cómo se difunden sus propuestas políticas y cómo se informa y se participa en las elecciones. La importancia de las plataformas digitales en los procesos electorales es innegable y se extiende a múltiples aspectos clave de la política contemporánea.

En un contexto donde la comunicación y la información fluyen rápidamente a través de la red, las plataformas digitales han democratizado la participación política y han abierto nuevas oportunidades para la transparencia y el compromiso cívico. La ciudadanía ya no es mera espectadora de la política, sino que puede convertirse en actor activo, expresando sus opiniones, compartiendo contenido político y organizándose en línea.

Asimismo, las plataformas digitales han permitido a las y los candidatos, y partidos políticos, llegar a audiencias más amplias y específicas, personalizando mensajes y adaptando estrategias de campaña en función de los datos y análisis en tiempo real. Esto ha revolucionado la forma en que se diseñan y ejecutan las campañas políticas, impulsando la eficacia de la movilización y la recaudación de fondos.

No obstante, esta transformación digital no está exenta de desafíos y preocupaciones. El uso de las redes sociales y otras plataformas en la política han planteado cuestiones relacionadas con la privacidad, la seguridad cibernética, la desinformación y la influencia negativa. Por lo tanto, comprender y gestionar de manera efectiva el papel de las plataformas digitales en los procesos electorales es esencial para garantizar elecciones justas, transparentes y equitativas en esta era de la información.[1]

[1] María del Mar Trejo Pérez. Aportación del Curso Internacional Especializado sobre el Uso de Plataformas Digitales en los Procesos Electorales y sus Principales Desafíos.

2. Sesión inaugural

Norma De La Cruz, Consejera Electoral, INE - México

Norma De La Cruz, Consejera Electoral del INE de México, destaca la importancia de compartir buenas prácticas y enfrentar juntos los desafíos comunes que enfrentan las autoridades electorales. Durante el curso, subrayó que la desinformación avanza a un ritmo más veloz de lo que se puede actuar y mucho más lento de lo que se puede legislar, creando un entorno complejo para los sistemas electorales.

En México, la diversidad de sus 32 sistemas electorales, cada uno con su propia Ley, Constitución, Poder Ejecutivo, Legislativo y Gobiernos Municipales, añade una capa adicional de dificultad. Todos estos sistemas están expuestos a campañas de desinformación, lo que subraya la urgencia de una colaboración internacional.

La consejera electoral también señaló que los espacios digitales son el principal escenario donde se manifiesta la violencia de género, haciendo un llamado a los participantes internacionales a unir esfuerzos para combatir los ataques de desinformación.

Asimismo, La Consejera De La Cruz enfatizó la necesidad de un uso ético de las plataformas sociales. Instó a convertir estas herramientas en instrumentos que empoderen a la ciudadanía, promuevan la apropiación de los procesos políticos y faciliten el debate directo entre actores políticos y la ciudadanía, en lugar de ser vehículos de polarización, desinformación o descalificación.

3. Los organismos de administración electoral y el uso de plataformas digitales:

- Integridad electoral y redes sociales
- Difusión de contenido veraz y certero
- Acuerdos institucionales entre organismos de administración electoral con medios tradicionales y digitales: (X, Google, Meta)

En la actualidad, la certeza de que los procesos electorales se desarrollan de manera eficiente es fundamental para la democracia. En este contexto, Norma De La Cruz, Consejera Electoral del Instituto Nacional Electoral (INE) de México, destacó la importancia de ampliar y fortalecer un equipo de monitores que analiza la información electoral a nivel nacional. Este equipo proporciona respuestas expeditas, lo que requiere la colaboración de todos los organismos públicos electorales.

Norma De La Cruz subrayó varias buenas prácticas que son esenciales para mejorar la gestión de la información electoral y combatir la desinformación:

- **Ser canales de información transparente y responsable para medios y ciudadanía:** Los organismos electorales deben actuar como fuentes confiables de información.
- **Establecer o reforzar alianzas con iniciativas ciudadanas y medios de comunicación:** La colaboración con diversos actores sociales es crucial para difundir información verídica.
- **Realizar pedagogía electoral:** Es vital educar a la ciudadanía sobre los procesos electorales y proporcionar información útil y precisa.
- **Fortalecer la comunicación e integración de equipos interinstitucionales:** La coordinación entre diferentes instituciones mejora la eficacia de la respuesta ante la desinformación.

La consejera electoral enfatizó que la existencia de convenios con plataformas digitales permite respuestas más inmediatas a publicaciones que no cumplen con las normas, ya que éstas se eliminan rápidamente conforme a las políticas de las plataformas. Un ejemplo destacado es la publicación de la “Guía para la prevención de la violencia mediática” a través de Facebook, que ha sido una herramienta útil para abordar esta problemática.

Norma De La Cruz concluyó subrayando la necesidad de una educación transversal institucional, con el objetivo de coadyuvar a erradicar la desinformación. Esta educación debe ser integral y abarcar todos los niveles y áreas de la administración electoral para garantizar la transparencia y la confianza en los procesos democráticos.

4. Panorama global sobre el uso y abuso de las nuevas tecnologías de la información para fines político-electorales

Gustavo Román, Director General de Estrategia y Gestión Política-Institucional, TSE- Costa Rica

Gustavo Román, Director General de Estrategia y Gestión Política-Institucional del Tribunal Supremo de Elecciones (TSE) de Costa Rica, analizó el impacto de las nuevas tecnologías de la información en los procesos político-electorales. Su discurso se centró en los usos y abusos de estas tecnologías, enfatizando la necesidad de promover el pensamiento crítico para combatir la desinformación.

Destacó la importancia de la tecnología en la competencia política dentro de los sistemas electorales. La competencia por la simpatía, la confianza y la credibilidad de los votantes ha sido influenciada significativamente por los avances tecnológicos. Aunque las tecnologías han cambiado, el objetivo principal sigue siendo conocer al elector, entender sus preferencias y persuadirlo en consecuencia.

A finales del siglo XX y principios del XXI, las innovaciones tecnológicas en el ámbito electoral generaron grandes esperanzas. Un ejemplo icónico de esto es la campaña de Barack Obama en 2008, que utilizó estrategias tecnológicas avanzadas para conectar con los votantes. Sin embargo, Gustavo Román se centró en los aspectos negativos y los abusos de estas tecnologías.

El ecosistema mediático actual es radicalmente diferente al del siglo XX, que inspiró las legislaciones vigentes en muchos países. Los abusos de las tecnologías de la información incluyen la manipulación de motores de búsqueda y el uso de herramientas de publicidad digital para difundir desinformación; posicionar información falsa en los primeros resultados de las consultas en motores de búsqueda, influyendo en la percepción pública.

Una de las estrategias utilizadas por los organismos electorales para combatir la desinformación es la promoción del pensamiento crítico. Román enfatizó la importancia de fomentar la desconfianza y la malicia en la ciudadanía, alentándola a cuestionar la información que recibe.

MARTES 7 DE NOVIEMBRE

5. **El nuevo ecosistema mediático y el modelo brasileño de verificación de información político-electoral.**
   Frederico Alvim, Experto internacional – Brasil

Frederico Alvim, presentó un análisis detallado sobre cómo Brasil combate la desinformación y las noticias falsas en el contexto político-electoral mediante estrategias de mapeo y análisis de riesgos. Este informe sintetiza sus observaciones y propuestas, destacando las ventajas y desventajas del modelo brasileño de verificación de información, así como los principios básicos y mecanismos implementados para mantener la integridad electoral en un ecosistema mediático en constante cambio.

En Brasil, se han implementado diversas estrategias para prevenir y mitigar la desinformación. Estas incluyen:

- **Mapeo y análisis de riesgos:** Se anticipan las posibles amenazas de desinformación y se diseñan soluciones preventivas.
- **Medidas de prevención:** Dado que la desinformación es externa, se implementan medidas específicas para prevenir su impacto.

Ventajas del Modelo Brasileño

- **Independencia:** Se garantiza que habrá desmentidos en todos los casos, manteniendo una postura neutral.
- **Agilidad:** Los verificadores tienen pericia en los temas y acceso directo e inmediato a datos oficiales, lo que permite una respuesta rápida.

Desafíos del modelo

- **Menor credibilidad intrínseca:** La percepción de falta de objetividad y la posible existencia de intereses pueden disminuir la credibilidad.
- **Efecto de rebote:** Una postura autoritaria o el monopolio de la verdad pueden generar rechazo.
- **Actuación no profesional:** La verificación de información requiere criterios y complejidades que pueden no ser manejados adecuadamente.
- **Fragilización del modelo de negocios de la prensa especializada:** La competencia con los medios tradicionales puede debilitar su modelo de negocios.

Principios básicos para la verificación de hechos

La Red Internacional de Fact Checkers ha fijado un código de principios que debe ser observado por periodistas y otros profesionales que manejan informaciones de interés público.

- **Apartidismo:** Mantener objetividad y neutralidad ideológica.
- **Transparencia de las fuentes:** Permitir la verificación de la verificación.
- **Transparencia del financiamiento:** Divulgar el origen de los ingresos.
- **Autonomía:** Garantizar la independencia de los financiadores.
- **Transparencia metodológica:** Explicar claramente los métodos utilizados.
- **Compromiso con correcciones:** Reconocer y alertar sobre posibles errores.

Brasil ha establecido una red de verificación con nueve agencias especializadas que operan de la siguiente manera:

- **Comunicación en tiempo real:** Utilizan un grupo de WhatsApp que incluye a todos los organismos electorales subnacionales, priorizando la atención a las demandas de comunicación.
- **Independencia financiera:** Las alianzas con estas agencias no tienen contrapartida financiera, lo que asegura la neutralidad. Las fuentes de ingresos incluyen suscripciones, donaciones, cursos de capacitación, consultorías y producción de contenido.

¿Cómo aprovechar la verificación de hechos?
Brasil ha desarrollado diversas herramientas para aprovechar la verificación de hechos:

1. **Portal de desmentidos:** Incluye todos los desmentidos que atacan la integridad del órgano electoral, con filtros y mecanismos de búsqueda.
2. **Chatbot de WhatsApp:** Responde a dudas de los ciudadanos.
3. **Canal de Telegram y aplicaciones oficiales:** Facilitan la difusión de información verificada.
4. **Aplicaciones para celulares:** Incluyen funciones para funcionarios de casillas, portar documentos electorales y realizar denuncias ciudadanas.
5. **Mapa de aclaraciones:** Visualiza las desinformaciones y aclaraciones.
6. **Alianzas con aplicaciones de comida:** Amplía el alcance de la información verificada.
7. **Medios analógicos y prebunking:** Se revisan y aclaran desinformaciones cíclicas.

Frederico Alvim concluyó que el principal problema de los organismos electorales no es la desinformación en sí misma, sino la receptividad de la población a ésta en la era de la posverdad. La implementación de un sistema robusto de verificación de hechos y la promoción del pensamiento crítico son esenciales para mantener la integridad de los procesos electorales.

6. **Mecanismos para el monitoreo de campañas políticas en las redes sociales.**
   Francisco Morales, Especialista en Marketing Digital, CEMDI - TE – Panamá

Lo importante a destacar con el monitoreo de redes sociales es que es la oficina que se encarga de hacer el monitoreo, es la primera fuente de información para la institución.

Los diferentes temas que se siguen en el monitoreo son:

1. Reputación y gestión de crisis
2. Detección de información falsa y desinformación
3. Análisis de tendencias y opiniones de las personas
4. Participación ciudadana
5. Detección de violaciones y delitos electorales

La información se recolecta de redes sociales, bibliotecas de anuncios, denuncias, herramientas de pauta y de monitoreo. Para llevar a cabo el monitoreo efectivo, se emplean diversas herramientas especializadas como Brandwatch y SentiOne, que permiten analizar patrones de comportamiento y detectar actividad sospechosa como granjas de bots.

El tipo de información recolectada se clasifica y se da el tratamiento necesario, es decir, se pasa a los agentes de toma de decisiones para que determinen la atención requerida.

1. **Violaciones del código electoral:** Cualquier pauta identificada fuera del periodo electoral está violando la ley. Al detectar una violación, se inicia un proceso que puede llevar a sanciones como el retiro de la publicación o una multa económica.
2. **Pauta de terceros:** Se identifican las pautas realizadas por familiares o simpatizantes a favor de un candidato. Estos gastos se contabilizan como realizados por el candidato.

El equipo realiza un monitoreo manual de imágenes y contenido de campaña en redes sociales para verificar la exactitud de los informes de fiscalización. Esto asegura que todas las actividades sean transparentes y conformes con las normativas electorales.

Análisis de Sentimientos

El análisis de sentimientos es crucial para entender la percepción de la ciudadanía ante determinados temas. Las publicaciones se clasifican como positivas, negativas o neutrales, lo que permite una comprensión más profunda de las opiniones y tendencias.

Se enfatiza la importancia de combatir la desinformación mediante acciones proactivas como desmentidos públicos y la colaboración con aliados como medios de comunicación e influencers. Es crucial mantener un manejo efectivo de crisis y coordinar con autoridades electorales para asegurar la integridad del proceso democrático.

7. **Violencia política en razón de género y acoso en contra de oficiales electorales en plataformas digitales**
   Ingrid Bicu, Experta Internacional, Rumania

"La violencia política en razón de género se da en plataformas digitales debido al aumento del consumo de contenido digital."

La exposición se estructuró en tres áreas principales de análisis:

1. **Análisis Global de la Desinformación:** Se destacó que la desinformación dirigida a procesos electorales, organizaciones y oficiales electorales es una tendencia preocupante. Durante la investigación, se identificaron múltiples actores involucrados en la propagación de narrativas falsas, incluyendo usuarios anónimos, figuras políticas y medios de comunicación en línea. Estos ataques suelen intensificarse en períodos electorales clave, lo que mina la confianza pública, reduce la participación electoral y puede aumentar la violencia política.
2. **Desafíos para Oficiales Electorales:** Los oficiales electorales enfrentan desafíos significativos en entornos informativos saturados de desinformación. La falta de medidas efectivas para contrarrestar estos ataques puede comprometer la integridad de los procesos electorales y afectar negativamente la percepción pública sobre la imparcialidad y la transparencia de las elecciones.
3. **Impacto y Dinámica del Entorno Informativo:** Se enfatizó que la desinformación no solo influye en las decisiones electorales, sino que también genera un ambiente de desconfianza y polarización. Es crucial que las instituciones electorales implementen estrategias proactivas basadas en un monitoreo continuo para mitigar los efectos nocivos de la desinformación durante las campañas electorales.

Finalmente proporcionó una visión integral y detallada sobre los problemas emergentes de la violencia política de género y el acoso en plataformas digitales. Destacó la importancia de fortalecer las capacidades institucionales y adoptar políticas inclusivas que promuevan entornos electorales libres de violencia y desinformación.

8. **Estrategia de manejo de crisis de comunicación para mantener la confianza ciudadana cuando surge desinformación durante las elecciones.**
   Lisa Reppell, Oficial Superior de Investigación, IFES – Estados Unidos de América

Lisa Reppell presentó una estrategia integral para gestionar crisis de comunicación durante elecciones, enfocada en pasar de respuestas reactivas a proactivas.

"La clave radica en anticiparse a los ataques, planificar, prepararse adecuadamente y activar estrategias efectivas para mantener la confianza pública."

- **Planear:** Anticiparse, identificar valores, definir el público, identificar audiencia.

Es fundamental anticiparse a los potenciales ataques de desinformación identificando principios y valores fundamentales del sistema electoral. Esto incluye desarrollar una narrativa robusta que enfatice la honestidad, la transparencia y el profesionalismo de las instituciones electorales. Definir con precisión las audiencias objetivo, incluyendo no solo detractores, sino también susceptibles, persuasibles y defensores, con el fin de dirigir mensajes efectivos que resuenen adecuadamente en cada grupo.

- **Prepararse:** Crear un equipo de respuesta a la desinformación

Para gestionar eficazmente las crisis de comunicación, se propone la creación de un equipo especializado en respuesta a la desinformación. Este equipo deberá estar equipado con herramientas de alerta rápida para monitorear y evaluar la relevancia de la información desinformativa. Se recomienda establecer un proceso de escalada que clasifique el riesgo de la información según su impacto potencial y su credibilidad ante las audiencias. Además, involucrar a partes interesadas externas como socios internacionales, académicos, partidos políticos, medios de comunicación y líderes comunitarios es fundamental para validar y respaldar las respuestas institucionales.

- **Activar:** Monitorear el entorno de la desinformación

La estrategia implica la activación continua del monitoreo del entorno de desinformación, identificando y contrarrestando narrativas problemáticas de manera oportuna. Los mensajes deben ser precisos, basados en hechos verificables y evitando repetir la desinformación.

Se enfatiza la importancia de mantener una voz institucional verificada que no solo asegure la información correcta, sino que también fortalezca la credibilidad y confianza del público en el proceso electoral.

Además, se proporciona un marco sólido y estructurado para enfrentar las crisis de comunicación durante elecciones, fortaleciendo la confianza ciudadana a través de acciones proactivas y mensajes estratégicos.

La aplicación efectiva de estas medidas puede mitigar el impacto de la desinformación y garantizar la integridad de los procesos electorales.

Finalmente, se recomienda implementar estas estrategias de manera sistemática y continua, actualizando y adaptando las tácticas conforme evoluciona el panorama de la desinformación y las tecnologías digitales.

"La capacitación constante del personal y la colaboración estrecha con todas las partes interesadas son clave para el éxito en la gestión de crisis de comunicación durante elecciones."

MIÉRCOLES 8 DE NOVIEMBRE

9. **Estrategia de comunicación política de prevención de violencia política en razón de género de candidatas en plataformas digitales.**
   Edurne Ochoa, Consultora en comunicación política, perspectiva de género y DDHH, México

Edurne Ochoa, destaca que la ciber violencia política contra las mujeres en razón de género es un fenómeno aún no reconocido adecuadamente en la legislación mexicana, específicamente en la Ley de Acceso para las Mujeres a una Vida Libre de Violencia. Esta forma de violencia se manifiesta en el espacio digital mediante el uso de internet, redes sociales, y tecnologías digitales para perpetuar ataques como intervención, hackeo, espionaje, denostación, persecución, amedrentamiento, entre otros actos que incluyen ciberacoso y difusión no autorizada de imágenes.

Las Tecnologías de la Información y la Comunicación (TIC) son recursos que pueden favorecer el ejercicio de los derechos de las mujeres, pero también pueden contribuir a su desvalorización y deslegitimación. El entorno virtual refleja las relaciones de poder en la sociedad y las prácticas discriminatorias y violentas en múltiples formas. Las mujeres enfrentan un juicio colectivo que cuestiona su capacidad para ocupar espacios de decisión.

Acciones, Recomendaciones y Estrategias

Estrategias de Prevención Digital

1. **Marca registrada:** Es fundamental proteger la identidad digital como medida preventiva.
2. **Doble verificación:** Utilizar correos electrónicos exclusivos y evitar la verificación por SMS ayuda a mantener la seguridad.
3. **Prevención de malware:** No abrir enlaces o archivos de remitentes desconocidos para evitar riesgos de ciberseguridad.
4. **Monitoreo constante:** Revisar periódicamente redes sociales y motores de búsqueda para detectar y manejar contenidos potencialmente dañinos.
5. **Seguridad familiar:** Implementar firewalls y estrategias digitales familiares para fortalecer la protección en línea.

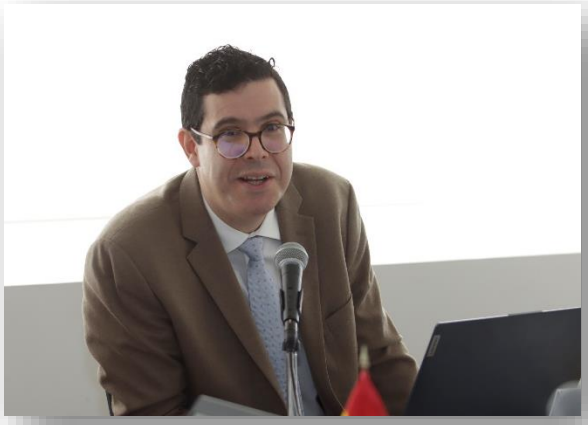
6. **Configuraciones de seguridad avanzadas:** Utilizar funciones como el modo hermético en iOS para aumentar la protección de datos personales.
7. **Gestión de contenido:** Evaluar cuidadosamente los contenidos compartidos en plataformas digitales para evitar riesgos de difamación o acoso.
8. **Conocimiento legal:** Familiarizarse con las leyes pertinentes que aborden la violencia mediática y digital.
9. **Separación de cuentas:** Utilizar cuentas separadas para actividades públicas y privadas.
10. **Red de apoyo:** Mantener una red de apoyo lista para intervenir en caso de incidentes de ciber violencia política.

Estrategias de Contención

1. **Mantener la calma:** Responder de manera calmada y estratégica ante situaciones de crisis en línea.
2. **Documentación de ataques:** Registrar detalladamente los incidentes de ciber violencia política, asegurando la recolección de pruebas.
3. **Gestión de visibilidad:** Controlar la visibilidad de contenidos personales y políticos para minimizar riesgos.
4. **Reporte de cuentas:** Denunciar ante las plataformas pertinentes las cuentas responsables de ataques cibernéticos.
5. **Mediatización controlada:** En casos extremos, considerar la mediación pública para proteger la integridad personal y familiar.
6. **Consulta con expertos:** Buscar asesoramiento especializado en ciberseguridad para identificar y mitigar amenazas en línea.
7. **Redes de apoyo:** Conectar con comunidades de activistas digitales que puedan ofrecer apoyo y solidaridad.
8. **Bienestar personal y familiar:** Priorizar el cuidado de la salud mental y emocional durante situaciones de crisis digital.
9. **Denuncia y visibilización:** No tolerar la ciber violencia política y utilizar los medios disponibles para denunciar públicamente estos actos.
10. **Resistencia al desplazamiento:** Defender el derecho a participar activamente en el espacio público digital sin temor a intimidaciones o exclusiones.

10. Dilemas y alternativas para la regulación de las redes digitales a la luz de principios y valores democráticos.

Gustavo Román, Director General de Estrategia y Gestión Política-Institucional, TSE - Costa Rica



Gustavo Román, Director General de Estrategia y Gestión Política-Institucional del Tribunal Supremo de Elecciones (TSE) de Costa Rica, destacó que el principal dilema que se presenta en la era digital es cómo hacer compatible la libertad de expresión en redes sociales con la protección de otros derechos humanos, cuidando la integridad de los procesos electorales.

En el contexto de las nuevas tecnologías digitales, se identifican cuatro bienes jurídicos esenciales que deben ser protegidos:

1. **Transparencia en la financiación:** Es crucial garantizar que la financiación de las campañas electorales sea transparente. En medios tradicionales, como la prensa escrita, la radio y la televisión, existe la obligación de reportar las tarifas y los gastos de propaganda electoral. Sin embargo, en redes sociales, la falta de regulación impide el acceso a información detallada sobre quién financia la publicidad y cuánto se invierte en ella.
2. **Equidad en la contienda:** Es esencial asegurar que todos los participantes en una contienda electoral tengan igualdad de oportunidades. La equidad debe ser protegida para evitar que actores con mayores recursos económicos tengan una ventaja injusta.
3. **Libertad de expresión:** Aunque es un derecho fundamental, la libertad de expresión debe ser regulada para evitar abusos. Las iniciativas para regular internet han enfrentado resistencia debido al temor de que se limite este derecho. Sin embargo, es necesario equilibrar la libertad de expresión con la protección contra el discurso de odio y la desinformación.
4. **Libertad del voto:** La integridad del voto es esencial para la democracia. La desinformación y la manipulación pueden influir en la toma de decisiones de los electores, lo que pone en riesgo la legitimidad de los resultados electorales.

El ecosistema mediático ha cambiado con la aparición de nuevos actores, como las empresas de plataformas digitales. Estos actores, junto con consultores, influencers y activistas extremistas, deben ser regulados para proteger los procesos electorales y a los ciudadanos de comportamientos que puedan tener consecuencias negativas para la democracia.

Actualmente, existe una brecha significativa entre la práctica de las campañas electorales en entornos digitales y la normativa que las regula. Pocos países tienen legislación específica para la regulación de la publicidad política en línea. Ejemplos de países con avances en este ámbito son Finlandia, Irlanda, España y Canadá. Sin embargo, a nivel global, la regulación es insuficiente.

Ha habido una resistencia sistemática a legislar sobre la regulación de internet debido al discurso de la imposibilidad de regulación y el temor a limitar la libertad de expresión. Sin embargo, es necesario reconocer que siempre existe algún tipo de regulación, y la cuestión es quién establece las reglas. Es fundamental que la regulación sea diseñada para proteger los derechos fundamentales sin coartar la libertad de los usuarios.

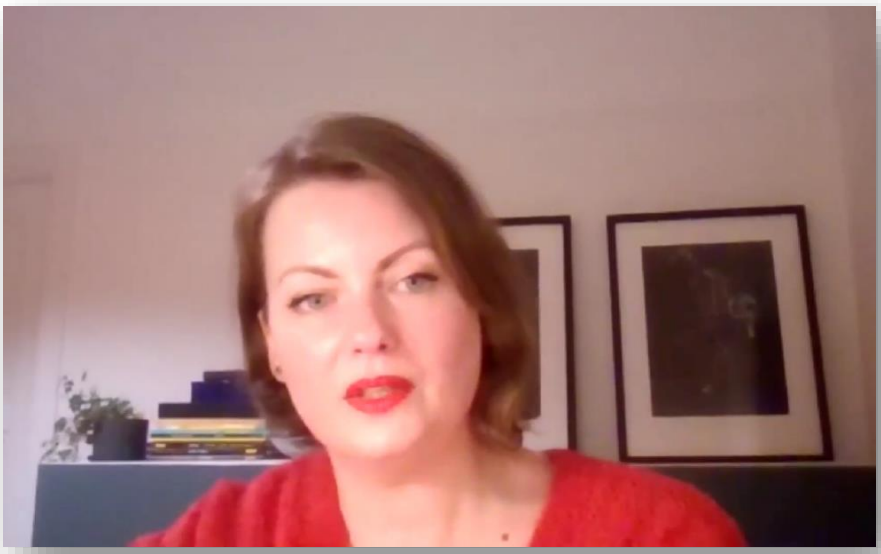
Para avanzar hacia una regulación efectiva, se proponen los siguientes principios y acciones:

- **Intervención mínima en el debate:** La regulación debe interferir lo menos posible en el debate público, evitando la censura arbitraria.
- **Responsabilidad de las plataformas:** Las empresas de plataformas deben ser responsables civilmente por los daños provocados por publicaciones de terceros y deben transparentar los algoritmos utilizados.
- **Co-regulación:** Se debe fomentar la cooperación entre las plataformas digitales y las autoridades electorales, avanzando hacia una co-regulación con rendición de cuentas.
- **Defensa del periodismo:** La prensa libre es esencial para la democracia, y debe protegerse la integridad y libertad de los medios de comunicación.
- **Limitación de la comercialización de datos:** Es necesario limitar la comercialización de datos personales y los resultados de modelos predictivos utilizados por las plataformas.

"Sin confianza en el Proceso Electoral y en la Autoridad que certifica los resultados, no hay estabilidad política ni paz social, y sin estabilidad política ni paz social, no hay libertad electoral."

11. Impacto de la inteligencia artificial en las elecciones.

Ingrid Bicu, Experta Internacional, Rumania



La experta internacional, Ingtid Bicu, refirió a la conceptualización de la Inteligencia Artificial (IA) como la simulación de la inteligencia humana en máquinas programadas para realizar tareas. Implica el desarrollo de algoritmos y programas informáticos que permiten a los sistemas procesar y analizar grandes cantidades de datos. Estos sistemas pueden funcionar de manera autónoma o en colaboración con humanos.

Antes de implementar la IA en el ámbito gubernamental, es crucial evaluar el nivel de preparación de los gobiernos. Según un estudio de Oxford (2022), los elementos a considerar incluyen:

- Visión, gobernanza y ética (regulación y marcos éticos)
- Capacidad digital
- Adaptabilidad
- Madurez
- Capacidad de innovación
- Capital humano
- Infraestructura
- Disponibilidad y representatividad de los datos

La IA presenta varios desafíos en el contexto electoral, tales como:

- **Deepfakes**: Imágenes y videos falsificados que parecen reales.
- **Suplantación de sitios web oficiales**
- **Phishing**: Intentos de obtener información confidencial a través de correos electrónicos fraudulentos.

Entender la dimensión de cada amenaza es vital para asignar los recursos adecuadamente y establecer las protecciones necesarias.

Perspectiva Feminista sobre el Impacto de la IA

Desde una perspectiva feminista, la IA puede perpetuar y amplificar los sesgos y desigualdades de género, especialmente si los sistemas están entrenados con datos sesgados. Las mujeres pueden enfrentar desafíos adicionales, como la creación de deepfakes con contenido sexual que explotan prejuicios de género y violencia psicológica. Esta información puede ser utilizada para campañas de difamación, acoso o chantaje.

Para contrarrestar estos efectos, se promueve la IA feminista, que busca desarrollar sistemas sensibles al género y otras identidades sociales, basados en principios y valores feministas para promover la justicia e igualdad.

Países como Canadá, Francia, Finlandia, Australia, México, Suecia, Reino Unido y Nueva Zelanda han avanzado en la adopción de buenas prácticas en materia de IA feminista y enfoques gubernamentales inclusivos.

Recomendaciones

- Facilitar la implementación (con marco legal e infraestructura)
- Garantizar la accesibilidad, inclusión y rendición de cuentas
- Ética y seguridad para todas las personas

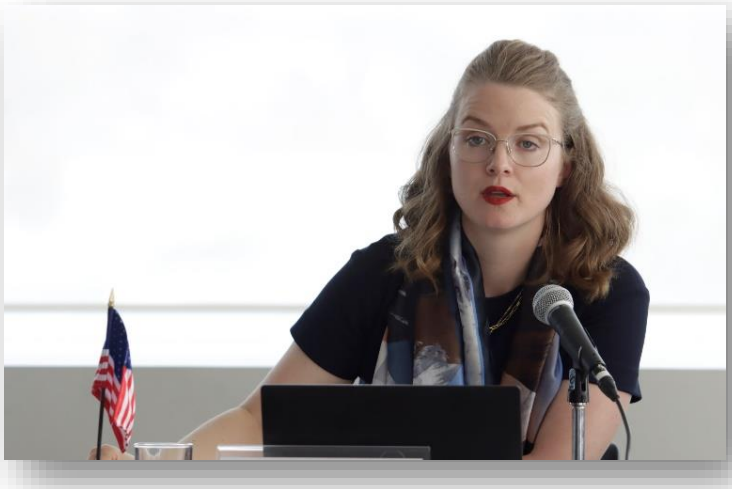
Medidas a Considerar

Para mitigar los desafíos asociados a la IA en el ámbito gubernamental, se deben considerar las siguientes medidas:

- Desarrollo y uso ético de la IA.
- Crear conciencia sobre sus implicaciones.
- Mantener el papel decisivo de los humanos en los procesos.
- Establecer marcos legales flexibles que fomenten la innovación.
- Promover un enfoque colaborativo entre desarrolladores, actores estatales, investigadores y la comunidad internacional.
- Ciberseguridad mejorada

12. Impacto de la inteligencia artificial en las elecciones.

Lisa Reppell, Oficial Superior de Investigación, IFES – Estados Unidos de América



"Por IA nos referimos al aprendizaje automático, aprendizaje avanzado y modelos lingüísticos extensos."

Lisa Reppell señaló que la IA puede ser utilizada en la toma de decisiones automatizada, implementando modelos de aprendizaje avanzado para clasificar y generar información.

Los modelos de aprendizaje avanzado, o técnicas de discriminación de la información que hace la IA, se dividen en:

- **Técnica Selectiva (Clasificación):** Utilizada para clasificar positivamente o negativamente publicaciones, juzgar datos y clasificar gastos financieros.
- **Técnica Generativa (Creación):** Utilizada para predecir resultados, describir información de manera accesible y ayudar a personas con limitadas habilidades tecnológicas.

Ejemplos en el Campo Electoral

1. **Clasificación:** La IA puede sugerir dónde colocar mesas de votación para optimizar el flujo de votantes. Es crucial considerar la calidad de los datos, la posibilidad de sesgos y la transparencia en el proceso.
2. **Generación:** La IA puede redactar materiales de capacitación acorde a la normativa, aunque es importante considerar la posible inexactitud y las "alucinaciones" del modelo, así como el riesgo de uso indebido.

IA Generativa y Publicidad Política

La IA generativa puede ser usada en campañas electorales para:

- Crear publicidad política.
- Generar avatares de candidatos y chatbots.
- Producir audios falsos y noticias creadas por agentes extranjeros malignos.

Riesgos Asociados al Uso de la IA en el Ámbito Electoral

Desinformación y Fake News

Los riesgos a corto plazo incluyen:

- Incremento de fake news y contenido más creíble.
- Personalización de la desinformación usando datos personales.
- Desconfianza generalizada en la información, incluyendo la veraz.

Los organismos de gestión electoral deben adaptar sus técnicas y estrategias para combatir la desinformación utilizando herramientas de IA. Las mismas herramientas que se utilizan para combatir la desinformación pueden ser reconfiguradas para responder a las nuevas amenazas.

La IA generativa podría ser útil para:

- Acelerar tareas repetitivas.
- Preparar respuestas rápidas.
- Colaborar en tareas creativas.
- Resumir y categorizar información.
- Realizar tareas de bajo riesgo que pueden ser revisadas por un humano.

El método M.A.S.T.E.R. es una guía para enseñar a la IA a redactar boletines de prensa en caso de crisis:

- **M:** Marcado (actuar acorde a un material de partida).
- **A:** Aportar contexto.
- **S:** Suministrar criterios concretos.
- **T:** Transformar instrucciones en acciones.
- **E:** Ejecutar y regenerar (repetir si no es perfecto).
- **R:** Revisar por un humano.

Es esencial establecer principios y normas internas para el uso de la IA, asegurando siempre la revisión por un humano.

JUEVES 9 DE NOVIEMBRE

13. Reporte Global: ciberataques en los procesos electorales.

Alberto Fernández, Jefe del Programa de Digitalización y Democracia, IDEA Internacional, Suecia

Alberto Fernández, en su exposición, destacó que la ciberseguridad es un tema complejo y crucial, especialmente debido al surgimiento de nuevas vulnerabilidades derivadas de la digitalización. Resaltó la existencia de tratados internacionales como el Convenio sobre la Ciberdelincuencia de Budapest, que buscan abordar estos desafíos.

¿Qué es un ciberataque?

Un ciberataque es un intento de robar, exponer, alterar, desactivar o destruir información o la función de un sistema digital. Entre los tipos más comunes de ataques se encuentran:

- **DDoS (denegación de servicio distribuido):** Sobrecarga los servidores para hacer un servicio inaccesible.
- **Malware:** Incluye virus, troyanos y ransomware, propagados a través de sitios web infectados o software malicioso.
- **Ataque de "hombre en el medio" (MiTM):** El hacker intercepta la comunicación entre dos partes.
- **SQL Injections:** Inserta código SQL en una aplicación web para alterar bases de datos.
- **Zero-day attack:** Aprovecha vulnerabilidades desconocidas por los desarrolladores.
- **XSS (Cross-Site Scripting):** Inserta código malicioso en sitios web legítimos.
- **Phishing:** Utiliza correos electrónicos o llamadas para obtener contraseñas o datos confidenciales.
- **Desinformación:** Usa redes digitales para alterar la información.
- **Combinación de varias técnicas.**

Objetivos de un Ciberataque en un Proceso Electoral:

- Alterar los resultados.
- Modificar la opinión pública.

- Dificultar la votación.
- Deslegitimar los resultados.
- Provocar la repetición de las elecciones.

Vulnerabilidades en un Proceso Electoral:

- **Infraestructura:** Cualquier dispositivo conectado es susceptible a ataques.
- **Software:** Hay un mercado de vulnerabilidades y expertos que las buscan y venden.
- **Cadena de Suministro:** Es crucial prestar atención a la procedencia de los componentes y proveedores.
- **Factor Humano:** La falta de cumplimiento de directrices de ciberseguridad por parte de una sola persona puede comprometer todo el sistema.
- **Físicas:** Protección insuficiente de hardware y software.
- **Información:** Campañas de desinformación y baja calidad en medios de comunicación.
- **Legales:** Políticas ambiguas y desactualizadas, y marcos legales que no abordan adecuadamente las necesidades de ciberseguridad.
- **Operacionales:** Los sistemas electorales deben ser resistentes a interrupciones y contar con planes de recuperación de datos.

Medidas de Ciberseguridad recomendadas:

1. Reducir vulnerabilidades tanto como sea posible, evitando la digitalización innecesaria.
2. Crear un plan de defensa cibernética integral.
3. Abordar todas las etapas del ciclo electoral.
4. Proveer formación continua en ciberseguridad para el personal electoral.
5. Incrementar la cantidad de talento especializado en ciberseguridad.
6. Fomentar la colaboración entre agencias para una defensa integral.

Durante la sesión de intercambio, se reafirmaron las medidas de ciberseguridad propuestas y se discutieron ejemplos de ataques a nivel internacional. Destacó que las impresoras son unos de los puntos más débiles en ciberseguridad en cuanto a robo de información.

14. Identificación y rastreo de ciberataques

Carlos Estrada, experto nacional, México

"El combate a la criminalidad cibernética requiere colaboración de triple hélice que involucre a empresas, universidades y gobierno."

Carlos Estrada presentó una serie de puntos críticos respecto a la identificación y rastreo de ciberataques. Su enfoque se centró en la necesidad de colaboración y la adopción de medidas éticas y apartidistas en la lucha contra la criminalidad cibernética.

Diseñó un tablero de control interactivo para que los participantes pudieran acceder a información y enlaces diversos desde sus dispositivos.

Acuerdos iniciales fundamentales para el trabajo en ciberseguridad:

1. Ser agnóstico con las empresas de tecnología.
2. Mantener una postura apartidista.
3. Contar con un perfil ético.

México cuenta oficialmente con sólo 10 peritos de cómputo forense en el poder judicial, especializados en la caza de hackers. Según el índice de ciberdefensa de Naciones Unidas, México no figura entre los primeros 50 países, lo que pone de manifiesto la urgencia de mejorar sus capacidades en esta área.

De cara al 2030, se prevé una militarización creciente de los ciberataques. Una de las principales preocupaciones de la Organización de los Estados Americanos (OEA) es la interferencia híbrida en los procesos electorales. Por ello, es crucial que las naciones se interesen en cursos de conflictividad social para monitorear estos riesgos, especialmente ante actores internacionales con financiamiento significativo.

Somos embajadores del metaverso y un día en internet equivale a 30 días de la vida real, cada 6 horas hay que actualizarse sobre los nuevos ataques, herramientas y reportes.

- ¿Qué están viendo los hackers que nosotros no estamos viendo?
- ¿A qué nos estamos enfrentando y cómo podemos protegernos?

Se destacó la oferta de una certificación gratuita de Google en ciberseguridad, así como la mención de varias comunidades en América Latina dedicadas a este tema. Estrada también alertó sobre la venta de bases de datos electorales de diferentes países en foros de la red oscura, foros que cambian de dueños cada cuatro meses debido a las acciones del FBI.

15. Taller
    Carlos Estrada, experto nacional, México

Herramientas de protección o ciberseguridad

1. Lo primero es usar un buen explorador. BRAVE Y LIBREWOLF que bloqueé los intentos de robo incluso de la sesión.
2. La VPN protege al dispositivo o computadora protonVPN.com
    - Una de las ventajas de la VPN es que puede seleccionar una ubicación diferente
    - Hay un falso sentido de seguridad sobre el doble factor de autenticación.

Hay páginas que se roban el poder de procesamiento de la computadora y/ o inician una cadena de ataque. En América Latina es donde más se usa el software de espionaje y muchas veces el vector de ataque es el buzón de voz porque las empresas de telefonía en la región dan niveles más bajos de protección a sus usuarios, por ejemplo, las claves del buzón de voz son de solo 4 dígitos y esa clave se rompe en un minuto y medio.

Se mencionó el célebre caso del programa Pegasus usado en México, dicho software fue desarrollado por personal egresado de la unidad de hackers de élite de Israel (una APT). Pegasus uno de más de 35 programas de hackeo en su tipo que emplea metodología militar que se llama modelo diamante. Hay alrededor de 12 grupos de cibercriminales que utilizan herramientas contra funcionarios públicos y población civil. Se emplean herramientas o programas que se diseñaron para uso militar o policiaco, pero en la región de AL se venden al mejor postor, que resulta ser el crimen organizado.

Se recomendó escanear el celular para ver si está intervenido con la Aplicación CERTO, la App hace un escaneo preliminar para ver que no tenga instalado un programa malicioso que filtre información App desarrollada en Stanford y es usada por el ejército de Estados Unidos.

Se mencionó que la popular aplicación de mensajería “WhatsApp” no es segura porque no ofrece cifrado punto a punto.

Hay gobernadores, funcionarios y empresarios que realizan medidas de contrainteligencia electrónica porque una medida de seguridad es una investigación de contrainteligencia electrónica. En México algunas personas crean páginas de internet falsas con información personal solo para saber quiénes los están investigando.

En la región grupos del crimen organizado tienen la capacidad en tiempo real para conocer la dirección IP, el número de teléfono al que está direccionado y rastrear en tiempo real la geolocalización.

Las bases de datos de los votantes es uno de los activos más importante de nuestros países. Oracle vende el principal cifrado para bases de datos en América Latina tiene hasta 9 capas de protección para evitar el envenenamiento de los datos.

Medidas de protección para detener y monitorear fugas de información

Uno de los primeros niveles para monitorear y detener en tiempo real la fuga de información es el cifrado, es decir, cómo encriptamos la información. **VeraCrypt**: Es el principal programa gratuito de cifrado.

Si bien con GPT hay mucha fuga de información, también es una herramienta valiosa porque en GPT se puede hace que nos dé el código en Python prescindiendo de conocimientos en dicho lenguaje de programación.

Carlos Estrada mencionó que las Deepfakes son la manipulación de fotos, videos y voz mediante Inteligencia Artificial

Cifrado de discos de trabajo

Regla 3-2-1**:** Hay tres criterios para proteger las la información confidencial personal o de la institución más importante.

1. Tener al menos 3 copias de seguridad de respaldo en unidades de disco externas
2. La información en las unidades de disco externas debe estar cifrada
3. Que las unidades de disco externas estén en otra ubicación física

Carlos Estrada mencionó algunas herramientas de ciberseguridad entre las que destacan VirusTotal y SandBox. El primero es el principal compendio de análisis de virus del mundo y es propiedad de Google, con VirusTotal se puede analizar la “cadena de ataque” (tipo de ataque, origen y el virus). El segundo, SandBox nos muestra que va a pasar al subir un archivo.

El Malware polimórfico cambia su código fuente cada 5 minutos. Los niveles de antivirus más elevados funcionan contra el malware polimórfico porque se basan en machine learning. El mejor antivirus del mundo es Kaspersky de origen ruso, el resto de los antivirus con buen desempeño también se basan en inteligencia artificial (machine learning)

Niveles de protección

1. Antivirus/Antimalware (Kaspersky)
2. Respaldos cifrados (VeraCrypt)
3. FireWall en dispositivo (ZoneAlarm)
4. Virtual Private Network (ProtonVPN)
5. Navegación cifrada (Brave, TOR)
6. Borrado profundo (Ccleaner)
7. Chat cifrado "end-to-end" (Wickr)

8. Múltiple Autenticación (USB, SMS, App Autenticación)
9. Telefonía VoIP (Skype)
10. Celular foráneo (Verizon, Sprint, etc)
11. Cifrado de arranque (Bitlocker)
12. Sandbox para archivos (Any.run)
13. Sistema operativo virtual (VMware)
14. Endpoint Detection and Response (EDR): Única manera de ver si hay intromisión de un hacker

Privacidad y protección de datos

Se recomendó el uso de un dispositivo llave de seguridad con el que la cuenta de email o el celular solo se abre si se introduce la llave de seguridad. Se recomendó el Programa Data Loss Prevention DLP que protege las bases de datos, detecta en tiempo real la extracción de información.

Se destacaron los procesos de transformación digital de automatización, migración a la nube, trabajo remoto, experiencia del usuario, ciencia de datos e internet de las cosas. Hay activos que no están en la lista de sistemas, pero interactúan con la organización como la computadora personal y el teléfono celular de los empleados. Se sugirió el uso de contraseñas robustas.

Las APT son células de hackers de élite de los ejércitos del mundo, compuestas por militares entrenados cibernéticamente para fines de guerra en función de los intereses geopolíticos. También atacan a la población civil con armas de ciberguerra.

El experto recomendó la búsqueda de direcciones IP y páginas para hacer el escaneo y revisar el grado de vulnerabilidad de una organización.

16. Colaboración sobre Ciberseguridad con países de América Latina.

Carlos Leonardo, Director del Equipo de Respuesta a Incidentes Cibernéticos, CSIRT- República Dominicana

¿Qué se entiende por ciberseguridad?

La protección de la integridad de la información, de la confidencialidad de la información y de la disponibilidad de esa información.

"Se requiere establecer una política pública en materia de ciberseguridad"

En los últimos años varios Estados, varias organizaciones han sido afectadas por incidentes cibernéticos que no únicamente sacan servicios de línea.

La otra razón por la que se habla de ciberseguridad es porque a nivel mundial los organismos internacionales ya lo consideran como uno de los principales riesgos a enfrentar. De hecho, la falla de ciberseguridad en los incidentes de ciberseguridad ocupa el riesgo número 7 en ese ranking de los 10 principales riesgos, de acuerdo con el informe del Foro Económico Mundial.

En materia de voto electrónico la agenda digital es la carta de ruta de cómo se quiere llevar a cabo la transformación digital en cada uno de los Estados, incluyendo todos los diferentes componentes, desde el establecimiento de los Marcos normativos.

¿Qué se necesita específicamente para hablar sobre temas de ciberseguridad?

En primer lugar, para disminuir el riesgo, la prevención es mucho menos costosa que la respuesta. La ciberseguridad se observa de una manera más preventiva y proactiva, más que reactiva.

Los Estados, al momento de desarrollar estrategias nacionales de ciberseguridad, ya no lo hacen a puerta cerradas, ya se hacen trayendo a bordo al sector privado, a la sociedad civil, al sector académico, al sector público y a los organismos internacionales.

Hoy en día se cuenta con muy buenas unidades de investigación de delitos cibernéticos distribuidas en la región, pero la judicialización o llevar a cabo hasta el final los procesos de investigación se hace muy difícil, primero con la volatilidad de la evidencia electrónica y segundo, no existen marcos legales homologados que permitan la evidencia electrónica.

Es necesaria la cooperación con organismos internacionales que permiten asistencia técnica, y asistencia en la generación de capacidades para aumentar esas competencias, no solamente respuesta, sino de prevención en materia de ciberseguridad.

Cuatro formas en la que los líderes pueden activar la resiliencia

1. Cooperación internacional y la respuesta oportuna
2. Ubicación distribuida de los datos
3. Establecer marcos legales para poder ejecutar la operación
4. Herramientas de cooperación internacional

En materia de cooperación internacional se cuenta con el Foro Global de Expertise Cibernética y el Convenio sobre la Ciberdelincuencia o Convenio de Budapest, ello con la finalidad de aumentar las competencias en materia de ciberseguridad de todos los países de la región.

"La ingeniería social seguirá siendo el vector de ataque más utilizado y por excelencia de los atacantes porque los usuarios son la primera línea de defensa."

17. Buenas prácticas

Estrategia de comunicación de contenidos.

A continuación, se presenta un análisis comparado de las mejores prácticas en estrategias de comunicación de contenidos utilizadas por las autoridades electorales de Bolivia, Paraguay, Ecuador, Costa Rica, Perú y República Dominicana.

1. Tribunal Supremo Electoral (TSE) de Bolivia

Estrategia:

- **Elementos Fundamentales:** Seguridad, imparcialidad y confianza.
- **Objetivos:** Generar confianza en el voto con bioseguridad y transparencia.
- **Fases de Estrategia:**
  - Promoción del voto con bioseguridad.
  - Pedagogía del voto y participación de jurados electorales.
  - Motivación del voto como mecanismo de reconciliación nacional.
  - Medidas de seguridad en el proceso electoral.
- **Alianzas:** Bolivia Verifica y Chequea Bolivia para combatir la desinformación y prevenir la violencia de género.

2. Tribunal Superior de Justicia Electoral (TSJE) de Paraguay

Estrategia:

- **Campaña:** "Voto informado" para garantizar la integridad del proceso electoral.
- **Acciones:**
  - Captar el interés ciudadano sobre la importancia de las elecciones.
  - Generar y difundir contenidos institucionales en medios masivos.
  - Campañas de concienciación cívica a través de materiales audiovisuales y redes sociales.

3. Tribunal Contencioso Electoral (TCE) de Ecuador

Estrategia:

- **Uso de Redes Sociales:**
  - Implementación de hashtags y contenido gráfico llamativo.
  - Enlaces a información adicional en la página web.
- **Capacitaciones en Línea:** Para asegurar el acceso a información sobre las funciones del Tribunal.
- **Monitoreo de Redes Sociales:** Informes para evaluar crisis potenciales y determinar acciones correctivas.

4. Tribunal Supremo de Elecciones (TSE) de Costa Rica

Estrategia:

- **Evaluación Post-Electoral:**
  - Evaluaciones para anticipar y mejorar procesos futuros.
  - Base de datos para cruzar información y entender la imagen del TSE.

- **Proceso de Mejora Continua:** Identificación de necesidades, investigación, formación, práctica y apoyo interinstitucional.
- **Monitoreo Permanente:** Desarrollo de un área para monitorear información en tiempo real.

5. Registro Nacional de Identificación y Estado Civil (RENIEC) de Perú

Estrategia:

- **Campañas de Actualización del Padrón:**
  - Campaña "El padrón lo hacemos todos" para actualizar DNI y reportar fallecimientos.
  - Utilización de celebridades e instituciones para amplificar el alcance.
- **Evaluación de Impacto:** Estudios post-campaña para medir el impacto y mejorar la imagen de RENIEC.

6. Junta Central Electoral (JCE) de República Dominicana

Estrategia:

- **Plan Estratégico 2020-2024:** Aumentar la confianza ciudadana y mejorar la comunicación.
- **Transparencia y Oportunidad:** Difusión oportuna de información a la sociedad.
- **Política de Comunicación Institucional:** Mejorar el intercambio de información interno y externo.
- **Estrategias de Comunicación:** Visibilización, sensibilización, gestión de crisis y comunicación interna y de servicio.
- **Manual de Desinformación:** Herramientas para enfrentar la desinformación en el proceso electoral.

Conclusión

Las estrategias de comunicación de contenidos de las autoridades electorales en los países mencionados comparten varios elementos clave como la transparencia, la imparcialidad, y la confianza. Sin embargo, cada país adapta estos principios a sus contextos específicos:

- **Bolivia** se enfoca en generar confianza en un entorno de alta polarización y post-pandemia.
- **Paraguay** enfatiza la educación del votante mediante el uso de tecnología electoral.
- **Ecuador** y **Costa Rica** priorizan el uso de redes sociales y la evaluación post-electoral, respectivamente.
- **Perú** utiliza campañas amplificadas por figuras públicas para actualizar el padrón electoral.
- **República Dominicana** se concentra en estrategias de visibilización y manejo de desinformación.

PARTICIPANTES

Marcio Mario Ortiz Sejas. *Responsable de Comunicación del Tribunal Supremo Electoral de Bolivia*

Dolly Ruiz Diaz Olmedo. *Directora de Difusión Técnica de Planes y Proyectos Electorales del Tribunal Superior de Justicia Electoral de Paraguay.*

Francis del Pilar Salas Sola. *Analista de Comunicación del Tribunal Contencioso Electoral de Ecuador*

Ingrid Paola Chaves Mora. *Profesional en Tecnologías de Información del Tribunal Supremo de Elecciones de Costa Rica.*

Jaime Alejandro Honores Coronado. *Jefe de la Oficina de Tecnologías de la Información*

Suedi León Jiménez. *Directora de Comunicaciones de la Junta Central Electoral de República Dominicana.*

A continuación, se presentan las buenas prácticas aplicadas sobre el uso de la inteligencia artificial por las autoridades electorales de México y El Salvador.

Uso de la inteligencia artificial para transparencia e información a la ciudadanía. INE – México

***Oscar Ruíz De Jesús**. Jefe de Departamento de Procesamiento de Estadísticas Electorales de la Dirección Ejecutiva de Organización Electoral*

Desarrollos y Aplicaciones de IA:

- **VotoBot:** Asistente virtual especializado en resultados electorales.
- **Ética en la IA:** Transparencia en la interacción ciudadana con el asistente virtual.
- **Privacidad:** Recopilación mínima de datos para fines estadísticos.
- **Seguridad:** Asociaciones para preservar la integridad del contenido y evitar accesos no autorizados.
- **Respuestas apropiadas:** Manejo de preguntas inapropiadas con respuestas políticamente correctas.
- **Casos de Uso:** Identificación de frases clave, vinculación de entidades y análisis de sentimiento en textos.
- **Plataforma en la Nube:** Gestión y almacenamiento de datos accesibles globalmente.
- **Mejora Continua:** Incorporación de servicios AI para predecir significados textuales y mejorar la accesibilidad.

El INE enfoca su uso de la IA en proporcionar información precisa y accesible sobre los resultados electorales, asegurando la privacidad y la ética en su implementación. La mejora continua y la seguridad del sistema son prioritarias, reforzando la confianza del público en la transparencia del proceso electoral.

Uso de la Inteligencia Artificial (IA) para mayor vinculación con la ciudadanía y para transparencia sobre estadísticas electorales. TSE - El Salvador

Mauricio Villagrán. Jefe de Comunicaciones del Tribunal Supremo Electoral

Desarrollos y Aplicaciones de IA:

- **Comunicación con Electores:** Chatbots y asistentes virtuales para información electoral.
- **Personalización de Mensajes:** Uso de IA para mensajes personalizados y generación de contenido para redes sociales.
- **Expresiones de Animación:** Creación de avatares animados con IA.
- **Análisis de Redes Sociales y Sentimiento:** Monitoreo y análisis de conversaciones y sentimientos en redes sociales.
- **Segmentación de la Población:** Estrategias de campaña personalizadas basadas en segmentación de votantes.
- **Seguridad Cibernética:** Uso de machine learning para detectar comportamientos sospechosos y reconocimiento facial para votación remota.

El TSE emplea la IA para mejorar la comunicación electoral y la personalización de mensajes, promoviendo una mayor participación y eficacia en la difusión de información. La seguridad cibernética es una prioridad, aplicando tecnologías avanzadas para proteger el proceso electoral, especialmente para votantes en el extranjero.

A continuación, se presenta un análisis comparado de las estrategias de ciberseguridad aplicadas por los organismos electorales de Perú, Honduras y Ecuador, resaltando sus prácticas, desafíos y resultados.

Fortaleciendo la Confianza Electoral: estrategias y resultados en Ciberseguridad. ONPE Perú

Roberto Montenegro de la Oficina Nacional de Procesos Electorales de Perú.

Contexto y Problemática:

- **Sistema Electoral Peruano:** Conformado por el Jurado Nacional de Elecciones, Registro Nacional de Identificación y Estado Civil, y ONPE.
- **Aumento de Amenazas:** Exponencial incremento de amenazas cibernéticas, destacando ataques como Ransomware, DDoS, Malware y Phishing.

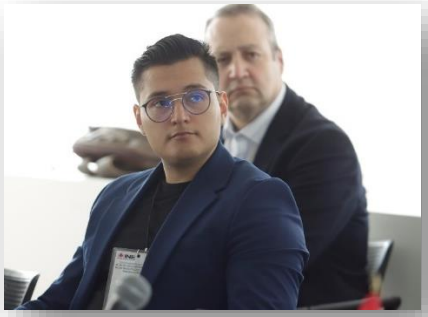
Estrategias de Ciberseguridad:

1. **Implementación del Modelo NIST:** La ONPE aplica un modelo de ciberseguridad basado en cinco etapas:
    - Identificar activos y riesgos.
    - Protección y defensa tecnológica.
    - Detección de vulnerabilidades y monitoreo de actividades maliciosas.
    - Respuesta a incidentes.
    - Recuperación de sistemas afectados.
2. **Uso de estándares internacionales:** Implementación de ISO 27001:2024 e ISO 12207:2016 para la seguridad de la información y el desarrollo del software.
3. **Centro de Operaciones de Seguridad (SOC) y Red (NOC):** Monitoreo continuo de incidencias y respuesta rápida a incidentes.

Resultados:

- Mayor confianza en los procesos electorales debido a la inversión en ciberseguridad.
- Mejora de la infraestructura tecnológica y adopción de una cultura de ciberseguridad.

Mecanismos de prevención contra ciber ataques y mecanismos de respuesta. CNE- Honduras
Wenceslao Flores del Consejo Nacional Electoral



Contexto y Problemática:

- **Nueva Entidad:** Creada en 2019, enfrentó la elección general de 2021 con la implementación de dispositivos biométricos.
- **Ataques Cibernéticos:** Reporte de ataques DDoS y uso de bots maliciosos.

Estrategias de Ciberseguridad:

1. **Contratación de servicios externos de ciberseguridad:** Utilización de Akamai Connected Cloud, Akamai App, y API Protector para proteger contra amenazas.
2. **Medidas Implementadas:** Bloqueo de IPs maliciosas y manejo de errores 503 durante ataques.

Resultados:

- La preparación y evaluación previa son esenciales para la efectividad de los perfiles de seguridad.
- Necesidad de más tiempo y acceso para evaluar y preparar perfiles de seguridad.

Ataque cibernético a voto por internet. CNE Ecuador

Desinformación sobre Voto Telemático y Ataques cibernéticos
Lucy Pomboza de la Coordinación Nacional de Seguridad Informática y Proyectos Tecnológicos Electorales del Consejo Nacional Electoral de Ecuador

Contexto y Problemática:

- **Organización Electoral:** Formada por el CNE y el Tribunal Contencioso Electoral.
- **Desafíos:** Organización de elecciones generales anticipadas y manejo de voto telemático.

Estrategias:

1. **Desarrollo interno de sistemas informáticos:** Aproximadamente 60 desarrolladores y una infraestructura tecnológica sólida.
2. **Contratación de empresa para votación telemática:** Aunque enfrentaron problemas, esta estrategia demostró la flexibilidad para adaptarse a nuevas tecnologías.
3. **Combate a la desinformación:** Talleres, reuniones, entrevistas y uso de múltiples canales de comunicación para garantizar la transparencia.

Resultados:

- La transparencia y la comunicación efectiva son claves para mitigar el impacto de ataques cibernéticos.
- La colaboración con medios y la diversificación de canales de publicación de resultados son estrategias efectivas.

Coincidencias en las actividades de ciberseguridad:

1. **Implementación de estándares y marcos internacionales:**
    - Perú utiliza ISO 27001 y NIST.
    - Honduras y Ecuador también adoptan prácticas basadas en estándares internacionales reconocidos.
2. **Monitoreo y respuesta a incidentes:**
    - Los tres países tienen estrategias para monitorear continuamente y responder rápidamente a incidentes de ciberseguridad.
    - Uso de SOCs y NOCs en Perú.
    - Contratación de servicios externos en Honduras y Ecuador.
3. **Colaboración y contratación de servicios especializados:**
    - Honduras y Ecuador han mostrado una tendencia a contratar servicios externos para fortalecer su ciberseguridad.
    - Perú colabora con el Centro Nacional de Seguridad Digital.
4. **Enfoque en la capacitación y sensibilización:**
    - Ecuador enfatiza la capacitación y sensibilización para combatir la desinformación.
    - Perú promueve una cultura de ciberseguridad dentro de la ONPE.

18. CONCLUSIONES

Por Arlene Cabral, Coordinadora de Asuntos Internacionales, INE – México

1. Se conocieron las experiencias, buenas prácticas y desafíos de 10 países (Incluyendo a México) y se destacó la importancia del uso de plataformas de inteligencia artificial para propósitos benéficos para la autoridad electoral, siendo que éstas pueden ser instrumentos para brindar certeza y fortalecer el contacto con la ciudadana.

2. En el contexto internacional, existen elementos que buscan influir en el imaginario colectivo a través de los ataques cibernéticos. Uno de los principales objetivos es generar caos.

3. En un contexto donde la desinformación es un elemento persistente en el ciclo electoral, las autoridades electorales deben considerar estrategias con soluciones y respuestas rápidas y efectivas. El tiempo puede ser el gran aliado de las autoridades electorales

4. Ante la laxa o inexistente legislación sobre la materia el papel de la autoridad para lograr equidad y promover los valores democráticos se vuelve un factor determinante.

5. Es necesario brindar justificación legal o normativa a las actividades emprendidas por la autoridad electoral para mitigar la desinformación y monitorear discursos.

6. Se debe de considerar construir una ciberseguridad ciudadana, no sólo a nivel institucional.

7. Lamentablemente, los ciberataques hacia las mujeres evidencian como este género es más propenso a sufrir ataques que afectan la vida privada, que el de los hombres.

8. Respecto al tema de estrategia de comunicación política de prevención contra la VPRG de candidatas en plataformas digitales, se puede destacar la necesidad de ampliar la cartera de delitos digitales y estar conscientes del impacto que éstos tienen, ya que los ciberataques pueden llegar a comprometer la salud mental de la persona afectada, así como su entorno privado y comprometer su seguridad o la de su familia.

9. Establecer grupos de trabajo multidisciplinarios dentro de las instituciones para generar procesos y procedimientos que desemboquen en el establecimiento de prácticas de monitoreo de medios digitales y redes sociales.

10. Si conocemos las amenazas, es más fácil establecer los controles.

11. La planeación no debe enfocarse solamente en contrarrestar una crisis, debe enfocarse principalmente en prevenirla.

12. Los ciber ataques profesionales no atacan los sistemas, atacan a las personas, por eso hay que enfatizar la capacitación a los usuarios.

13. Las crisis no avisan, debemos tener un plan de respuesta para una crisis potencial, basados en la experiencia de nuestro entorno.

14. La cooperación internacional para la profesionalización, actualización y la protección es fundamental, ya que al compartir experiencias y herramientas nos fortalecemos.