OEA
Más derechos para más gente

Consideraciones de Ciberseguridad del proceso democrático para América Latina y el Caribe

Consideraciones de Ciberseguridad del proceso democrático para América Latina y el Caribe

Preparado y publicado por el Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo (cybersecurity@oas.org).

Los contenidos expresados en este documento se presentan exclusivamente con fines informativos y no representan la opinión oficial o la posición de la Organización de los Estados Americanos, su Secretaría General o sus Estados Miembros.

Esta publicación ha sido posible gracias al apoyo financiero de UKFCO.

Agradecemos su interés en esta guía. El Gobierno del Reino Unido desea comprender mejor el impacto que tienen los proyectos que financia y si han logrado los resultados deseados. Sus comentarios sobre cómo usted ha utilizado esta guía y si le ha ayudado a mejorar la respuesta a incidentes de ciberseguridad serán información valiosa que podremos usar para ayudar a diseñar proyectos futuros.

Por favor comuníquese con la Oficina de Asuntos Exteriores y de la Mancomunidad en CyberCapacity.Building@fco.gov.uk para compartir sus comentarios.

OEA | Más derechos para más gente

Foreign & Commonwealth Office

Consideraciones de **Ciberseguridad**

del **proceso democrático** para **América Latina** y el **Caribe**

Créditos

Luis Almagro
Secretario General
Organización de los Estados Americanos

Farah Diva Urrutia
Secretaria de Seguridad Multidimensional
Organización de los Estados Americanos

Francisco Guerrero Aguirre
Secretario para el Fortalecimiento de la Democracia

Equipo Técnico de la OEA
Gerardo de Icaza
Alison August-Treppel
Brenda Santamaría
Cristóbal Fernández
Yerutí Méndez
Alex Bravo
Belisario Contreras
Kerry-Ann Barrett
Rolando Ramírez

Equipo Consultor
Lara Pace
David Marcos

Esta guía fue desarrollada por el Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo de la Secretaría de Seguridad Multidimensional, con el apoyo y la colaboración de la Secretaría para el Fortalecimiento de la Democracia y la revisión y aportes de la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos.

Tabla de Contenido

Tabla de contenido

Prólogo

En una era donde la tecnología converge con la vida cotidiana, el tejido mismo de una sociedad digital estable requiere la protección de las redes y dispositivos que soportan los procesos democráticos. Incluso los países que usan tecnología limitada al realizar sus elecciones enfrentan riesgos cibernéticos para la integridad electoral. Este tema requiere una seria consideración incluso en esas circunstancias limitadas. Uno de los procesos democráticos más visibles es el ciclo electoral. Hasta hace poco, el debate sobre la ciberseguridad y el ciclo electoral se centraba principalmente en la votación electrónica y la transmisión de resultados preliminares: los países con procesos electorales en papel se consideraban, en gran medida, libres del riesgo de ciberataque. Sin embargo, las tecnologías que se utiliza en las elecciones cambian potencialmente con cada ciclo electoral, al igual que los adversarios y sus herramientas.

En el nivel más básico, el uso de la tecnología en las elecciones implica el registro de votantes, partidos y candidatos, así como de sitios web de los Organismos de Gestión Electoral (OGE). La conexión de estos sistemas a Internet los vuelve más vulnerables a los ataques de ciberseguridad. Si no están asegurados adecuadamente, se convierten en objetivos fáciles y se utilizan como una herramienta para cuestionar la validez de partes del proceso electoral o incluso la elección misma en algunos casos. Es fundamental garantizar la confianza de la ciudadanía para lograr mantener la seguridad pública en el proceso y es integral para que se acepten los resultados de las elecciones. La Organización de los Estados Americanos (OEA) y la Mancomunidad, al ser dos organismos regionales, reconocen la necesidad de garantizar que sus Estados Miembros sean conscientes de la amenaza que enfrentan sus democracias en este entorno digital, y que estos estados consideren qué acciones pueden ser necesarias para sus planes estratégicos y respuestas.

La Organización de los Estados Americanos (OEA), siendo la organización regional más antigua del mundo, se remonta a la Primera Conferencia Internacional Americana, celebrada en Washington, D. C., desde octubre de 1889 hasta abril de 1890. En 1948, a través de la Carta de la OEA, se estableció la OEA para lograr entre sus Estados Miembros, como se estipula en el Artículo 1 de la Carta, “un orden de paz y justicia, fomentar su solidaridad, robustecer su colaboración y defender su soberanía, su integridad territorial, y su independencia”. Al reunir a los 35 estados independientes de las Américas, la OEA utiliza un enfoque de cuatro ejes para implementar efectivamente sus propósitos esenciales, basados en sus pilares principales: democracia, derechos humanos, seguridad y desarrollo. La Commonwealth es una comunidad diversa de 53 naciones que trabajan juntas para promover la prosperidad, la democracia y la paz. Construir, apoyar y fortalecer los sistemas legales en sus países miembros incluye la promoción de elecciones periódicas y el fortalecimiento de las capacidades de los órganos, instituciones y procesos electorales. La Commonwealth le da mucho valor a ser una comunidad de países pacíficos y democráticos y garantizar que los valores políticos fundamentales compartidos, incluido el compromiso con los derechos humanos, el estado de derecho y el gobierno civil, estén activamente protegidos y promovidos.

Este documento, desarrollado por la OEA con el apoyo de la Commonwealth, busca crear conciencia sobre los problemas relacionados con la tecnología y la democracia y alentar el diálogo global sobre el tema. La primera sección establece el contexto al explorar cómo la distribución de información a través de Internet impacta el proceso democrático. Partiendo de ese tema, nos basamos en los resultados de una encuesta aplicada entre los Estados Miembros de la OEA sobre las amenazas cibernéticas en los sistemas democráticos. El documento concluye con sugerencias y recomendaciones sobre cómo facilitar el discurso y las prácticas positivas en los ámbitos locales, regionales y nacionales.

Habrá muchos factores alrededor de los cuales la democracia necesitará navegar y la llegada del COVID-19 como una pandemia global lo hizo aún más evidente. Las democracias han tenido que adaptarse a estas circunstancias cambiantes y confiar en soluciones tecnológicas para apoyar procesos esenciales como las elecciones. Esta profunda integración de la tecnología, ahora más que nunca, exige la necesidad de fortalecer las medidas de seguridad cibernética para generar una confianza continua en los procesos democráticos.

Objetivo

Este documento está destinado a crear conciencia entre los Estados Miembros de la OEA sobre los procesos que rodean y sostienen nuestras democracias. Más específicamente, pretende centrar la atención en las implicaciones de ciberseguridad que pueden afectar los procesos que apoyan la democracia y, en particular, los procesos electorales. Incluso si se considera que los procesos democráticos están libres de tecnología, es de suma importancia considerar la ciberseguridad en el contexto más amplio del panorama democrático.

Según la Carta Democrática Interamericana (CDI), "Son elementos esenciales de la democracia representativa, entre otros, el respeto a los derechos humanos y las libertades fundamentales; el acceso al poder y su ejercicio con sujeción al estado de derecho; la celebración de elecciones periódicas, libres, justas y basadas en el sufragio universal y secreto como expresión de la soberanía del pueblo; el régimen plural de partidos y organizaciones políticas; y la separación e independencia de los poderes públicos" (GA/OEA 2001).

Teniendo en cuenta la definición de la CDI, este documento pretende cubrir algunos aspectos de las medidas de ciberseguridad que garantizan los derechos humanos y las libertades fundamentales y la celebración de elecciones periódicas, libres y justas. La sensibilización de los ciudadanos, los partidos políticos y los candidatos sobre los probables efectos devastadores de los ataques cibernéticos, contribuirá a mitigar las posibles consecuencias de los ataques cibernéticos contra los partidos políticos y sus campañas. La necesidad de contar con un marco de ciberseguridad para las elecciones se ha convertido recientemente en un tema muy debatido. El asunto de abordar las amenazas cibernéticas que afectan específicamente las elecciones no solo está en la mira de los funcionarios y profesionales de seguridad de la tecnología de la información, sino también entre los tomadores de decisiones y el público en general. Por lo tanto, es necesario no solo educar al público sobre cómo pueden afectar los incidentes cibernéticos los procesos democráticos en su conjunto, sino también desarrollar herramientas que puedan ser útiles para los políticos, los ciudadanos y los medios de comunicación y proteger mejor a las instituciones electorales contra los ataques cibernéticos.

Recientemente, se han presentado presuntos incidentes de piratería en elecciones latinoamericanas[1], desde desfigurar sitios web de campañas, entrar en las bases de datos de otros partidos para realizar espionaje y usar software malicioso. Sin embargo, la existencia de polarización política y cierta inestabilidad económica reciente ha preparado el terreno para realizar ataques más sofisticados. Las tecnologías digitales e Internet han ofrecido medios adicionales para llevar a cabo una elección, como son la votación por Internet, el trámite del proceso electoral en línea, o el registro de votantes en línea. Por lo tanto, más allá de la manipulación de las redes sociales o la propaganda moderna, un proceso electoral puede volverse vulnerable a medida que las instituciones adoptan nuevas tecnologías.

Este documento presenta varios temas a considerar que destacan los posibles desafíos e impactos de la tecnología en el proceso democrático. No es una guía autoritativa, para seguir paso a paso, en la implementación de medidas de ciberseguridad, ni es un informe en profundidad sobre las tendencias actuales y las amenazas contra la tecnología utilizada en el

proceso democrático, aunque sí se ofrecen algunas recomendaciones específicas. Es importante cambiar la mentalidad de la región desde el considerar el proceso democrático como un evento lineal (ya sea un referendo para un propósito específico o un ciclo electoral). Más bien, el proceso democrático debe abordarse continuamente dentro de una mentalidad cíclica y a través de un enfoque cíclico. El desafío de identificar buenas prácticas tecnológicas para una región tan diversa como la OEA es grande, particularmente dada la naturaleza dinámica de las amenazas de ciberseguridad. Con esta complejidad en mente, este documento se enfoca más en cómo se puede manejar la tecnología para controlar su impacto en el proceso democrático, en el contexto de los diversos puntos en común en las diversas regiones de las Américas y el Caribe. Iniciar un diálogo entre todos los interesados en la región es necesario para aumentar su comprensión de la amenaza que la tecnología le genera al proceso democrático. Debemos ampliar y aumentar su conocimiento para mitigar uno de los desafíos más apremiantes de nuestro tiempo.

Cuando se trata de ciberseguridad, hemos visto varias publicaciones que abordan la complejidad que tenemos ante nosotros. Este documento trae a discusión algunas ideas alternativas que unen democracia, ciberseguridad e información. Al abordar el desafío de frente y reforzar las libertades de expresión, esperamos que la voluntad política en la región pueda aumentar para abordar esta nueva realidad.

Introducción

La Organización de los Estados Americanos (OEA) sirve como un foro político para las Américas, donde los países independientes de América del Norte, Central y del Sur y el Caribe se unen para avanzar en sus objetivos compartidos y resolver sus diferencias. El diálogo político es importante en cada uno de los cuatro pilares de la OEA: democracia, derechos humanos, seguridad y desarrollo. Dicho diálogo condujo al desarrollo, por la OEA y sus Estados Miembros, de la Carta Democrática Interamericana, un modelo de cómo debería ser la democracia en la región.

De conformidad con la Carta Democrática Interamericana, adoptada por la Asamblea General en su sesión especial celebrada en Lima, Perú, el 11 de septiembre de 2001, (GA / OEA 2001):

> ***[Artículo 1]*** *"Los pueblos de América tienen derecho a la democracia y sus gobiernos la obligación de promoverla y defenderla.*
> *La democracia es esencial para el desarrollo social, político y económico de los pueblos de las Américas".*
>
> **Además,**
> ***[Artículo 7]*** *"La democracia es indispensable para el ejercicio efectivo de las libertades fundamentales y los derechos humanos, en su carácter universal, indivisible e interdependiente, consagrados en las respectivas constituciones de los Estados y en los instrumentos interamericanos e internacionales de derechos humanos".*
>
> **También,**
> ***[Artículo 2]*** *"El ejercicio efectivo de la democracia representativa es la base del estado de derecho y los regímenes constitucionales de los Estados Miembros de la Organización de los Estados Americanos. La democracia representativa se refuerza y profundiza con la participación permanente, ética y responsable de la ciudadanía en un marco de legalidad conforme al respectivo orden constitucional".*

En este sentido, la OEA promueve una cultura democrática y continúa llevando a cabo programas y actividades diseñados para promover principios y prácticas democráticas para fortalecer una cultura democrática en el hemisferio, teniendo en cuenta que la democracia es una forma de vida basada en la libertad y mejora de las condiciones económicas, sociales y culturales para los pueblos de las Américas.

La OEA continúa trabajando más concretamente en asuntos democráticos desde varios ángulos y continuar su larga historia en el despliegue de Misiones de Observación Electoral (MOE). Desde 1962, la OEA ha desplegado más de 275 MOEs en 28 Estados Miembros[2]. Como parte de su proceso de sistematización y estandarización de las Misiones de Observación Electoral, el Departamento para la Cooperación y Observación Electoral (DECO, por sus siglas en inglés) de la Secretaría para el Fortalecimiento de la Democracia (SFD) de la OEA desarrolla varias herramientas y metodologías para apoyar a los Estados Miembros en el fortalecimiento de sus sistemas y procesos electorales a nivel institucional[3]. Un documento particularmente relevante de la Secretaría General de la OEA es "Observación del uso de tecnología electoral: un manual para las misiones de observación electoral

de la OEA" (SG / OEA 2010). Los observadores en el campo utilizan este documento cuando examinan el uso de tecnologías. Cubre aspectos que generalmente deben considerarse en la observación de cualquier elección en la que la tecnología sea un factor.

Los países del hemisferio occidental, salvo algunas excepciones, están experimentando el período más largo de democracia ininterrumpida en la historia de la región. En ese contexto, los medios deben considerar el papel que desempeñan en el entorno social y las condiciones dentro de las cuales compiten los candidatos. Los medios de comunicación son un elemento cada vez más influyente en un proceso electoral y un nivel asociado de influencia en la democracia. En ese sentido, mantenerse al tanto de los problemas actuales, como las amenazas de ciberseguridad y las implicaciones de estos en la democracia, es fundamental. A raíz de un ataque, los medios de comunicación podrían informar sobre eventos sin tener la terminología correcta o informar de manera incorrecta sobre el impacto que algunos incidentes cibernéticos pueden tener en los resultados generales de los procesos democráticos.

Este documento, por lo tanto, presenta algunos temas centrales en torno a la información, los medios y el proceso democrático en los siguientes capítulos: **El poder de la desinformación en la era digital; Desafíos de ciberseguridad en el proceso democrático: América Latina y el Caribe; Esfuerzos mundiales en ciberseguridad y democracia; El proceso democrático: Infraestructura institucional y consideraciones de ciberseguridad; Compromiso de la comunidad en procesos democráticos; y Facilitar el diálogo y considerar los próximos pasos: Recomendaciones.**

Reflexión:
El poder de la desinformación en la era digital

El acceso y la distribución de información han jugado un papel esencial en el establecimiento, así como en la consolidación, de muchas democracias en todo el mundo. La disponibilidad de información influye en la democracia. Debemos considerar la influencia pasada, presente y futura de la información a medida que continuamos adaptando nuestras instituciones y procesos democráticos en preparación de una era moldeada por la tecnología de la información. Debemos estar preparados para responder a las nuevas amenazas, así como a las nuevas oportunidades para la democracia en su conjunto.

Contexto

La información ha existido desde tiempos inmemoriales, pero tal vez se refería a esta, o era identificada, por otro nombre. El arte de contar historias fue la base de miles de años de historia compartida. El acto de compartir e impartir conocimiento a las generaciones futuras ha definido las diversas culturas que compartimos entre nuestra gente en todo el mundo.

Este intercambio histórico de conocimiento y formación de nuestras culturas a través de la palabra hablada comenzó a tomar forma escrita en tabletas de arcilla alrededor del 3200 a. C. Mucho más tarde, Gutenberg dio vía libre a la producción en masa de impresiones, y es quizás aquí cuando comenzamos a pensar en este intercambio de ideas o intercambio de conocimientos como información o, más concretamente, intercambio de información (Nelson 1998).

La información y sus modalidades requieren alguna forma de definición, ya que hay varias opiniones sobre el significado del término información, especialmente dentro de un contexto cibernético. Para el diálogo actual, consideramos que la información es una forma de mensaje, que puede ser una imagen, un video o la palabra escrita, así como la palabra hablada, todo lo cual informa o forma el debate público y la opinión. Esta definición ofrece la idea más útil y más amplia de información, de modo que es muy ventajoso en el contexto de este documento. Es posible que una definición más técnica del término información (específicamente, paquetes de información técnica distribuidos a través de una red) sea más apropiada para una discusión y audiencia de ciberseguridad, pero eso no se ajustaría al amplio alcance que creemos que tiene la información en el panorama democrático.

> *"La información se ve cada vez más como un bien común, cuya protección recae en todos los ciudadanos interesados en la calidad del debate público" (Vilmer 2018).*

Si uno mirara hacia atrás en los últimos 100 años, no sería demasiado difícil establecer casos específicos en los que la información jugó un papel vital en las diversas administraciones de la época. También podríamos extraer ejemplos en los que la información, o sea, información de acceso público, contribuyó incluso a la percepción occidental sobre guerras importantes, que contaminan nuestra historia compartida[4]. Del mismo modo, podríamos recurrir a ejemplos específicos en los que la información simplemente ha creado líderes mundiales y les ha conservado su poder. El tema común en estos ejemplos variados es el poder abrumador de la información. Ya sea dentro del contexto de un hogar, el lugar de trabajo o incluso un cargo público, la capacidad de controlar una narrativa dentro de estos contextos ofrece un control total sobre esos mismos contextos.

A nivel internacional, se discute mucho sobre lo que constituye el poder duro o poder blando, pero quizás hemos llegado a un punto en nuestras sociedades donde podemos comenzar a hablar sobre el poder real. El poder real es la capacidad de controlar una narrativa, sin importar el contexto en el que uno está operando. La información y su distribución permiten que se cuente una narración, que se establezca y se refuerce mediante su redifusión. Es en este punto donde se deben tomar en cuenta las medidas de seguridad, dentro de sus propios contextos, a nivel de distribución y la escalabilidad del proceso de distribución.

Hay discusiones dentro del Sistema Interamericano[5] sobre el equilibrio entre la necesidad del Estado de ejecutar su función de proveer una seguridad pública y la de las garantías de derechos humanos de un ciudadano. En este sentido, cualquier restricción "debe interpretarse en estricto cumplimiento de las demandas justas de una sociedad democrática, que tenga en cuenta el equilibrio de los diferentes intereses en juego y la necesidad de preservar el objeto y el propósito de la Convención Americana"[6].

Transitando esa delgada línea

Uno de los logros más poderosos que Internet ha hecho posible es la capacidad de distribuir contenido a gran escala, con gran facilidad y a costos significativamente más bajos que las vías tradicionales de distribución de contenido, como los medios impresos, de radio y televisión, espacios de galería, el cine, entre otros. Internet también ha permitido compartir contenido a velocidades increíbles. El acceso a Internet permite, en la mayoría de los casos, que cada estrato de la sociedad comparta información por igual, y es esta capacidad, asociada con la libertad de expresar opiniones, la que ha generado volúmenes y volúmenes de contenido diario, con diversos grados de interés y precisión. Esta libertad de expresión sigue siendo un derecho humano universal que debe respetarse en todo momento, consciente de que es necesario evitar cualquier castigo de opiniones a menos que esté 'respaldado por pruebas reales, verdaderas, objetivas y fuertes de que la persona no estaba simplemente emitiendo una opinión (incluso si esa opinión era dura, injusta o perturbadora), sino que la persona tenía la clara intención de cometer un delito y con una posibilidad real, actual y efectiva de lograr este objetivo. Actuar de otra manera significaría admitir la posibilidad de castigar opiniones, y todos los Estados estarían autorizados a suprimir cualquier tipo de pensamiento o expresión crítica de las autoridades que -al igual que el anarquismo y las opiniones radicalmente opuestas al orden establecido- cuestionen la existencia de las instituciones actuales. En una democracia, la legitimidad y la fuerza de las instituciones se fortalecen por la fuerza del debate público sobre su funcionamiento, no por su represión'.[7]

Cualquier expresión puede tener un alcance inconmensurable a través de canales de distribución en Internet. Si comparáramos la distribución de un solo mensaje en Internet con la distribución de ese mismo mensaje a través de las reuniones tradicionales municipales, podríamos imaginar que se llegaría a un acuerdo a una escala solo limitada al alcance del mensaje cuando se distribuye en Internet, contrario al alcance finito generado por la reunión municipal.

La conexión de ciberseguridad

En las secciones anteriores de este documento, hemos abordado algunos de los argumentos más directos con respecto a la relación entre la información e Internet. Hasta ahora existe una suposición implícita de que la información distribuida a través de Internet es positiva, objetiva, verdadera, precisa y en pos del bien común.

Sin embargo, si observamos la situación de manera más amplia, podemos encontrar que la información es opuesta a la descripción anterior, es decir, es negativa, no objetiva, falsa, deshonesta y en busca de ganancias y poder políticos. ¿Qué pasos podrían tomarse para evitar que esta narrativa inútil se establezca y se arraigue en una sociedad?

El desafío es increíblemente difícil, dados los principios de libertad de expresión tal como están consagrados en la Declaración Universal de Derechos Humanos, el Artículo 19, y el derecho humano a tener acceso a Internet e igualmente a información confiable y objetiva (ONU 2016).

> ***[Artículo 19]*** *"Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión".*

No son necesariamente los tecnicismos de la ciberseguridad los que hacen de este desafío un desafío de ciberseguridad. Es la capacidad de Internet para difundir información viral a niveles nunca antes vistos lo que hace que todo el tema de la información sea una cuestión de ciberseguridad. Con este fin, la OEA ha recomendado a los estados que "lleven a cabo acciones positivas de educación, capacitación y sensibilización sobre el fenómeno de la desinformación"[8].

Información errónea, Desinformación[9], Noticias falsas y la Manipulación de la información

Las publicaciones de los gobiernos nacionales describen asuntos como las noticias falsas, información errónea, desinformación y un número de términos que se pueden usar para describir diversas formas de distribución de información inexacta[10]. Toda esta terminología que describe los diferentes tipos de información errónea es simplemente un aspecto del problema que debe tenerse en cuenta al abordar la distribución de información.

> *"Vivimos en un mundo donde hay más y más información, y cada vez menos significado". (Baudrillard 1983)*

Es a través de una conciencia sobre la profundidad y amplitud de la información errónea, la desinformación y otras formas de manipulación de la información, que podemos comenzar a comprender cómo los actores relevantes pueden afectar el resultado de su propio proceso electoral. Del mismo modo, a través de las mismas tácticas y enfoques, podemos comenzar a comprender el surgimiento de la interferencia de un estado extranjero de esa misma manera, afectando el resultado de un proceso electoral de un país extranjero.

La manipulación de estado a estado también es una problemática y podría incluir ataques cibernéticos tradicionales a la infraestructura. Esta manipulación podría resultar en la inhibición de la conducta real de un proceso electoral, reduciendo la participación en la votación y afectando directamente un resultado.

El problema de escalabilidad

El crimen siempre ha existido y con Internet entrando con fuerza en el mercado, ha permitido el acceso a los delincuentes. Es esta escalabilidad la que el mundo está enfocado en combatir, mediante diversas iniciativas nacionales e internacionales para contrarrestar el delito cibernético. Del mismo modo, la propaganda y los mensajes políticos siempre han existido. Internet ha exacerbado su impacto y alcance. No existe una solución técnica para el creciente escalamiento del delito cibernético y su impacto en el proceso democrático. Por lo tanto, se deben considerar e implementar soluciones estratégicas a más largo plazo.

La economía de una audiencia cautiva

Durante ese instante en el que un mensaje, expresión o información se distribuye y se vuelve viral, se presenta una característica adicional de una audiencia cautiva, es decir, una audiencia masiva que se distrae con el contenido viral, que a menudo se pasa por alto. Mientras que los mensajes se pueden compartir casi instantáneamente, como lo que sucede con una reunión municipal virtual, también se puede compartir información de naturaleza más negativa con la misma rapidez. La capacidad de acceder a una audiencia cautiva para introducir malware para obtener ganancias económicas en una comunidad que comparte a un ritmo rápido por lo general se combate a través de mecanismos tradicionales destinados a contrarrestar el delito cibernético, y de manera similar se puede mitigar a través de herramientas disponibles para las fuerzas de la ley y la industria.

El asunto de los datos personales

Las redes sociales han creado una nueva dimensión a los desafíos de la tecnología y el proceso democrático al poner a disposición una gran cantidad de información de acceso público sobre todos los miembros de la sociedad. Hay varios ejemplos de cómo la explotación de la información personal y los datos personales apuntan a una mayor ganancia económica o política. Es importante aceptar las realidades del panorama actual por el que navegamos como ciudadanos y votantes en un país, entendiendo que la información que publicamos en las redes sociales puede usarse de formas que no entendemos[11]. Comenzar a cambiar la mentalidad en torno a los datos personales al aumentar la noción de valor que los individuos les atribuyen a sus propios datos, junto con un sólido régimen de protección de datos, puede comenzar a reducir el poder y la influencia de las empresas de redes

sociales en la distribución de información política[12]. También es imprescindible que las grandes empresas, cuyo modelo de negocio se basa en el almacenamiento masivo de datos personales y el intercambio de esos datos[13], asuman responsabilidades (a corto plazo) para garantizar que el bien común o la voluntad de la gente no se comprometa debido a la manipulación de datos disponibles públicamente que se mantienen en sus plataformas e infraestructura.

Las grandes corporaciones que poseen grandes bancos de datos deben asumir la responsabilidad de los datos que poseen y controlar la forma en que se utilizan esos datos. Esta responsabilidad va más allá de los requisitos legislativos internacionales, cuyo objetivo es evitar el mal uso de la información personal. También abarca la responsabilidad moral de estas empresas de garantizar que los datos no solo estén protegidos desde una perspectiva de seguridad puramente técnica, dentro de los límites y mandatos del estado de derecho, sino también que las personas estén informadas sobre el uso -y el posible uso indebido- de sus datos personales.

Las empresas que no tienen grandes bancos de datos del público aún tienen datos sobre sus empleados, que deben protegerse. Es responsabilidad de los empleadores asegurarse de que sus empleados comprendan la política de la entidad sobre el procesamiento de la información personal y cómo se mantiene -y defiende- en la mayor medida posible.

Información política

> *"Describirnos (también) como inforgs, que buscamos, producimos, cultivamos, curamos, procesamos y consumimos información, habitando un entorno también hecho de datos y procesos computacionales, significa adoptar una perspectiva ecológica" (Floridi 2013).*

En su artículo, "El marketing como control de las interfaces humanas y su explotación política", el profesor Floridi describe el cambio en el paisaje y el cambio en la relación entre el marketing y la política.

> *"La política se ha convertido en una cuestión de marketing, es importante entender por qué esto es cierto".*

No es que la política haya cambiado su posición. En cambio, es el marketing y la capacidad de acceder y distribuir información lo que ha cambiado. La relación entre los individuos, las plataformas que estos navegan y el recurso que estos poseen o intercambian abarca dos paradigmas. El primer paradigma es que el individuo es el objetivo de las campañas de marketing (es decir, donde el marketing político está diseñado para acariciar el ego individual). El segundo es el proceso de intercambio de recursos que está en el centro de la relación (es decir, donde un recurso es nuestro crédito económico o datos o voto).

Educar a la población

A medida que nuestra sociedad de la información continúa desarrollándose y abarcando todos los aspectos de la vida, existe un requisito dramático y urgente para empoderar al público en general con las habilidades necesarias para poder navegar en el complejo paisaje que domina la vida cotidiana. El sector educativo, con el apoyo de la academia, tiene un papel aquí para comenzar a construir, de manera verdadera y significativa, el conocimiento y las habilidades requeridas por el público en general para pensar críticamente sobre la información.

La ambición de todas las partes interesadas debe ser equipar al público en general, a la edad más temprana posible, con las siguientes habilidades:

1. Descifrar mensajes publicitarios y de marketing (en este caso político, pero debe ser amplio)
Equipar al público en general con la capacidad de comprender la veracidad de los mensajes y el contexto dentro del cual existe el mensaje es de suma importancia. La amenaza que tenemos ante nosotros para comprender la comunicación no solo en un contexto político, sino también en un entorno comercial, les permite a las personas pensar críticamente y tomar decisiones informadas, y construir un filtro directo sobre un nivel significativo de estrategias de manipulación de información que están en juego en este momento. Construir un filtro personal de la información disminuye la exacerbación de la manipulación de la información a través de medios en línea.

2. Fuentes e identificación del periodismo de investigación
Desarrollar una apreciación y comprensión del mundo del periodismo en todo el mundo para combatir las tendencias actuales que ven una disminución en el valor del periodismo independiente. Alentar y capacitar al público en general para identificar y seguir a los medios de comunicación que brindan un informe transparente sobre el discurso y el debate político permite un diálogo valioso y le da forma al panorama político. La variedad en las fuentes de información, identificada a través de una sólida comprensión de descifrar mensajes, permite esto.

3. Desarrollar una comprensión de la transparencia y la rendición de cuentas
El principio de transparencia y responsabilidad, junto con el respeto de los derechos humanos fundamentales, es la base de la buena gobernanza. Como la manipulación de la información ha abrumado el discurso político actual tan interconectado con una audiencia mundial, es fundamental recordarle al público en general la importancia de la transparencia y la rendición de cuentas.

4. Reforzar la comprensión del conflicto de intereses
Lograr una comprensión del conflicto de intereses también es parte integral de la amenaza ante el mundo. Sin comprender cómo se ve la conducta ética, el público en general no puede juzgar qué es correcto y qué es incorrecto. Las campañas de comunicación en línea constantes y específicas para obtener ganancias o favores políticos son una táctica de manipulación de la información cada vez mayor. Es importante alentar el pensamiento crítico por parte del público en general para mitigar la implacable propaganda que busca normalizar la tolerancia al conflicto de intereses en el cargo público.

La solución funcional

No existe una respuesta directa a los desafíos que el mundo enfrenta actualmente en todo el espectro y los sistemas políticos. No existe un libro de reglas o una guía paso a paso para combatir la distribución de campañas de información maliciosas o malignas. En cambio, debemos centrar nuestra atención en soluciones a largo plazo y comenzar a sembrar las semillas para empoderar a nuestras naciones para que tomen decisiones adecuadamente informadas cuando participen en procesos democráticos. Es responsabilidad de cada administración, en colaboración con empresas de datos masivos o poseedores de información, asegurar y fomentar información confiable y pensamiento crítico por parte del público a fin de mantener las democracias saludables. Sin embargo, hay dos conclusiones clave de este ejercicio:

1. El hecho de que haya varias publicaciones a nivel mundial centradas en el tema de la información errónea y las noticias falsas y una serie de debates e investigaciones académicas que se están llevando a cabo actualmente es un testimonio de que las personas están prestándole más atención a lo que ocurre a su alrededor. Este nivel de análisis es una muy buena cosa para la democracia. Nuestras sociedades se están moviendo en la dirección correcta, centrándose en gran medida en programas de sensibilización para contrarrestar la amenaza.

2. Es importante revisar y evaluar eventos e intervenciones anteriores, menoscabando el mito de que una vez que se termina un proceso electoral, podemos dejar de lado la prioridad de abordar los desafíos que enfrenta el proceso democrático durante la duración del mandato. En este punto, debe llevarse a cabo una evaluación adecuada para extraer las lecciones aprendidas de cada ciclo electoral. Debemos asegurarnos de que haya colaboración en todos los ámbitos para desarrollar, construir y mantener la conciencia y la comprensión de cómo se utilizan los datos en todo el proceso democrático para informar a los regímenes adecuados de protección de datos.

Es importante empoderar a nuestras sociedades. Tenemos que evaluar continuamente el entorno en el que nos encontramos porque cambia continuamente. Establecer vínculos y relaciones sólidas con las redes sociales y los proveedores de servicios de Internet es una herramienta para que esta evaluación sea práctica.

Desafíos de ciberseguridad en el proceso democrático en las Américas

En los últimos 20 años, Internet y las Tecnologías de la Información y la Comunicación (TIC), entre otras tecnologías emergentes, han revolucionado diferentes ámbitos de la vida diaria. Las soluciones digitales se han desarrollado continuamente para facilitar la interacción social y la comunicación, así como el acceso a la información. Las aplicaciones de estas tecnologías han sido ilimitadas, y los procesos democráticos no han sido la excepción. Los procesos electorales, por ejemplo, integran tecnología en muchos de sus pasos: los OGE usan sitios web para publicar resultados de votación y otros sistemas para mantener registros electorales. En muchos países, los OGE también usan diferentes tipos de soluciones tecnológicas para procesar y transmitir hojas de conteo de manera más eficiente, transparente o más rápidamente (en comparación con opciones más manuales).

A medida que se siguen adoptando soluciones digitales, su exposición a los riesgos de ciberseguridad puede ser inevitable. La región de las Américas es un objetivo notable y una fuente de ataques cibernéticos. El Informe sobre amenazas a la seguridad en Internet clasificó a las tres economías más grandes de la región, Brasil, Argentina y México, en el tercer, octavo y décimo lugar, respectivamente, en su clasificación global de origen de ataques cibernéticos (Symantec 2019). De manera similar, en un artículo de 2017 publicado por Kaspersky, se informó que los usuarios de Internet en América Latina eran víctimas de más de 177,500 ataques de malware por hora, lo que se traduce en un promedio de 33 ataques por segundo en la región (Kaspersky 2017). Más recientemente, según un informe presentado por el Registro de direcciones de Internet de América Latina y el Caribe en su grupo de Alertas, Recomendaciones y Punto de Reporte e Intermediación (LACNIC WARP, por sus siglas en inglés) durante el seminario web titulado “Tendencias de ciberseguridad en nuestra región”, se analizó cómo el phishing continúa como la principal causa de amenazas cibernéticas en América Latina y el Caribe, representando más del 60% de los ataques registrados, mientras que el uso de malware (18,9%) y la redirección (16,35%) han seguido aumentando en los últimos años (LACNIC 2018). En otras palabras, los países de la región son y continuarán siendo un objetivo y una fuente de actividad de ciberseguridad maliciosa.

El creciente número de soluciones digitales utilizadas en los procesos democráticos, además de las crecientes amenazas de ciberseguridad en la región, han creado una demanda para comprender el grado de adopción de soluciones digitales en los procesos democráticos y sus respectivos desafíos de ciberseguridad en las Américas.

Por lo tanto, la OEA elaboró una encuesta dirigida a partes interesadas específicas involucradas en los procesos democráticos de sus 34 Estados Miembros. Esta encuesta tomó en consideración el cambiante panorama de ciberseguridad en la región, así como las aplicaciones tecnológicas utilizadas para los procesos electorales. La encuesta analizó: (1) el grado de digitalización del proceso electoral, (2) marcos legislativos, (3) amenazas cibernéticas contra el proceso democrático y (4) niveles de implementación de medidas de ciberseguridad para proteger el proceso electoral. Utilizando muestreo agrupado, la OEA identificó a funcionarios electorales, parlamentarios, equipos nacionales de respuesta a incidentes y representantes de ministerios gubernamentales como el conjunto de la muestra apropiado para responder a la encuesta. Las preguntas se respondieron sobre la base de lo que cada parte interesada respectiva podría responder o divulgar. Por ejemplo, las preguntas dirigidas a los OGE fueron respondidas específicamente por funcionarios electorales.

La OEA distribuyó electrónicamente la encuesta de 28 preguntas a las entidades mencionadas anteriormente, que participaron en los cuatro talleres y en un seminario web (consulte el Anexo II), o a los OGE que forman parte de la lista de correo de la Secretaría para el Fortalecimiento de la Democracia de la OEA. Se recibieron respuestas de 17 países[14] con perfiles compuestos principalmente por funcionarios electorales (85% de las respuestas) y el 15% restante consistió en representantes del Ministerio de Gobierno, parlamentarios y equipos nacionales de respuesta a incidentes.

Esta muestra no es representativa de los 34 Estados Miembros; no se puede suponer que los resultados reflejan las opiniones institucionales de cada parte interesada que está directa o indirectamente involucrada en los procesos electorales dentro de cada país. Sin embargo, aunque se requiere un estudio más exhaustivo para proporcionar una comprensión más profunda de este tema en la región, se espera que el análisis de los datos recopilados a través de esta encuesta aún pueda arrojar algo de luz en un esfuerzo por comprender los desafíos de ciberseguridad en los procesos electorales en la región.

A los fines del análisis, las respuestas se agruparon en dos regiones: (1) América Latina y (2) el Caribe. Como los países de cada región respectiva comparten niveles similares de madurez en las capacidades de ciberseguridad, esto proporcionó una base útil para un análisis exhaustivo de la región. El análisis se complementó a través de una serie de entrevistas en profundidad con expertos regionales que entregaron información adicional que complementó los resultados de la encuesta.

Teniendo en cuenta las limitaciones antes mencionadas de este estudio, los resultados de la encuesta revelaron que aproximadamente 13 de los 17 países que respondieron (75% de los encuestados) habían implementado bases de datos de registro de votantes (proporcionalmente bastante equilibradas tanto en el Caribe como en América Latina) y páginas web institucionales (en los que Estados Miembros latinoamericanos han implementado esta herramienta con más frecuencia).

En comparación con sus contrapartes caribeñas, los países latinoamericanos son más activos en la utilización de páginas web institucionales, sistemas de información electoral, redes sociales y sistemas de conteo de votos. Las máquinas de votación y la votación por Internet no son soluciones

ampliamente utilizadas en la región, ya que ningún país del Caribe las ha implantado. Solo el 57% de la Autoridad / Comisión / Agencia Nacional indicó que usa servicios en la nube, con cierto grado de correlación entre el tamaño del país y siendo evidente su introducción[15].

Además, más del 50% ha implementado la identificación digital, y aproximadamente el 58% utiliza las redes sociales, siendo más amplia la integración en América Latina. En relación con la asignación presupuestal, aunque hay algunas indicaciones iniciales sobre la prioridad de la implementación digital, más del 50% de los encuestados indicaron que no tienen un presupuesto dedicado ni un equipo dedicado para mejorar la ciberseguridad del proceso democrático. Esto es cierto a pesar del hecho de que más del 70% de los encuestados anticipan un aumento en el número de ataques cibernéticos en las próximas elecciones y el 90% de ellos indican que una colaboración más profunda entre las agencias y un Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT) tendría un impacto positivo en la seguridad general de los procesos democráticos.

Con respecto al conocimiento general de posibles incidentes de ciberseguridad, más del 50% de los encuestados desconocen dichos incidentes hacia sus procesos electorales. Una explicación de esto podría ser que hay un número significativo de eventos que no se detectan. Esta explicación sugiere que se deben asignar más recursos para identificar estos incidentes correctamente y para aumentar la conciencia de todos los interesados sobre los problemas que sustentan la ciberseguridad.

Otra observación de los resultados de la encuesta es que hay desafíos continuos en términos de concientización y medidas políticas que se deberán tomar. Se identificó como una necesidad las actualizaciones legales, el establecimiento de un grupo de trabajo o comité para asegurar el proceso electoral y, en general, una mejor coordinación[16]. Además, según los encuestados, no hay suficiente colaboración entre organizaciones en los países incluidos en la muestra, aunque la mayoría de ellos creen que una mejor colaboración aumentaría la seguridad general del proceso electoral.

Un tema común para los encuestados representados en la encuesta es que, aunque es crítico, la importancia de la ciberseguridad en el proceso democrático pierde impulso una vez que terminan las elecciones. El tema se ve opacado hasta el siguiente ciclo electoral, o en el momento en que se descubre un ataque. Cuando ocurre esto último, la falta de estructuras definidas como comités, grupos de trabajo o incluso legislación actualizada puede conducir a una protección insuficiente y, en última instancia, empeorar las consecuencias.

Este documento, por lo tanto, tiene como objetivo contribuir a la difusión de buenas prácticas y su implementación progresiva para prevenir incidentes de ciberseguridad en el contexto de las elecciones.

Grado de digitalización del proceso democrático

El avance de las herramientas de digitalización tiene el potencial de impactar la democracia casi tanto como cualquier otra área, como la ciencia o la educación. Los efectos del mundo digital en la política y la sociedad son difíciles de medir, y la velocidad con la que evolucionan las nuevas tecnologías hace que ese efecto sea particularmente difícil de rastrear (Pogrebinschi 2017). La digitalización de la información ha llevado, en algunos países, a contar con un proceso más abierto y transparente. También se ha convertido en una herramienta para coordinar la voz de las personas, dando lugar al uso de redes sociales para crear conciencia sobre cuestiones políticas clave. Algunos de los aspectos del proceso democrático que han facilitado estas innovaciones digitales incluyen el registro de votantes en línea, el voto electrónico y los foros para la participación pública, entre otros.

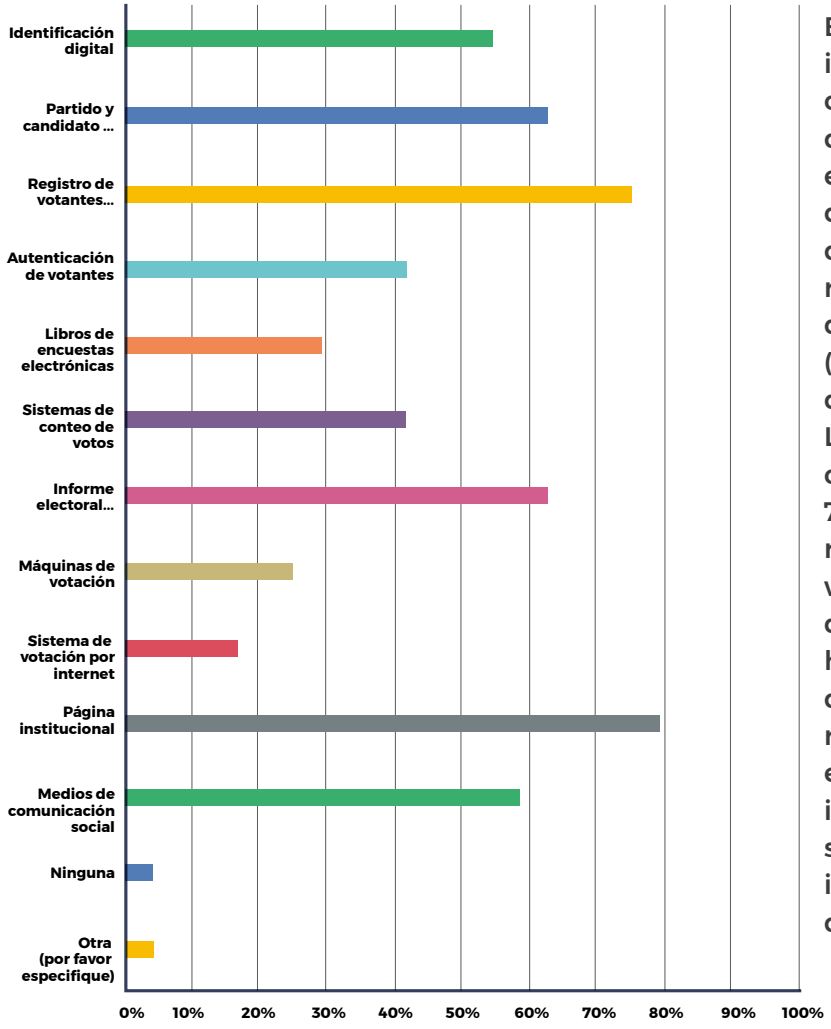

Figura 1. Soluciones digitales implementadas según lo indicado por los encuestados

El primer paso para tener una imagen confiable del panorama de ciberseguridad dentro del proceso democrático en América Latina y el Caribe es comprender el nivel de digitalización de los procesos que apoyan la democracia. Los resultados de la encuesta indican que casi todos los encuestados (93%) han digitalizado sus procesos democráticos en un grado u otro. Las herramientas más utilizadas, con una penetración de más del 75%, son las bases de datos de registro de votantes y las páginas web institucionales. Mientras que el 60% de los encuestados han implementado los sistemas de informes de elecciones y el registro de partidos y candidatos, el 58% informó sobre el uso de la identificación digital y las redes sociales para transmitir mensajes institucionales y / o distribuir declaraciones.

Marcos legislativos

Como se mencionó anteriormente, el primer paso para tener una imagen confiable del panorama de ciberseguridad es determinar cuál es la capacidad en la región para la digitalización de la información. El segundo paso es evaluar el estado de la legislación electoral al incorporar el uso de soluciones digitales, dado que esas soluciones podrían exigir tener las herramientas que abordarían los riesgos relacionados con la ciberseguridad en el proceso democrático. En este sentido, más del 50% de los encuestados indicaron que sus países no habían actualizado su legislación electoral para reflejar la transformación digital que está teniendo lugar. Mejorar el estado de la legislación electoral es un aspecto de la ciberseguridad que debe abordarse, dado que es un primer paso indispensable para mejorar la postura general de ciberseguridad.

Curiosamente, del 90% de los encuestados que no han actualizado su Legislación Electoral, la mayoría cree que es esencial que las modificaciones se realicen para reflejar el proceso de digitalización, lo que sugiere un nivel de conciencia sobre el desafío. Vale la pena señalar que casi el 75% de los encuestados señaló que anticipan una mayor digitalización. El mismo porcentaje de encuestados sabía que cuanto más se digitalice un proceso electoral, mayor será la seguridad general requerida. Todo esto sugiere que se deben identificar más recursos financieros y humanos para mejorar la seguridad de las herramientas y procesos de digitalización.

Amenazas cibernéticas contra el proceso democrático

Como resultado de este nuevo cambio para incorporar más y más soluciones digitales al proceso democrático, debemos considerar los posibles problemas relacionados con la capacidad de proteger los procesos democráticos y, por extensión, proteger la democracia misma al garantizar que cada elección sea justa, libre, y segura. En 2018, la mitad de todas las democracias avanzadas que celebraron elecciones nacionales tuvieron su proceso democrático dirigido por la actividad de amenaza cibernética[17] (CCS 2019).

Dependiendo del contexto del país, algunas amenazas cibernéticas están bajo el mandato de diferentes niveles de administración electoral. En algunos países, ni siquiera se discuten las amenazas cibernéticas en el contexto de las elecciones. Las amenazas al proceso democrático a menudo son responsabilidad de otros actores estatales. Por ejemplo, cuando existe la posibilidad de un alto descontento civil, generalmente se considera que es la responsabilidad de las fuerzas de la ley. Sin embargo, una vez que se involucra la tecnología, vale la pena pensar en un enfoque de todo el gobierno, con énfasis en la colaboración interinstitucional en materia de ciberseguridad en las elecciones, sin importar a qué nivel. Puede haber varios beneficios al establecer un grupo de trabajo de tecnología electoral o seguridad antes de una elección, por ejemplo. Algunos países organizan la colaboración interinstitucional a través de foros dedicados, como grupos de trabajo que se reúnen de manera ad hoc, mientras que otros pueden tener un solo grupo de trabajo sobre ciberseguridad electoral. Este enfoque interinstitucional garantiza que todas las amenazas sean tomadas en cuenta y trabajadas para garantizar la integridad de los resultados electorales. A continuación, se muestra un gráfico que

describe la intersección de la colaboración interinstitucional (por ejemplo, en forma de un grupo de trabajo) con el OGE en relación con la ciberseguridad y las elecciones.

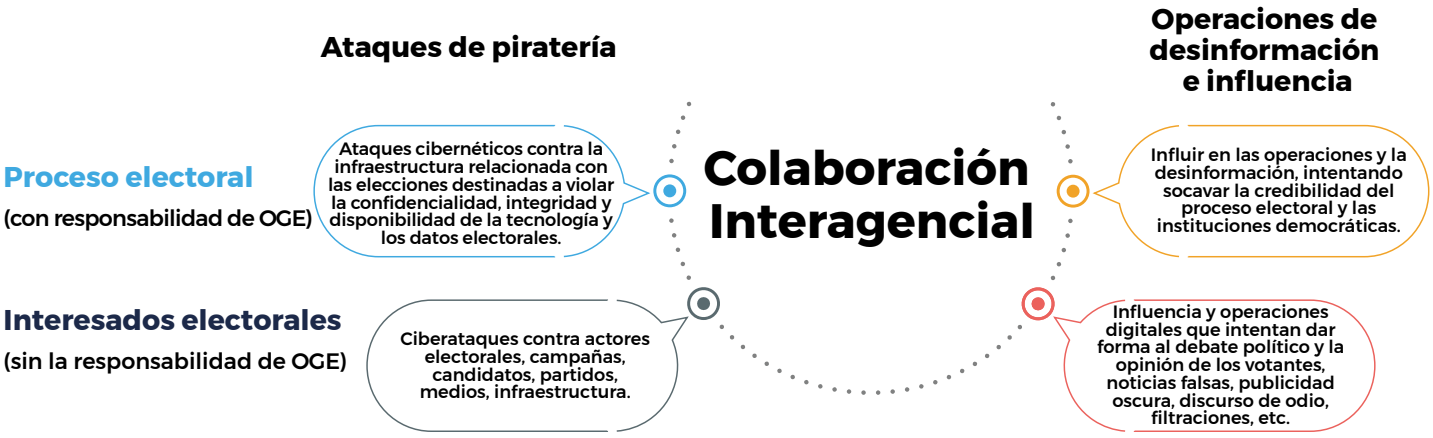

Figura 2. Riesgos cibernéticos en elecciones vs Mandato OGE – Fuente: IDEA Internacional

Los resultados de la encuesta revelaron tres hallazgos principales sobre las amenazas cibernéticas contra el proceso democrático en todos los Estados Miembros de la OEA:

1. Más del 55% de los encuestados no tenían conocimiento de ningún incidente. Esto podría interpretarse como una indicación de que la mayoría de los países están total y completamente protegidos contra los ataques cibernéticos, o podría sugerir que hay un número significativo de incidentes no detectados y una falta de conocimiento de esos incidentes.

2. Algunos de los encuestados anticipan un aumento en los incidentes de ciberseguridad en el proceso democrático en los próximos doce meses. Se pudo observar una correlación evidente entre el tamaño de la población y la sensibilización: cuanto más grande es el país, más se anticipa un aumento en las amenazas cibernéticas esperadas.

3. Casi el 60% de los encuestados indicaron que su país no tiene un grupo de trabajo o un comité de ciberseguridad responsable de asegurar el proceso democrático. Es perfectamente comprensible que, dependiendo del tamaño y los recursos de cada país, el comité de ciberseguridad pueda variar en términos de tamaño y capacidades. Aun así, la existencia misma de un grupo de trabajo capaz de respetar los derechos humanos y las garantías debe considerarse un primer paso. El diseño de estos organismos debe lograr el equilibrio adecuado entre ser efectivos y también conscientes de la posible infracción de los derechos que pueden estar involucrados en las acciones que toman. El 50% de los encuestados sin un grupo de trabajo o un comité electoral de ciberseguridad con un mandato cibernético tampoco esperan tenerlo antes del próximo ciclo electoral.

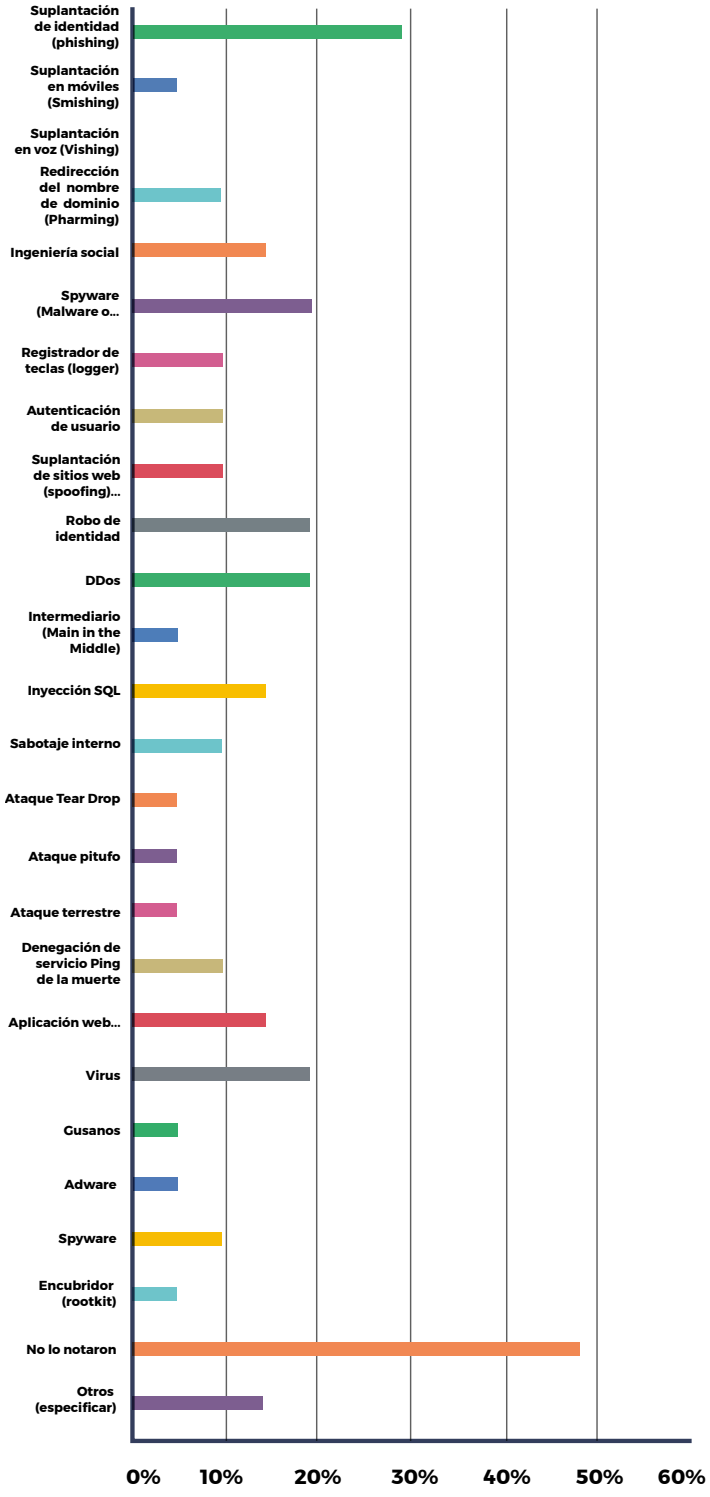

Figura 3. Tipos de incidentes de seguridad digital que se han utilizado contra el proceso electoral, identificado por los encuestados

Los tres hallazgos mencionados anteriormente refuerzan la noción de que crear conciencia sobre este tema es una necesidad urgente. La ciberseguridad debe convertirse y seguir siendo relevante para los legisladores. De lo contrario, la naturaleza temporal del ciclo electoral significa que todo el enfoque y la consideración sobre la ciberseguridad en asociación con el proceso electoral se termina hasta la siguiente precampaña, aumentando peligrosamente las posibilidades de ataques exitosos no detectados. Es fácil olvidar la importancia de revisar las lecciones útiles aprendidas del proceso general para evitar repetir esos errores en el futuro.

Curiosamente, el 90% de los encuestados están totalmente de acuerdo con que una mejor colaboración entre agencias gubernamentales u OGE y agencias de ciberseguridad tendría un impacto positivo en la postura general de ciberseguridad en los procesos electorales. Mostraría que, en una posición de implementación, hay buena voluntad. Sin embargo, la falta de recursos (tanto de capacidad humana como financiera) sigue siendo un obstructor del progreso.

Nivel de implementación de medidas de ciberseguridad para proteger el proceso democrático

De los resultados, se supo que el 50% de los encuestados indicaron que no tienen un presupuesto para la ciberseguridad asociado con el proceso democrático.

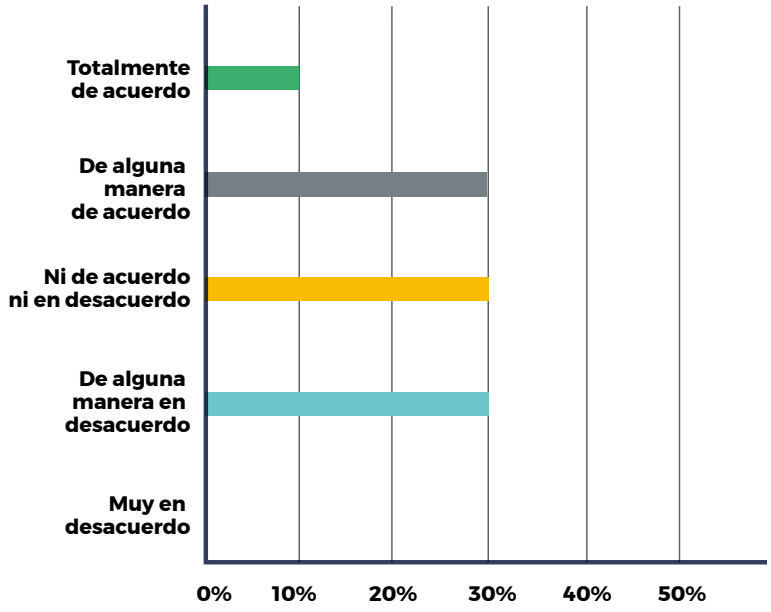

Figura 4. Pregunta: "Está de acuerdo o en desacuerdo con la siguiente declaración: Hay suficientes recursos dedicados a la ciberseguridad para el proceso electoral en mi país".

Existe la necesidad de tener más esfuerzos de sensibilización y comunicación sobre este tema para que los responsables de la toma de decisiones puedan comprender la urgencia en torno a la inclusión de medidas de ciberseguridad en apoyo del proceso democrático, y poner la ciberseguridad de primero en sus agendas.

Los resultados de la encuesta también indican que el 35% de los encuestados actualmente no están considerando la introducción de procesos de gestión de incidentes o planes de contingencia en caso de un ataque al proceso democrático. Además, más del 40% de los encuestados no estaban al tanto de los esfuerzos de coordinación entre la entidad responsable de una elección y el CSIRT local, si esto existe.

Desafíos comunes

Utilizando los resultados de la encuesta y los desafíos que enfrentan las partes interesadas en los campos electoral y democrático en el ciberespacio, se identificaron las siguientes categorías principales como desafíos comunes:

- ***Desafíos digitales***
- ***Capacidad humana***
- ***Voluntad política***
- ***Marco legal***
- ***Medidas de procedimiento***

Desafíos digitales

Los desafíos tecnológicos o digitales pueden describirse como el conocimiento o las capacidades que necesita cada parte interesada para proteger proactivamente los dispositivos utilizados en las actividades electorales. Por ejemplo, actividades como el registro de votantes, la comunicación con las partes interesadas, el acto de hacer campaña o incluso la recaudación de fondos están sujetas a amenazas debido a la incapacidad o falta de conocimiento que las partes interesadas tienen para proteger sus dispositivos contra posibles ataques cibernéticos. La falta de conocimiento e implementación de protocolos de seguridad básicos hace que las partes interesadas sean propensas a la suplantación de identidad (phishing), que interactúen con terceros que no son de fiar y potencialmente les entreguen información clasificada o secreta, lo que a su vez puede comprometer un sistema electoral en su conjunto.

Capacidad humana

El desafío de la capacidad humana consiste en los tipos de acciones y actividades que las personas realizan cuando se involucran con la tecnología en un entorno democrático o electoral. Estos pueden estar asociados con errores o el incumplimiento de los protocolos de ciberseguridad, así como la ausencia de un alto nivel de escrutinio al implementar estos protocolos. Los ejemplos comunes incluyen no proporcionar capacitación adecuada y continua para el personal, tener una alta tasa de rotación dentro de las organizaciones, no estar al tanto de los servicios disponibles para la protección, no tener regulaciones formales a seguir y no poder hablar sobre temas de ciberseguridad. Las reglas y las mejores prácticas requeridas para mejorar la ciberseguridad deben estar inmersas en la cultura y las actividades diarias de todos los interesados. La ausencia de mejores prácticas o la aplicación laxa de las mejores prácticas comprometen el rigor necesario para mantener la credibilidad de una institución democrática.

Voluntad política

La necesidad de aumentar la ciberseguridad como parte del debate político es quizás uno de los desafíos más apremiantes para todos los interesados en la región. A todas las partes interesadas les interesa tener un mayor reconocimiento de la importancia de la ciberseguridad y garantizar que las conversaciones se mantengan continuamente y se revisen regularmente para capitalizar acciones más tangibles sobre el tema. Si no hay un interés activo, todos los esfuerzos para mejorar la ciberseguridad pueden fallar.

Marco legal

Traducir el debate activo en políticas y legislación beneficia el proceso democrático y es otro desafío fundamental para todas las partes interesadas. Proporciona las mejores prácticas de ciberseguridad para que se conviertan en ley o políticas cuando sea necesario. Este apoyo legal permite que haya un esfuerzo organizado y coordinado que puede responder continuamente a cualquier amenaza emergente que pueda comprometer la democracia y el proceso electoral. Sin este marco, las partes interesadas no tendrán una orientación suficiente para instituir las mejores prácticas de ciberseguridad.

Medidas procesales

Esta gestión abarca múltiples capas en las cuales se debe organizar y monitorear la colaboración de manera continua. Los desafíos de procedimiento son complicados debido al hecho de que la ciberseguridad, en lugar de seguir siendo una responsabilidad individual, se convierte en un esfuerzo de colaboración. Por ejemplo, las partes interesadas deben reaccionar rápidamente ante ataques y amenazas y aumentar su presencia y auditorías internas. Si la ciberseguridad no se integra al ciclo democrático, la protección de la democracia en el ciberespacio no será sostenible.

Esfuerzos globales en ciberseguridad y democracia

Como se presentó anteriormente, la naturaleza y la percepción de la ciberseguridad aplicada a los procesos democráticos ha evolucionado a lo largo de los últimos años. Inicialmente, los esfuerzos se basaron más en la tecnología, con énfasis en los "ataques cibernéticos clásicos" dirigidos a las máquinas o software de votación, los sistemas de conteo u otras vulnerabilidades de codificación / criptografía[18] (Australia 2017).

Desde entonces, varias interferencias electorales han aumentado el nivel de conciencia sobre los ataques basados en la información, como la información errónea, la desinformación, las noticias falsas y la manipulación de la información (como se describió anteriormente en la sección "La conexión de ciberseguridad"). Como resultado, las mismas partes interesadas han incorporado el tema de los ataques basados en información en su diálogo local[19].

A medida que los ataques basados en la información cobraron impulso, también lo hizo la atención y la presión hacia las principales plataformas de redes sociales y su papel en la propagación de tales ataques. Afortunadamente, han tomado medidas para abordar el problema41, 42. Sin embargo, es fundamental implementar una vigilancia continua para garantizar un nivel de compromiso de acuerdo con los desafíos cada vez mayores, de manera transparente y responsable. Como se describe en el Informe de Libertad de Expresión e Internet de 2019, "es necesario insistir en la necesidad de que sus prácticas de moderación de contenido respeten las garantías fundamentales del debido proceso, la autoridad independiente, la transparencia, para que puedan fortalecer, enriquecer y ampliar el debate público"[20].

Un aspecto final que vale la pena mencionar cuando se trata de frustrar ataques basados en información es la educación electoral. Este documento ha incluido al votante como uno de los perfiles de las partes interesadas. El derecho al voto implica la responsabilidad de mantenerse informado y educado sobre asuntos relacionados con la votación. Hay varias herramientas disponibles para el votante, incluido el documento "Alfabetismo y seguridad digital" de la OEA

(OEA 2019) y las diversas iniciativas de verificación de los hechos en la región. Un votante educado reduce el éxito de los ataques basados en información. En esencia, todas las partes interesadas del proceso democrático se beneficiarían de hacer un esfuerzo adicional para facilitarles el acceso a los recursos educativos a los votantes.

Riesgo cibernético a nivel internacional

Los objetivos concretos de los ataques cibernéticos contra una elección suelen ser el sitio web de los OGE o las bases de datos de votantes. Desde un enfoque de costo / beneficio, a menudo es más eficiente lanzar un ataque contra estos objetivos, incluso si las posibilidades de que tenga éxito son muy bajas y se centre en generar dudas sobre la integridad de una elección[21].

Muchos atacantes saben que los recursos necesarios para comprometer la infraestructura de TI de una elección suelen ser bastante altos; y ellos o no tienen esos recursos, o no ven suficiente retorno en la inversión para que el ataque valga la pena. Según una publicación del Gobierno de Canadá, Actualización 2019: Amenazas cibernéticas al proceso democrático de Canadá, menos del 5% de los ataques cibernéticos contra el proceso democrático se dirigieron a dichos elementos de las elecciones (CSE 2019).

Aun así, los riesgos de un posible ataque contra la infraestructura central de TI no son insignificantes, especialmente en el caso de que un país permita el uso de herramientas de votación remota. La votación electrónica remota, incluidos su despliegue, los desafíos de seguridad y los últimos desarrollos, no es un tema cubierto en detalle en el presente documento, pero merece una atención futura ya que su papel es relevante y periódicamente atrae considerable atención.

Tradicionalmente, los ataques cibernéticos relacionados con los procesos electorales se centraban en los dispositivos electrónicos, el software o las conexiones de red involucradas. Sin embargo, la intensa popularización de las redes sociales ha permitido que haya un mayor número de ataques basados en información, en lo que podría considerarse una versión refinada de propaganda del siglo XXI. Según la Harvard Kennedy School (Harvard 2020), los incidentes basados en información se pueden clasificar de la siguiente manera:

a. Difusión de información falsa o engañosa con la ayuda de cuentas falsas de redes sociales, bots, etc., para desacreditar a los candidatos, el sistema de votación o los resultados.

b. Fugas de información confidencial sobre campañas, vulnerabilidades o comunicación privada para socavar la credibilidad del sistema.

c. Amplificación o debilitamiento del contenido en función de su fuente, favoreciendo las opiniones polarizadoras o populistas que intentan transladar el foco de los medios y los votantes a temas inmediatos y no relevantes.

La prevalencia reciente de este tipo de amenaza cibernética también debe explicarse a través de la aparición de dos mecanismos de amplificación: bots (actores automáticos o semiautomáticos que involucran cuentas falsas de Twitter o Facebook) y trolls (personas que prácticamente acosan,

calumnian o manipulan) (Vilmer 2018). Como ejemplo, y de acuerdo con la misma fuente, hubo un incidente en el que una fábrica de trolls compuesta por unas pocas docenas de personas controlaba, a pesar de su tamaño y recursos limitados, más de 3,800 cuentas individuales, 50,000 bots y llegó a más de 150 millones de personas a través de Facebook e Instagram.

Los ataques basados en información en la región de la OEA también han sido influenciados por los siguientes factores:

a. Recesiones económicas en varios países de la región.

b. Un marco regulatorio generalmente menos desarrollado y estricto que el de Europa o Estados Unidos.

c. El rápido aumento en la penetración de dispositivos móviles, seguido de un salto en la utilización de las redes sociales en la región, especialmente Facebook y WhatsApp (Vilmer 2018).

Si bien el aumento de los ataques basados en información ha sido notable en los últimos años, también es cierto que el nivel de conciencia ha aumentado entre los interesados en la región, con iniciativas interesantes para prevenir campañas de desinformación como en Brasil, Argentina[22] y México[23].

La discusión, el debate y la sensibilización continuas son esenciales para ser siempre resilientes en la lucha contra las amenazas cibernéticas tanto para las elecciones como para el proceso democrático en su conjunto. El objetivo de los ataques cibernéticos en las elecciones es socavar la confianza del público en el proceso democrático y el sistema electoral. El eslabón perdido para proteger las elecciones de los ataques cibernéticos es comprender completamente lo que el "adversario" quiere obtener del ataque.

El proceso democrático: Infraestructura institucional y consideraciones de ciberseguridad

Este documento ha abordado la amenaza de seguridad para la democracia y los procesos que la respaldan. Hemos visto que la amenaza no es específica de una región; es una amenaza que el mundo entero está enfrentando en todo el espectro político. El siguiente paso es considerar algunos de los componentes críticos necesarios para facilitar los procesos democráticos. A partir de ahí, podemos considerar cómo abordar el riesgo cibernético dados los diferentes niveles de capacidad institucional, y las consideraciones de ciberseguridad necesarias para mitigar parte de este riesgo.

Un marco legal integral

Es esencial considerar el marco legal que apoya a las diversas instituciones que defienden nuestra democracia.

Conceptualmente, el término Marco legal para las elecciones generalmente se refiere a un conjunto de leyes y reglas que incluyen: las disposiciones aplicables en la constitución, la ley electoral, las leyes sobre los partidos políticos, así como los reglamentos relacionados con la ley electoral y las instrucciones y reglamentos emitidos por el OGE a cargo. El marco legal de cada país y territorio tiene particularidades cuando se trata de elecciones democráticas, aunque hay algunos aspectos comunes clave.

A nivel mundial, por ejemplo, el artículo 21 de la Declaración Universal de Derechos Humanos introduce un conjunto de principios básicos para las elecciones democráticas:

> *"Toda persona tiene derecho a participar en el gobierno de su país, directamente o por medio de representantes libremente elegidos.*
>
> *La voluntad del pueblo será la base de la autoridad del poder público; esta voluntad se expresará mediante elecciones auténticas que habrán de celebrarse periódicamente, por sufragio universal e igual y por voto secreto u otro procedimiento equivalente que garantice la libertad del voto". (ONU 1948)*

Paralelamente, el Consejo de Europa declara que:

"...los cinco principios del patrimonio electoral europeo (sufragio universal, igual, libre, secreto y directo) es esencial para la democracia"[26].

Cuando se piensa en las disposiciones legales que deberían estar operando, vale la pena considerar lo siguiente[24]:

- Legislación que reconozca la necesidad de proporcionar disposiciones para la persecución los delitos digitales relacionados que afectan el proceso democrático. Estas disposiciones deben respetar los derechos humanos fundamentales, como la libertad de expresión.

- El mantenimiento y la actualización del registro electoral, el registro de partidos y candidaturas, y el registro de votación, incluidos los requisitos específicos de manejo y protección de datos.

- Las reglas sobre financiamiento de partidos y transparencia en las fuentes de financiamiento, especialmente para publicidad política.

Además, la OEA define el concepto de elecciones democráticas (SG / OEA 2011) cuando cumplen las siguientes cuatro condiciones básicas:

- Elecciones inclusivas
- Elecciones limpias
- Elecciones competitivas y
- Cargos de elección popular

TABLA 1. EL CONCEPTO DE ELECCIONES DEMOCRÁTICAS I: UNA PRIMERA APROXIMACIÓN

Implementación de tecnología en el proceso democrático

Para ilustrar ejemplos de otros países fuera de América Latina y el Caribe, la implementación de soluciones tecnológicas en procesos democráticos se hizo cada vez más popular a principios de la década de 2000 después del escándalo de las elecciones generales de ese año en Estados Unidos con motivo de las tarjetas perforadas en Florida[25]. Durante esos años, varios países lanzaron pilotos de votación electrónica, incluidos Francia, Alemania, los Países Bajos, el Reino Unido y Noruega. Cada país adoptó un enfoque único al respecto, contribuyendo a la atomización continua del espacio tecnológico.

Algunos de ellos, como Estados Unidos, Francia y Suiza, priorizaron a sus votantes no residentes. En contraste, otros han limitado las experiencias al nivel local o regional, como en el caso de Canadá y Australia. Después de eso, varios de esos países han decidido suspender los pilotos, como fue el caso de los Países Bajos, el Reino Unido, Noruega y Alemania debido a la dificultad de asegurar simultáneamente la verificabilidad y la privacidad de extremo a extremo.

Sin embargo, como ejemplo alternativo, Estonia ha demostrado un crecimiento constante en apoyo de las soluciones de votación por Internet, al implementar la votación por Internet (i-Voting) para cada elección vinculante en el país para la totalidad del electorado desde 2005 (Toots 2016).

En los últimos años, fuertes defensores de las soluciones de votación basadas en Internet, como Australia y Suiza, han identificado varias fallas en estos sistemas y están pidiendo una introducción gradual y cuidadosa de las tecnologías de votación electrónica (Lewis 2019). Cada país es diferente, al igual que las legislaciones electorales y las infraestructuras de ciberseguridad disponibles. Lo que ha resultado válido para un territorio generalmente no es aplicable en otros casos. La opción más recomendable es un enfoque cuidadoso en términos del tipo de elección y electorado a los que se les permite usar tecnología para votar (Blanco 2018).

Medios de comunicación

Los medios de comunicación, incluidos los medios de comunicación tradicionales y los proveedores de redes sociales, son fundamentales para lograr una comunicación clara. Esta comunicación clara se vuelve aún más crítica durante un ataque cibernético, y más específicamente, en una campaña de desinformación. Un ambiente que permita la libertad de expresión siempre ha sido esencial para una democracia saludable.

Algunas de las funciones principales de los medios de comunicación durante una elección incluyen proporcionar información sobre los partidos políticos y los candidatos que participan en el proceso, ofrecer preguntas para el debate, informar sobre el proceso de votación y cualquier otro elemento que fomente un proceso informado para el electorado. Es importante la imparcialidad y la presentación equilibrada de la cobertura de las noticias electorales (cobertura que no presente programas o artículos que favorezcan a un candidato o partido político en particular). En otras palabras, se debe mantener la independencia de los medios.

La OEA ha trabajado para fortalecer la capacidad de los actores de los medios en el proceso democrático y desarrolló la publicación Fortaleciendo los procesos y sistemas electorales en todo el hemisferio: el papel de los medios en las campañas electorales y la relación entre los órganos de gestión electoral y los partidos políticos (SG / OEA 2011). En ese documento, se destacó que:

> *Las autoridades electorales deberían desarrollar mecanismos para colaborar con los medios de comunicación a fin de garantizar el respeto de tres principios democráticos básicos: la responsabilidad de garantizar la igualdad de acceso a la información, el derecho de los medios a informar y el derecho de los ciudadanos a ser informados. Estos derechos se aplican por igual a partidos políticos, candidatos e incluso a autoridades electorales. Tanto los partidos políticos como los candidatos tienen derecho a informar al público sobre sus propuestas y plataformas, y las autoridades electorales deben informar al público sobre el proceso de votación en sí. En la realización de estas tareas, la relación entre los medios y las autoridades electorales es claramente interdependiente.*

Más específicamente, la OEA reconoce que las Autoridades Electorales deben ser especialmente conscientes de los avances de los medios en la era digital y la aparición de los llamados "nuevos medios". Numerosas fuentes informan cada vez más a las personas más allá de los formatos tradicionales de radio, televisión y periódicos. En cambio, se están volcando a Internet y otros medios digitales, que se han vuelto extremadamente influyentes en la forma en que se produce y se difunde la información.

Es importante reconocer que la libertad de prensa y un sistema de medios de comunicación pluralista son elementos clave para garantizar procesos electorales libres y justos. La OEA desarrolló la "Metodología para la observación de medios de comunicación en elecciones: un manual para las misiones de observación electoral de la OEA", que siguen las diferentes MOE (SG / OEA 2011). Esa publicación reconoce el importante papel de los medios durante los procesos electorales, ya que, a pesar del progreso observado en la organización de los procesos electorales en la región, es crucial tener en cuenta que las condiciones de acceso a los medios tienen una influencia significativa en las condiciones para competir en igualdad de condiciones para cargos electorales.

Participación comunitaria en procesos democráticos

Es una consideración fundamental que cualquier OGE, o función con una responsabilidad similar, respete los principios de independencia y autonomía mientras el OGE realiza su mandato. Además de la capacidad institucional descrita anteriormente, mostrar independencia y autonomía fomenta la confianza entre las instituciones y el electorado al que sirve el OGE.

Tanto el electorado como las instituciones deben confiar y tener la certeza de la independencia y autonomía de un OGE para que puedan trabajar juntos para garantizar la realización exitosa de cualquier proceso democrático. Puede que no esté muy claro que se requiere colaboración aquí. Aun así, para garantizar la realización fluida, justa y transparente de un proceso electoral, la colaboración es esencial debido a la naturaleza de la responsabilidad compartida de la ciberseguridad nacional. Todas las partes interesadas deben comprender sus roles y responsabilidades en un proceso electoral y el riesgo de ciberseguridad asociado a él.

Las Tecnologías de la Información y la Comunicación (TIC) influyen en la vida cotidiana de miles de millones de ciudadanos en los sectores de educación, salud, finanzas y más. Del mismo modo, las TIC también están teniendo una influencia e impacto comparables en numerosos elementos de los procesos electorales y democráticos. Por ejemplo, las campañas electorales se ejecutan de manera significativamente diferente. El público accede a noticias e información a través de plataformas de redes sociales, así como a diálogo y debate, y se lleva a cabo principalmente en línea. El compromiso con todas las partes interesadas ha cambiado bajo la influencia de las TIC, y los mecanismos digitales resultantes utilizados para los procesos democráticos pueden generar desafíos, que a su vez pueden influir en diversos grados en las partes interesadas que son parte integral del proceso democrático.

Los responsables de gestionar y apoyar un proceso electoral deben demostrar independencia tanto de las administraciones en funciones como de los partidos de oposición. No se debe subestimar la realidad de este desafío. Este capítulo ofrece algunas ideas para los OGE con respecto al fomento de la confianza a través de la transparencia y la rendición de cuentas entre los diversos interesados identificados.

Es solo a través de una sólida participación de los interesados que las instituciones pueden comenzar a mitigar el riesgo de la amenaza. La mitigación del riesgo y la creación de confianza son los objetivos finales de la participación con la comunidad y los grupos específicos de partes

interesadas. La intención de la participación y su alcance deben estar claramente definidos desde el principio. Esta participación es una oportunidad para que el OGE sea estratégico para maximizar los recursos que puedan estar disponibles para las elecciones. Existen razones importantes por las cuales la participación con las partes interesadas es clave para lograr la buena conducta de un proceso democrático. Por ejemplo:

1. Un OGE que mantiene la confianza de todos los grupos de partes interesadas a través de procesos transparentes y autonomía e independencia demostrables asegura una buena conducta dentro de los procesos democráticos.

2. Un OGE permite garantizar que cada parte interesada comprenda sus responsabilidades y las de sus pares.

3. Un OGE puede compartir mensajes de ciberseguridad y mejores prácticas de ciberseguridad, mejorando así el perfil de riesgo cibernético para el país.

4. Un OGE fomenta la colaboración entre las partes interesadas.

La participación con las partes interesadas identificadas debe mantenerse durante los períodos cíclicos del proceso democrático. Las partes interesadas siempre deben entender por qué se lleva a cabo la participación y quienes lideran la participación deben ser sinceros sobre el propósito y el objetivo del ejercicio. Una forma de hacer esto es ofrecer una invitación para participar que explique completamente la intención de la participación desde el principio. Si las partes interesadas continúan su participación, el OGE debe mantener el alcance y los objetivos del ejercicio de participación muy presente en cada comunicación entre el OGE y las partes interesadas relevantes.

Ya sea que una nación elija establecer una entidad separada con responsabilidad para los procesos democráticos (véase el resumen de todas las consultas en el Anexo II) o simplemente elija una función dentro del gobierno, podemos suponer que existe la intención de seguir buenas prácticas para fomentar la percepción de independencia en un electorado. Es necesario, si no vital, defender el principio de independencia para esta responsabilidad porque establece la confianza de los votantes en el proceso democrático. Sin la confianza del votante en el proceso en sí, es probable que la participación de esas mismas personas sea mínima, lo que resulta en un electorado desconectado, que es un signo de una democracia poco saludable.

El objetivo principal de cualquier OGE es celebrar una consulta basada en la transparencia y la rendición de cuentas. Para alcanzar este objetivo, la autoridad identificada debe establecer una posición de confianza entre todos los interesados identificados y los diferentes sectores que representan.

Es a través de una participación sostenida a largo plazo y comunicaciones claras a lo largo de todo el ciclo de un proceso democrático que una entidad a cargo o una función a cargo puede garantizar que no se perciba ningún sesgo dentro de sus operaciones y así retener la autonomía y la independencia.

Participación con las partes interesadas

En un contexto gubernamental, se ha asociado la ciberseguridad en gran medida con las comunidades de inteligencia, a veces asentadas en el ejército. A medida que el mundo lo comprende mejor, y hay una aceptación de que la ciberseguridad no es solo una consideración técnica para las comunidades de inteligencia, se requiere un enfoque multidisciplinario que ponga a las personas en el centro. Hemos notado un aumento en las entidades o agencias que se están estableciendo fuera de las comunidades de inteligencia tradicionales para permitir que la entidad se relacione más directamente con el público [26].

No es frecuente que exista una entidad de este tipo en países particulares del mundo. La existencia de una organización centrada en la ciberseguridad no es una disposición general que resuelva todos los problemas abordados en este documento. En algunos casos, la geografía es tan irregular que una agencia nacional puede no ser la respuesta apropiada para el desafío de la ciberseguridad. Al no contar con una agencia como se describió anteriormente, el OGE puede buscar colaborar con otros profesionales acreditados en ciberseguridad para involucrar a las partes interesadas en el período previo a un período electoral como parte de la participación continua a lo largo del ciclo de vida del proceso democrático. La colaboración es esencial, especialmente si no se establece una entidad aparte para administrar y supervisar la realización de un proceso democrático porque el tiempo y los recursos se verán impactados dramáticamente. A través de la colaboración, el alcance podría ser más efectivo y eficiente al incluir al principio experiencia en ciberseguridad.

Partes interesadas esenciales a considerar

Es difícil ser integral al decidir qué partes interesadas deben incluirse en un programa de participación. No existe una lista única que pueda servirle a un grupo de países tan diversos como son los miembros de la Organización de los Estados Americanos. La siguiente es una categorización que puede sugerir la amplitud de las partes interesadas que deberían ser consultadas e invitadas a participar en dicho programa de participación y comunicación. Se puede encontrar una descripción más detallada de los grupos de partes interesadas en el Anexo I.

- ***Actores políticos***

  Los candidatos políticos, así como los partidos políticos, deben ser parte de la conversación de ciberseguridad en lo que respecta al proceso democrático. No solo deben ser conscientes del riesgo, sino que deben asegurarse de que operan con una mentalidad de datos y una comprensión de la conducta y ejecución adecuadas de las campañas políticas. Deben ser informados del riesgo interno y garantizar que se adopten las mejores prácticas en términos de todos los asuntos relacionados con la protección de datos y la privacidad.

- ***Público en general***

  Es importante garantizar que el público en general, el 'votante', tenga una comprensión básica de los riesgos de ciberseguridad y las habilidades esenciales necesarias para ser un ciudadano digital informado. La participación directa con el público en general no debe ser definido

demográficamente. Se debe considerar e implementar un aumento general en la conciencia del riesgo y la amenaza en todos los ámbitos, siempre que sea posible. La participación de la sociedad civil al respecto sería de gran beneficio para sensibilizar al público en general.

• ***Actores gubernamentales involucrados en el proceso***
Los servidores públicos que tienen alguna responsabilidad en la realización y ejecución de un proceso democrático, pero que no necesariamente son expertos en ciberseguridad o tienen conocimientos básicos sobre el riesgo de ciberseguridad, son un grupo de partes interesadas válido. Al involucrarlos en una conversación sobre la planificación de gestión de riesgos y crisis, estarán mejor equipados para enfrentar una crisis en caso de que ocurra. Esta agrupación también podría incluir representantes electos y funcionarios electos que pueden no ser conscientes del riesgo de ciberseguridad que enfrentan.

• ***Proveedores de servicios de Internet y medios: impresos, radio, radiodifusión***
Los medios de comunicación deben incluirse en cualquier programa de participación para que puedan estar mejor informados sobre el panorama de riesgos. Deben estar preparados para planificar internamente cualquier ataque de ciberseguridad que puedan enfrentar durante el proceso democrático y antes de una elección. Los medios de comunicación (incluidas las redes sociales) contribuyen significativamente al debate público tanto en línea como a través de los canales de transmisión tradicionales, por lo que su participación es necesaria y debe considerarse parte de la infraestructura crítica de la región.

• ***Organizaciones de respuesta a incidentes***

- Equipos de respuesta a incidentes

Es crucial que la capacidad nacional de respuesta a incidentes, si existe, sea parte de esta conversación. No solo es importante que el CSIRT nacional comprenda su papel y responsabilidad en ocasiones especiales, como en las elecciones generales, sino que es de mayor importancia que los actores críticos de la infraestructura nacional comprendan el papel del equipo nacional del CSIRT. Es mejor involucrar también a los equipos más pequeños de respuesta a incidentes, como los equipos regionales y los sectoriales, para que, en su proceso preparatorio y establecimiento de escenarios, se pueda establecer una cadena de mando o una cadena de comunicación.

La entidad CSIRT nacional podría realizar sus propias consultas con sus unidaddes constructivas, recordándole a cada unidad sus términos de referencia específicos para cada equipo. Esta actividad alentaría la claridad sobre las referencias a los que responden y las agencias de aplicación de la ley. Las consultas a los grupos también podrían impulsar la planificación de la gestión de crisis con ejercicios de escenarios implementados para garantizar la sostenibilidad de los planes. A través de las consultas de la Agencia Nacional CSIRT, habrá una mayor urgencia para establecer vínculos sólidos entre las unidades constructivas y varios medios de comunicación para garantizar el manejo de mensajes en caso de un incidente.

- Proveedores de Infraestructura Nacional Crítica (CNI, por sus siglas en inglés).

Por lo general, se considera que un proveedor de CNI es de servicios de transporte, servicios públicos y control fronterizo. Es importante involucrar a estos proveedores de servicios para asegurarse de que sean conscientes del riesgo cibernético en cualquier proceso democrático. Es importante alentar a las partes interesadas a que se involucren con expertos en ciberseguridad y realicen auditorías periódicas y escenarios de crisis para elaborar de manera efectiva un plan de gestión de crisis en caso de que uno de sus servicios sea atacado durante un período de importancia democrática.

La participación con este sector, ya sea directamente o a través de la agencia nacional CSIRT, debe usarse para alentar la planificación de la gestión de crisis, las verificaciones de auditoría y los ejercicios de escenarios regulares centrados en procesos democráticos (elecciones o referendos).

El valor de garantizar que todas estas partes interesadas sean parte del plan de participación radica en establecer una comprensión mutua de los roles y responsabilidades de cada actor en el proceso. Ayuda a ilustrar sobre los roles y responsabilidades de los diversos actores y cuándo o cómo es esencial escalar a la siguiente línea de supervisión. La comunicación puede conducir a la identificación de lagunas de información entre los grupos de partes interesadas.

Facilitar el diálogo y considerar los próximos pasos - Recomendaciones

Estas recomendaciones se desarrollaron teniendo en cuenta el proceso descrito en este documento. El proceso incluyó una revisión cuidadosa del panorama de amenazas de ciberseguridad en el proceso democrático, una reflexión sobre el poder de la información en la era digital, y la identificación y participación de las partes interesadas y los desafíos asociados, que se han dividido en:

- Desafíos digitales
- Capacidad humana
- Voluntad política
- Marco legal
- Medidas procesales

Luego, las recomendaciones se definieron y clasificaron por agrupación de partes interesadas con el objetivo principal de facilitarle al lector identificar la agrupación de partes interesadas y tener una pauta de los pasos a considerar para aumentar su preparación para la ciberseguridad.

A continuación, se muestra una tabla resumen sobre la lógica y las diferentes categorías de la lista de recomendaciones:

Dado que ciertas partes interesadas comparten algunas características, parte de las recomendaciones están presentes en más de un perfil, especialmente en asuntos relacionados con la sensibilización, la capacitación o la independencia.

Desafíos digitales

Los desafíos digitales se pueden describir como el conocimiento o las capacidades que necesita cada parte interesada para proteger proactivamente los dispositivos utilizados en las actividades electorales y el sistema democrático.

Actores Políticos

1. Tener en cuenta cuáles son las mejores prácticas de ciberseguridad para todos los dispositivos que utilizan, como dispositivos móviles y computadoras portátiles o de escritorio.

2. Tener en cuenta cuáles son las mejores prácticas de ciberseguridas para software en particular para lo que respecta a los datos almacenados sobre los electores locales.

3. Comprender las normas locales de protección de datos y privacidad, particularmente en lo que respecta a los datos almacenados sobre los electores locales.

Público en general

1. Tener en cuenta cuáles son las mejores prácticas de ciberseguridad para todos los dispositivos que utilizan, como dispositivos móviles y computadoras portátiles o de escritorio.

2. Tener en cuenta cuáles son las mejores prácticas de ciberseguridas para software en particular para lo que respecta a los datos almacenados sobre los electores locales.

3. Conocer las herramientas y servicios que existen para verificar la información durante un ciclo electoral, como el documento de la OEA "Alfabetización mediática y seguridad digital".

Actores gubernamentales u OGE

1. Tener en cuenta cuáles son las mejores prácticas de ciberseguridad para todos los dispositivos que usan los miembros de OGE, como dispositivos móviles y computadoras portátiles o de escritorio.

2. Tener en cuenta cuáles son las mejores prácticas de ciberseguridas para software en particular para lo que respecta a los datos almacenados sobre los electores locales.

3. Considerar los activos criticos de los sistemas de infraestructura de información clave y segregarlos, permitiendo el control de acceso redundante (electrónico y analógico).

4. Establecer relaciones con las compañías de redes sociales y los proveedores de servicios de Internet para garantizar que la información pueda ser verificada y corregida según sea necesario.

5. Ayudar a identificar más recursos financieros y humanos para mejorar la seguridad de las herramientas y procesos de digitalización.

ORI

1. Proporcionar estándares y pautas para las partes interesadas clave sobre la línea de base mínima de ciberseguridad, como son implementar la autenticación de 2 factores, las mejores prácticas de protección de contraseña, actualizaciones de software / firmware y realizar pruebas de penetración exhaustivas y auditorías de código.

2. Establecer reclutamiento de talentos para especialistas en ciberseguridad.

Capacidad humana

El desafío de la capacidad humana consiste en los tipos de acciones y actividades que las personas realizan cuando se involucran con la tecnología en un entorno democrático o electoral. Estos pueden estar asociados con errores o el incumplimiento de los protocolos de ciberseguridad, así como la ausencia de un alto nivel de escrutinio al implementar estos protocolos.

Actores Políticos

1. Implementar las mejores prácticas de contraseña, así como mantener actualizadas las versiones de software / firmware y considere adoptar Cloud Solutions de un proveedor de confianza para ayudar en la seguridad de extremo a extremo.

2. Informar a CSIRT / ORI y OGE sus cuentas oficiales de redes sociales y cualquier comunicación, evento o incidente sospechoso.

3. Establecer fuertes lazos y relaciones con las compañías de redes sociales y los proveedores de servicios de Internet. Identificar colaboradores (cuando sea necesario) y establecer una asociación de colaboración para establecer un programa de participación cuando sea necesario.

4. Implementar la autenticación de 2 factores para dispositivos y cuentas compatibles con Internet.

Público en general

1. Mantenerse informado del panorama de amenazas a través de canales oficiales e informar al CSIRT / ORI y al OGE de cualquier comunicación, evento o incidente sospechoso durante el proceso electoral.

2. Adquirir información relevante de múltiples fuentes sobre procesos democráticos.

3. Verificar la información electoral antes de compartirla en las redes sociales.

Actores gubernamentales u OGE

1. Implementar una buena "higiene cibernética", como la autenticación de 2 factores, buenas prácticas de contraseña y actualizaciones oportunas de software y firmware, y administrar la cadena de suministro de sistemas de información que respalden procesos democráticos.

2. Dado que los sistemas auxiliares son cada vez más objetivos de ataques cibernéticos, evitar los "nodos críticos de falla" que, si se ven comprometidos, eliminan todo el sistema, como en el caso de un ataque DDoS.

3. Desarrollar mecanismos para colaborar con los medios de comunicación para garantizar el respeto de tres principios democráticos básicos: la responsabilidad de garantizar el acceso equitativo a la información, el derecho de los medios de informar y el derecho de los ciudadanos a ser informados.

Medios de comunicación

1. Informar a CSIRT / ORI y OGE de sus cuentas oficiales de redes sociales e informar a CSIRT / ORI y OGE sobre cualquier comunicación, evento o incidente sospechoso.

2. Monitorear incidentes facilitados por bots, trolls y herramientas de publicación automatizadas.

3. Mejorar la verificación de hechos a través de fuentes oficiales o partes confiables.

4. Establecer vínculos y relaciones sólidas con las compañías de redes sociales y los proveedores de servicios de Internet y mantener canales de comunicación para facilitar la reducción de entregar información errónea al público.

ORI

1. Implementar un enfoque unificado para la integridad de los datos, de conformidad con los estándares de ciberseguridad, y mantener controles sobre las soluciones tecnológicas y los datos.

2. Implementar tecnologías compatibles con los sistemas del OGE y realizar pruebas de seguridad combinadas, asegurando la compatibilidad técnica con las soluciones digitales del OGE.

3. Preparar un código de conducta para ser firmado por el personal y los asociados con respecto a las plataformas de redes sociales e implementar políticas (que se adhieran a los principios de privacidad) sobre monitoreo de redes, análisis de archivos de registro, segmentación de privilegios de usuario y un enfoque que no sea de caja negra para reducir amenazas internas.

Voluntad política

La necesidad de aumentar la ciberseguridad como parte del debate político es quizás uno de los desafíos más apremiantes para todos los interesados en la región.

Actores Políticos

1. Hacer de la ciberseguridad una prioridad de seguridad nacional con un enfoque público-privado. Este nivel de prioridad garantizará la sostenibilidad durante los períodos cíclicos, lo que permitirá una mayor intensidad durante un período electoral.

2. Mantener el tema de la ciberseguridad en los procesos democráticos como una tendencia para contrarrestar la propensión a que sea pasado por alto cuando no están en período electoral. Introducir la ciberseguridad y promover la prevención de la manipulación de la información como parte integral del plan de estudios de educación obligatoria.

3. Colaborar para desarrollar, construir y mantener regímenes completos de protección de datos y comprometerse a salvaguardar la neutralidad de Internet.

4. Apoyar la creación de canales de comunicación oficiales para actualizar en tiempo real los incidentes relacionados con procesos democráticos (piratería y manipulación de información). Tener en cuenta los ataques cibernéticos y la manipulación de la información a otros procesos democráticos que conducen a su período electoral.

5. Comprometerse con el establecimiento de un grupo específico de jueces y fiscales especializados en ciberseguridad y manipulación de información para resolver asuntos urgentes dentro de las 48 horas.

Público en general

1. Participar en movimientos de sociedad civil respetados relacionados con la ciberseguridad para promover la transparencia y la apertura durante los procesos democráticos.

2. Aumentar la influencia siendo parte activa del debate político y de consultas legislativas a través de la sociedad civil.

Actores gubernamentales u OGE

1. Trabajar con las autoridades elegidas en períodos no electorales para crear conciencia sobre la importancia de la ciberseguridad.

2. Mantener la independencia de la presión política, del lobby y de las grandes corporaciones.

Medios de comunicación

1. Solicitar activamente a su gobierno para que aumenten los recursos para el desarrollo de capacidades y la capacitación de los actores de los medios en ciberseguridad.

2. Mantener el tema de la ciberseguridad en los procesos democráticos como tema tendencia para contrarrestar la propensión a ser pasado por alto fuera del período electoral, a través de la publicación de artículos y otros temas relevantes para mantener informado al público.

3. Permanecer atento en la salvaguarda de la neutralidad de Internet y la libertad de expresión.

4. Mejorar la verificación de hechos a través de fuentes oficiales o actores fiables y participar en clasificaciones reconocidas internacionalmente para evaluar la confiabilidad de los medios.

ORI

1. Generar confianza con los votantes y los diferentes medios a través de canales de comunicación disponibles permanentemente.

2. Asegurar los recursos informáticos, independientemente del partido político.

3. Colaborar con las partes interesadas clave para desarrollar, construir y mantener regímenes completos de protección de datos.

4. Delimitar la interferencia política en la ORI.

5. Nombrar a un auditor principal políticamente independiente y cooperar con organismos internacionales y regionales y / u observadores independientes.

Marco legal

Traducir el debate activo en políticas y legislación beneficia al proceso democrático y es otro desafío fundamental para todas las partes interesadas.

Actores Políticos

1. Fortalecer los marcos legales para la protección de datos personales, la transparencia de la publicidad electoral y la manipulación de la información [27].

2. Revisar la legislación pertinente para abordar las preocupaciones de ciberseguridad en los procesos democráticos.

Público en general

1. Mantenerse al tanto de cualquier problema de ciberseguridad que se debata en todos los niveles del gobierno y entregarle comentarios a su representante.

Medios de comunicación

1. Participar activamente en los procesos de consulta legislativa para introducir actualizaciones normativas relacionadas con la ciberseguridad

ORI

1. Introducir el marco legal requerido para la ciberseguridad y la mitigación de riesgos en procesos democráticos basados en la última versión disponible de estándares reconocidos ,como la familia ISO 27K.

2. Establecer un grupo interno a cargo de presentar propuestas de mejora legal y participar en los comités de actualización legislativa electoral.

3. Desarrollar instrumentos legales para apoyar el establecimiento de un marco permanente para la ciberseguridad, como un grupo de trabajo y un presupuesto dedicado a la ciberseguridad.

Medidas procesales

Este esfuerzo abarca múltiples instancias en las cuales se debe organizar y monitorear la colaboración de manera continua. Los desafíos de procedimiento son complicados debido al hecho de que la ciberseguridad, en lugar de seguir siendo una responsabilidad individual, se convierte en un esfuerzo de colaboración.

Actores Políticos

1. Establecer una estructura clara en el organismo independiente recién creado, de modo que este organismo pueda ser ágil en las respuestas a los ataques de ciberseguridad.

2. Establecer un sistema de informes para denunciar cualquier comportamiento sospechoso o posible incidente cibernético en la campaña.

3. Apoyar a la sociedad civil y al periodismo de calidad, independientemente de la ideología, para garantizar la transparencia y la apertura al debate durante cualquier proceso democrático.

Público en general

1. Informar rápidamente al OGE / ORI sobre cualquier comportamiento sospechoso o posible incidente / manipulación de campaña.

Actores gubernamentales u OGE

1. Realizar simulaciones periódicas de piratería y manipulación de información coordinadas con el CSIRT / ORI y los medios de comunicación como parte de las actividades de capacitación.

2. Conjuntamente con la Agencia responsable de ciberseguridad diseñar e implementar una política y protocolos integrales de Evaluación y Gestión de Riesgos.

3. Diseñar, implementar y actualizar un Plan de Mitigación de Riesgos mucho antes de las elecciones con el asesoramiento de la ORI.

4. Aumentar los controles / auditorías internas para minimizar las amenazas internas y establecer un plan de comunicación seguro con un Sistema de gestión de contenido (CMS, por sus siglas en inglés) actualizado y compartirlo con el CSIRT / ORI.

5. Desarrollar un programa de participación y un plan y presupuesto de comunicación asociado. Este programa incluiría un protocolo de comunicación para ataques, mejorando la

transparencia tanto como sea posible, sin ser contraproducente en términos de filtraciones de detalles que podrían ayudar a posibles intrusos.

6. Implementar medidas para la divulgación responsable de ataques cibernéticos e incidentes de intentos de manipulación de información.

7. Coordinar con CSIRT / ORI para aumentar la resistencia del sitio web oficial contra los ataques cibernéticos y establecer un grupo de trabajo permanente con el OGE para hacer cumplir los protocolos de ciberseguridad. Este grupo de trabajo debe coordinarse con los representantes del grupo de medios (medios tradicionales, corporaciones privadas, sociedad civil y organizaciones multilaterales) para mantenerlos actualizados en tiempo real sobre noticias / incidentes relevantes.

8. Implementar controles cruzados de seguridad para infraestructuras críticas e implementar controles de acceso estrictos a sitios físicos de los sistemas de información, especialmente los servidores que soportan procesos democráticos.

Medios de comunicación

1. Las plataformas digitales deben considerar los procesos democráticos como una unidad de negocios rentable sujeta a cumplir con una ética rigurosa.

2. Cumplir cuidadosamente las normas de privacidad de información y datos.

3. Crear y mantener una base de datos oficial de cuentas falsas y grupos de medios, perfiles de redes sociales, empresas privadas y organizaciones no confiables.

4. Informar rápidamente al OGE / ORI cualquier comportamiento sospechoso o posible incidente / manipulación de campaña.

5. Establecer una relación con el OGE y ORI para mantenerlos actualizados en tiempo real sobre noticias / incidentes relevantes si se descubren, para alentar una respuesta más rápida a los incidentes.

6. Fomentar que las plataformas digitales cooperen con investigadores independientes y académicos para mejorar la respuesta a la manipulación de la información.

7. Mejorar la detección y el tiempo de respuesta a la manipulación de la información, especialmente con respecto a bots, netbots y cuentas anónimas.

ORI

1. Diseñar, implementar y actualizar un protocolo detallado de vigilancia cibernética tanto para amenazas cibernéticas como para actividades de manipulación de información.

2. Implementar mecanismos de detección temprana y coordinar con las políticas de mitigación de riesgos y respuesta cibernética del OGE.

3. Conjuntamente con el OGE, diseñar e implementar una política y protocolos integrales de evaluación y gestión de riesgos.

4. Crear un Equipo de Respuesta a Incidentes designado para procesos democráticos y desarrollar planes de comunicación dirigidos por grupo de partes interesadas con información sobre incidentes de ciberseguridad e intentos de manipulación de información.

5. Establecer campañas de mensajes de concientización sobre ciberseguridad para mantener informado al público y crear una persona / grupo designado para monitorear la ocurrencia de desinformación e informes.

6. Establecer un grupo de trabajo permanente con representantes de los grupos de medios (medios tradicionales, corporaciones privadas, sociedad civil y organizaciones multilaterales) para mantenerlos actualizados en tiempo real sobre noticias / incidentes relevantes.

7. Establecer un grupo de trabajo permanente con el OGE para hacer cumplir los protocolos de ciberseguridad.

8. Realizar ejercicios de fortalecimiento y simulaciones de manipulación de información coordinados con el OGE y los medios de comunicación como parte de las actividades de capacitación para mejorar los planes de respuesta a incidentes cibernéticos.

Conclusión

En resumen, surgen tres desafíos predominantes en la región:

- **Conciencia** para todos los actores involucrados en el proceso democrático.

- **Marcos legislativos que contengan disposiciones** para la coordinación de las políticas de ciberseguridad en los procesos democráticos con un sentido de urgencia, ya que las amenazas cibernéticas en el campo están claramente en aumento.

- **Continuidad:** la naturaleza inherente de un proceso democrático tiende a poner el aspecto de la ciberseguridad en el centro de atención antes de las elecciones y el día de las elecciones, perdiendo la mayor parte de su visibilidad durante el resto del ciclo democrático.

Los hallazgos de la encuesta de la OEA sugieren que existe una creciente conciencia del panorama de amenazas en las Américas y el Caribe con respecto a la necesidad de mejorar las prácticas de ciberseguridad y las implicaciones asociadas de las amenazas cibernéticas para una elección. La concienciación está aumentando entre los encargados de formular políticas, aunque los recursos finitos significan que el progreso se limita solo a los ciclos políticos. Es importante que la mentalidad en torno a la planificación política cambie a un enfoque holístico más amplio. En este contexto, la necesidad de tener un examen más detallado de este tema no solo se recomienda, sino que se necesita para la región.

Gran parte de la amenaza y el riesgo pueden mitigarse mediante enfoques legislativos, técnicos y operativos tradicionales, así como mediante el apoyo al aumento de las capacidades de cada grupo de partes interesadas. Con el fin de fortalecer la integridad del proceso democrático, también es importante fomentar una mayor conciencia y una comprensión real de los beneficios y los riesgos que la tecnología le trae a la sociedad en general. Esta conciencia, junto con las habilidades para poder descifrar eventos en torno a campañas políticas, es fundamental para apoyar la democracia en nuestra región. En conclusión, los procesos democráticos se fortalecen mediante el diálogo continuo entre los diversos interesados, durante e incluso fuera del período electoral.

Los medios de comunicación como sector tienen la oportunidad de alentar y fomentar el debate independiente y basado en hechos para que cualquier democracia funcione de manera saludable. Si los medios independientes aumentan su comprensión de los riesgos cibernéticos que enfrentan nuestras democracias, asegurando que su propio perfil de ciberseguridad sea lo más resiliente posible, pueden ser una fuerza impulsora del debate basado en hechos que el mundo necesita tan desesperadamente.

Por último, es importante reconocer que el progreso depende de que haya capacidad humana y recursos financieros para impulsar la ambición de mejores prácticas de ciberseguridad en el proceso democrático. Es importante que exista voluntad política para que se asignen los marcos legislativos y presupuestos adecuados o apropiados para contrarrestar la creciente amenaza al núcleo de nuestras democracias.

Anexo I

Partes interesadas

Entre las partes interesadas identificadas incluimos: (a) Actores políticos, (b) Público en general, (c) Actores gubernamentales y / u OGE, (d) Medios de comunicación, y (e) Organizaciones de respuesta a incidentes (ORI). A continuación, se ofrece una descripción detallada de cada grupo de partes interesadas identificadas a los fines de este documento y su papel en el proceso democrático.

Actores Políticos

Los Actores Políticos se consideran los funcionarios electos, o cualquier persona elegida en una elección general o especial para cualquier cargo público, por voto del electorado apropiado, los partidos políticos y los funcionarios de los partidos políticos. Su papel es indispensable ya que son los únicos responsables de proponer, promulgar y aprobar cambios legislativos. Su poder generalmente se ve controlado por:

- La Constitución.

- Un poder judicial independiente con el poder de declarar inconstitucionales los actos legislativos (por ejemplo, tribunal constitucional, Tribunal Supremo).

- Iniciativas deliberativas o medidas populares directas (por ejemplo, iniciativa, referendo, elecciones revocatorias). Sin embargo, estos no siempre son vinculantes, y el poder legal generalmente permanece con los representantes.

Público en general

El público en general cubre a los 'votantes', quienes 'son personas que tienen el derecho legal de votar en las elecciones, o personas que votan en una elección en particular', según el diccionario Collins [28]. Son los titulares de la soberanía de un territorio y, como tal, el objetivo final debe ser mantenerlos libres de manipulaciones y ataques, para que puedan ejercer su derecho libremente.

Actores gubernamentales y / u organismos de gestión electoral (OGE)

Un OGE es "una organización u organismo que tiene el único propósito, y es legalmente responsable, de administrar algunos o todos los elementos que son esenciales [para] realizar elecciones e instrumentos de democracia directa, tales como referendos, iniciativas ciudadanas y revocación de votos, si esos son parte del marco legal". [29] Incluso:

- Determinar quién es elegible para votar;

- Recibir y validar las nominaciones de los participantes electorales (para elecciones, partidos políticos y / o candidatos);

- Contar y tabular el voto, entre otros.

Los principios rectores [de este tipo de entidades] deben ser independencia, imparcialidad, integridad y transparencia.

Un OGE puede gestionar aspectos adicionales como cobertura de medios, actividades educativas o resolución de conflictos. No obstante, si la actividad relacionada con la OGE no incluye ninguno de los aspectos esenciales antes mencionados, no se podrá considerar como una OGE y deberá considerarse como una comisión de vigilancia de cobertura de medios, una comisión de educación cívica o un tribunal electoral, respectivamente.

Dependiendo del territorio, el OGE puede ser (y probablemente debería ser) parte de la Comisión responsable de la Ciberseguridad en los Procesos Democráticos (IFES 2018).

Medios de comunicación

La digitalización de nuestra sociedad, especialmente a través del surgimiento de las redes sociales, ha tenido un gran impacto en el papel que juegan los medios en los procesos democráticos. Los grupos de medios ejercen una gran influencia sobre la opinión pública, y esta influencia puede deberse a la representación de un grupo particular de personas, los recursos y el prestigio, el alcance o el acceso a medios financieros.

Hemos incluido en esta categoría plataformas de redes sociales como Facebook, Twitter, Instagram, WhatsApp, Telegram, etc. dado que su cooperación también es indispensable en términos de colaboración activa y rápida con gobiernos, OGE y CSIRT en caso de un ataque. En ese sentido, iniciativas como la audiencia de Mark Zuckerberg de Facebook en 2018 relacionada con Cambridge Analytica y la multa de 5 mil millones de dólares que se aplicará sin duda marcan la pauta para un futuro en el que los Gigantes de la tecnología deben implementar mejores medidas de privacidad para proteger al usuario y sus datos relacionados.

Organizaciones de respuesta a incidentes (ORI)

A los fines de este documento, una Organización de Respuesta a Incidentes, que incluye un CSIRT (Equipo de Respuesta a Incidentes de Ciberseguridad) o CERT (Equipo de Respuesta a Emergencias Informáticas), es un grupo de expertos a cargo de tratar los incidentes de seguridad informática. Puede ser de naturaleza pública, privada o híbrida (público-privada). Muchos de los CSIRT más relevantes, incluidos los públicos, forman parte de la organización FIRST (Foro de Equipos de Respuesta a Incidentes de Seguridad Informática)[30].

Con respecto a la ciberseguridad de los procesos democráticos, el papel de un CSIRT es fundamental para dar una respuesta de manera oportuna y técnicamente sólida a cualquier evento que pueda surgir. El equipo CSIRT puede integrarse en un Comité de Seguridad Electoral (ESC, por sus siglas en inglés) o Fuerza de Tarea, que tiene la responsabilidad final de salvaguardar la integridad y la seguridad del proceso democrático.

El establecimiento de dinámicas y tareas correctamente diseñadas e implementadas entre el OGE, el CSIRT y los proveedores de tecnología tendrá un enorme impacto en la ciberseguridad general de los procesos electorales.

Anexo II

Resumen de actividades

Taller I

Fecha: 29 y 30 de noviembre de 2018
Ubicación: Mordan Hall, St Hugh's College, Oxford, Reino Unido
Número de asistentes: 19
Países involucrados: Antigua y Barbuda, Barbados, Belice, Brasil, Colombia, Costa Rica, Guatemala, Guyana, Jamaica, México, Nicaragua, Paraguay, San Vicente y las Granadinas, Surinam y Trinidad y Tobago.

Hallazgos principales:

- Identificación de los puntos comunes de los Estados Miembros con respecto al proceso democrático: pasos del proceso (por ejemplo, base de datos de registro de votantes, dispositivos de votación, sistemas de conteo, informe de resultados), actores democráticos (por ejemplo, electores, políticos, parlamentarios, autoridades electorales), infraestructura crítica, amenazas, entre otros. Al definir los puntos comunes, sería más claro el alcance de la directriz.

- Roles y responsabilidades: los participantes destacaron la importancia de incluir los roles y responsabilidades de los diferentes actores nacionales con respecto a la ciberseguridad de los procesos democráticos. Además, destacaron la importancia de discutir los mecanismos de cooperación y colaboración.

- Enfoque basado en el riesgo que considera no solo los aspectos técnicos, sino también los sociales.

- Importancia de la confianza en el sistema: los participantes mencionaron que "generar confianza" es clave para el proceso democrático, y que esto debería reflejarse de alguna manera en el título del documento. También se llamó la atención sobre la palabra "resiliencia".

- Buenas prácticas + Principios generales: la guía podría incluir experiencias de la región y otros países como una buena práctica sobre ciberseguridad y procesos democráticos. Algunos participantes también sugirieron que deberían considerarse los principios básicos para promover la ciberseguridad en el proceso democrático.

- Guía regional adaptable a las necesidades nacionales y locales: aunque la guía se redactará para una audiencia regional, los participantes sugirieron que la guía podría usarse como modelo para crear su guía de ciberseguridad nacional y local para procesos democráticos.

Taller II

Fecha: 27-28 de febrero de 2019
Ubicación: Oxford Martin School, Universidad de Oxford
Número de asistentes: 30 (10 M y 20 H)
Países involucrados: Antigua y Barbuda, Barbados, Bolivia, Chile, El Salvador, Guatemala, Jamaica, Santa Lucía, San Vicente y las Granadinas, Bahamas y Trinidad y Tobago.

Hallazgos principales:

- Las evaluaciones de riesgos deben ir más allá de las elecciones y también examinar cómo se financian y comunican.

- Fomento de la confianza: colaboración y mejores prácticas.

- Énfasis en las operaciones internas de los parlamentarios y cómo manejan su propia información.

- Los procesos electorales deben considerarse una infraestructura crítica.

- En relación con la IA, se está convirtiendo en un facilitador invisible. IA elimina la responsabilidad de la capacidad humana y es importante que nosotros, como capacidades humanas, no perdamos nuestras habilidades y capacidades.

- Se debe pensar en el proceso democrático de manera integral, incluida la cadena de suministro para los procesos electorales, incluidos los sistemas de terceros.

- Uno de los riesgos, si no se aplica la ciberseguridad, no es solo la posibilidad de que el sistema sea pirateado, sino que la confianza en el sistema se erosione.

- La guía debe tener una herramienta de evaluación, protocolos de seguridad; esto debería abarcar a todos los actores del proceso electoral, incluidas las agencias de apoyo, como los primeros en responder, las autoridades regionales, incluidos los medios. Debe haber códigos y reglas para las agencias de observación.

- Es una persona, un voto. Por lo tanto, piratear no es el único problema, sino la capacidad de tener múltiples votos. La guía debe ser simple y clara, especialmente si las propias legislaturas pueden ser más antiguas y no estar adaptadas a la tecnología. Debe haber recomendaciones para las leyes de protección de datos y las leyes de delitos informáticos.

- Las leyes no son actuales y necesitan actualización. No hay leyes de campañas financieras.

- Es posible que sea necesario actualizar las normas de medios, pero no podrá cambiarlas siempre.

Taller III

Fecha: 18-19 de marzo de 2019
Ubicación: Edificio principal de la OEA, Washington D. C., EE. UU
Número de asistentes: 13 (3 M y 10 H)
Países involucrados: Antigua y Barbuda, Brasil, Canadá, Colombia, Granada, México, Paraguay y Estados Unidos.

Hallazgos principales:

- Los participantes identificaron noticias falsas, información errónea, ingeniería social y denegación de servicio y ataques de malware, entre otros, como algunos de los riesgos más apremiantes para los procesos electorales.

- En términos de soluciones, los participantes enfatizaron la importancia de implementar políticas de comunicación, asignar un presupuesto específico para abordar las preocupaciones de ciberseguridad y desarrollar un enfoque basado en el riesgo para combatir noticias falsas, desinformación y ataques cibernéticos, así como un aumento de coordinación entre todas las partes relevantes.

- La intervención debe estar bien coordinada y tal vez una implementación de un centro común con personal clave.

- Los participantes acordaron la necesidad de tener una matriz de riesgos para identificar lo que es necesario para formalizar procedimientos basados en procedimientos documentados. Sería útil para una evaluación de impacto, medidas de control adoptadas y la implementación de planes de mejora.

- Debe incluir términos y definir lo que está abarcando (por ejemplo, la cibernética no incluye noticias falsas).

- Debe incluir información errónea, noticias falsas y temas de redes sociales.

- Recomendaciones sobre encuestas: los países deberían considerar extender el tiempo de la difusión de encuestas.

- Uso de la sociedad civil para el proceso de auditoría tecnológica del sistema (responsabilidad compartida, más confianza en el proceso).

- Establecer cuáles serán las instituciones de auditoría (ciudadanía, experiencia, capacidad técnica, etc.).

- Debe incluir la importancia de la verificación de identidad.

- Importancia de carácter multirregional: enfrentar las diferencias entre la región y adaptarse a la realidad de cada país.

- Importancia del uso de la tecnología en un marco legal.

- ISO 2705: el análisis de riesgos es general y debe sentar las bases. La guía debe incluir un catálogo / lista de verificación para tener una lista de amenazas.

- Definir un rol claro del OGE en Ciberseguridad.

- Crear una lista de verificación o un procedimiento de respuesta a incidentes que indique cómo escalar las amenazas, especialmente cuando se trata de las fuerzas de seguridad nacional o la policía. ¿Qué sucede cuando se detecta una amenaza? (incluir lista de verificación).

Seminario web

Fecha: 11 de julio de 2019
Ubicación: https://vimeo.com/347556001
Número de asistentes: 67
Países involucrados: Antigua y Barbuda, Argentina, Barbados, Canadá, Chile, Colombia, Costa Rica, Dominica, República Dominicana, Ecuador, España, Reino Unido, Guatemala, Honduras, Jamaica, San Cristóbal y Nieves, República de Moldavia, México, Panamá, Perú, Surinam, Trinidad y Tobago, Estados Unidos y Uruguay.

Principales hallazgos: la principal lección aprendida fue la identificación de partes interesadas críticas. La discusión también tuvo un representante de la Secretaría de la Commonwealth que participó en el seminario web.

Cara a cara

Fecha: 25-26 de julio de 2019
Ubicación: Washington D. C., EE. UU
Número de asistentes: 5
Países involucrados: N/A

Principales hallazgos: durante esta sesión con los consultores que están desarrollando la Guía, discutimos capítulo por capítulo las conclusiones y los principales puntos de discusión que se incluirán en la guía. Se proporcionaron comentarios concretos sobre los capítulos propuestos, incluidas recomendaciones para garantizar que la guía esté alineada con los pilares de la OEA sobre democracia y derechos humanos. Los aportes recibidos además de los resultados de la encuesta se incorporaron al borrador actualizado.

Taller IV

Fecha: 30 de septiembre - 1 de octubre de 2019
Ubicación: Hyatt Regency Hotel, Puerto España, Trinidad y Tobago
Número de asistentes: 40 (19 M y 21 H)
Países involucrados: Antigua y Barbuda, Barbados, Belice, Chile, Colombia, Dominica, Ecuador, Granada, Guyana, México, Nicaragua, Santa Lucía, San Vicente y las Granadinas, Surinam y Trinidad y Tobago.

Principales hallazgos:

- Es necesario tener un equipo de ciberseguridad listo durante las elecciones.

- La independencia de los medios es crítica.

- Se necesita responsabilidad social y conciencia de los problemas.

- La creación de capacidad debe ser sostenible y a largo plazo para los actores del proceso democrático.

- Debe haber un mecanismo para implementar las mejores prácticas una vez que se publique la guía.

- La alfabetización tecnológica de los ciudadanos, representantes electos, etc. es crítica.
- Se necesita personal calificado en seguridad digital en el proceso democrático.

- Algunos participantes argumentaron que debería haber un proceso para fortalecer la ciberseguridad en lugar de responder a incidentes después del hecho.

- Debe haber un equilibrio entre la tecnología, la legislación y las libertades civiles, como la libertad de expresión.

- También es necesario equilibrar el derecho a la información y el papel de los medios y las libertades.

- Los representantes elegidos deben considerar:

  • Gestionar su presencia en las redes sociales
  • Interferencia de actores estatales.
  • Legislación para abordar la interfaz en línea con representantes
  • Habilitación de la capacidad mediante disposiciones legislativas

- Votantes:

  • Cualquier amenaza a la confianza de la OGE es una amenaza política
  • Debe haber protección en la legislación para los votantes cuando hay una violación

Anexo III

Bibliografía

"2018 CIRA Canadian Internet Security Survey – Spring edition," Canadian Internet Registry Authority, https://www.cira.ca/resources/cybersecurity/report/2018-canadian-cybersecurity-survey-spring-edition.

"2018 CMO Cybersecurity Survey: Key Findings," Cyberthreat Alliance, June 2018, https://www.cyberthreatalliance.org/wp-content/uploads/2018/06/2018-Cybersecurity-Survey-Key-Findings_Final_06222018.pdf.

"2018 Deloitte-NASCIO Cybersecurity Study - States at risk: Bold plays for change," a joint report from Deloitte and the National Association of State Chief Information Officers (NASCIO), 2018, https://www2.deloitte.com/content/dam/Deloitte/co/Documents/risk/DI_2018-Deloitte-NASCIO-Cybersecurity-Study.pdf.

"2018 HIMSS Cybersecurity Survey", Healthcare Information and Management Systems Society, 2018, https://www.himss.org/2018-himss-cybersecurity-survey

"2018 UN E-Government Survey 2018," United Nations, 19 July 2018, https://www.un.org/development/desa/publications/2018-un-e-government-survey.html.

"2019 Internet Security Threat Report," Symantec, February 2019, https://www.symantec.com/security-center/threat-report.

"Cisco 2018 Annual Cybersecurity Report," Cisco Corporation, February 2018, https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf

"Compendium on Cybersecurity of Election Technology," European Commission, 2018. http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53645

"Cybersecurity: Protecting Local Government Digital Resources", International City/County Management Association and Microsoft, 25 October 2017. https://icma.org/cyber-report

"The Cybersecurity Campaign Playbook, European Edition," Harvard Kennedy School, Belfer Center for Science and International Affairs, May 2018. https://www.belfercenter.org/publication/cybersecurity-campaign-playbook-european-edition.

"Cybersecurity regained: preparing to face cyber-attacks - 20th Global Information Security Survey 2017-2018," EY, 2017, https://www.ey.com/Publication/vwLUAssets/ey-cybersecurity-regained-preparing-to-face-cyber-attacks/$FILE/ey-cybersecurity-regained-preparing-to-face-cyber-attacks.pdf.

Defending Digital Democracy Project, Harvard Kennedy School, Belfer Center for Science and International Affairs, accessed 16 February 2020, https://www.belfercenter.org/project/defending-digital-democracy.

"Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe", Organization of American States, 2018, http://www.oas.org/es/sms/cicte/sectorbancariospa.pdf

"Guidelines for reviewing a Legal Framework for Elections," second edition, OSCE Office for Democratic Institutions and Human Rights, 2013, https://www.osce.org/odihr/elections/104573?download=true.

"INTER-AMERICAN DEMOCRATIC CHARTER (Adopted by the General Assembly at its special session held in Lima, Peru, on September 11, 2001)," Organization of American States, 11 September 2001, https://www.oas.org/OASpage/eng/Documents/Democractic_Charter.htm.

"International Electoral Standards: Guidelines for reviewing the legal framework of elections," Institute for Democracy and Electoral Assistance (IDEA), 1 June 2002, https://www.idea.int/es/publications/catalogue/international-electoral-standards-guidelines-reviewing-legal-framework?lang=en.

IFES: International Foundation for Electoral Systems, https://www.ifes.org/publications/cybersecurity-elections

"Media Literacy and Digital Security: Twitter Best Practices," Organization of American States, 13 September 2019, https://www.oas.org/en/sms/cicte/docs/20190913-DIGITAL-ENG-Alfabetismo-y-seguridad-digital-Twitter.pdf.

"Methodology for Media Observation During elections: A Manual for OAS Electoral Observation Missions," General Secreteriat of the Organization of American States, 2011, http://www.oas.org/es/sap/docs/deco/ManualMedia_WEB.pdf.

"Observing the Use of Electoral Technologies: A Manual for OAS Electoral Observation Missions," General Secretariat of the Organization of American States, 2010, http://www.oas.org/es/sap/docs/Technology%20English-FINAL-4-27-10.pdf.

"Promise and Problems of E-Democracy: Challenges of Online Citizen Engagement," OECD, 2003, http://www.oecd.org/gov/digital-government/35176328.pdf.

"Protección de la Infraestructura Crítica en América Latina y el Caribe", Organization of American States and Microsoft, 2018. https://www.oas.org/es/sms/cicte/cipreport.pdf

"Tendencias sobre ataques de ciberseguridad," LACNIC, 30 October 2018, https://www.lacnic.net/3366/1/lacnic/.

"Universal Declaration of Human Rights," United Nations, 10 December 1948, https://www.un.org/en/universal-declaration-human-rights/.

ACE Project Electoral Knowledge Network: "Electoral Management," EMBs definition, last accessed 16 February 2020, https://aceproject.org/ace-en/topics/em/ema/ema01

Emefa Addo Agawu, "How to Think About Election Cybersecurity: A Guide for Policymakers," New America, 3 April 2018. https://www.newamerica.org/cybersecurity-initiative/policy-papers/how-to-think-about-election-cybersecurity/

Panizo Alonso L., Gasco M., Marcos del Blanco D.Y., Hermida Alonso J.A., Barrat J., Alaiz Moreton H., "E-voting system evaluation based on the Council of Europe recommendations: Helios Voting," IEEE Transactions on Emerging Topics in Computing. 19 November 2018, DOI: 10.1109/TETC.2018.2881891

Australian Cybersecurity Centre, "ACSC Threat Report 2017," Australian Signals Directorate of the Australian Government, October 2017, https://www.acsc.gov.au/publications/ACSC_Threat_Report_2017.pdf

Jean Baudrillard, "Simulacra and Simulations (The Body, In Theory: Histories of Cultural Materialism," University of Michigan Press, 1983.

DYM del Blanco, LP Alonso, JAH Alonso, "Review of Cryptographic Schemes applied to Remote Electronic Voting systems: Remaining challenges and the upcoming post-quantum paradigm," Open Mathematics, 23 February 2018, DOI: 10.1515/math-2018-0013

D.Y. Marcos del Blanco: "Ciberseguridad Aplicada a la E-Democracia: Análisis Criptográfico y Desarrollo de una Metodología Practica de Evaluación para Systemas de Voto Electrónico Remoto y Suaplición a las Soluciones Más Relevantes," thesis, 2018 (in Spanish).
https://buleria.unileon.es/bitstream/handle/10612/7959/Tesis%20David%20Marcos%20del%20Blanco.pdf?sequence=1

Jakob Bund, "Cybersecurity and democracy Jakob Bund, Hacking, leaking and voting", European Institute for Security Studies, November 2016. https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief_30_Cyber.pdf

Canadian Centre for Cyber Security, "Global Trends and the Threat to Canada," Government of Canada, 26 March 2019, https://cyber.gc.ca/en/guidance/global-trends-and-threat-canada-0.

Communications Security Establishment, "2019 update: cyber threats to Canada's democratic process," Government of Canada, 2019, http://publications.gc.ca/site/eng/9.872398/publication.html.

Council of Europe Venice Commission, "European Standards of Electoral Law in Contemporary Constitutionalism,"Council of Europe Publishing, ISBN: 92-871-5909-2 , 2005. Available from: https://books.google.es/ks?id=7xo7NUSrthIC&pg=PA17&lpg=PA17&dq=European+Standards+of+Electoral+Law+in+Contemporary+Constitutionalism&source=bl&ots=2uuCmyGSNn&sig=jKw-Za0JHjs26MQN83xpY6QfxU&hl=es&sa=X&ved=0ahUKEwiJ6vfZx7bSAhXHaRQKHZ3GCa4Q6AEISzAG#v=onepage&q=European%20Standards%20of%20Electoral%20Law%20in%20Contemporary%20Constitutionalism&f=false.

Katherine Ellena, Goran Petrov, "Cybersecurity in Elections: Developing a Holistic Exposure and Adaptation Testing (HEAT) Process for Election Management Bodies," International Foundation for Electoral Systems, 17 October 2018, https://www.ifes.org/sites/default/files/2018_heat_cybersecurity_in_elections.pdf.

David Fidler, "Transforming Election Cybersecurity," Council on Foreign Relations, 17 May 2017.
https://www.cfr.org/report/transforming-election-cybersecurity.

Luciano Floridi, "Marketing as Control of Human Interfaces and Its Political Exploitation,"
published online 10th August 2019, https://www.academia.edu/attachments/60279708/download_file?st=MTU4MTg4NzE1Myw3MS4yMzEuMjE2LjEw&s=profile.

Frost & Sullivan. "2017 Global Information Security Workforce Study Benchmarking Workforce Capacity and Response to Cyber Risk". https://iamcybersafe.org/wp-content/uploads/2017/06/europe-gisws-report.pdf **Password protected**

Nellie M. Gorbea, "Elections Cybersecurity in Rhode Island", Rhode Island Department of State, April 2018,
https://vote.sos.ri.gov/Content/Pdfs/cyber_security_ri_2018.pdf.

V. Hahanov, E. Litvinova, M. Brazhnikova and A. Hahanova, "Cyber democracy and digital relationship," 2016 13th International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET), Lviv, 2016, pp. 545-548, https://ieeexplore.ieee.org/document/7452110.

Dr. Sven Herpig, Julia Schuetze, Jonathan Jones: "Securing Democracy in Cyberspace: An Approach to Protecting Data-Driven Elections" October 2018. https://www.stiftung-nv.de/en/publication/securing-democracy-cyberspace-approach-protecting-data-driven-elections.

Human Rights Council of the United Nations General Assembly, "Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development – Oral Revisions of 30 June," A/HRC/32/L.20, United Nations, 30 June 2016, https://www.article19.org/data/files/Internet_Statement_Adopted.pdf.

Brooks Jackson, "The Florida Recount of 2000," FactCheck.Org, 22 January 2008 https://www.factcheck.org/2008/01/the-florida-recount-of-2000.

"33 ataques por Segundo: Kaspersky Lab registra un aumento del 59% en ataques de malware en América Latina," Kapersky Lab, 11 September 2017, https://latam.kaspersky.com/about/press-releases/2017_33-attacks-per-second-increase-in-malware-attacks-in-latin-america.

S.J. Lewis, O. Pereira and V. Teague. "Trapdoor commitments in the SwissPost e-voting shuffle proof". The University of Melbourne, 2019. https://people.eng.unimelb.edu.au/vjteague/SwissVote.

Wade Payson-Denney, "So, Who really won? What the Bush v. Gore studies showed," CNN, 31 October 2015, https://edition.cnn.com/2015/10/31/politics/bush-gore-2000-election-results-studies/index.html.

Thamy Pogrebinschi, "Does digital democracy improve democracy?" openDemocracy, 2 March 2017, https://www.opendemocracy.net/en/democraciaabierta/does-digital-democracy-improve-democracy/.

K. Reinasalu, "Handbook on E-democracy," pace theme publication, January 2010.

V. Teague. "Faking an iVote decryption proof". University of Melbourne, 2019. https://people.eng.unimelb.edu.au/vjteague/iVoteDecryptionProofCheat.pdf.

Maarja Toots, Tarmo Kalvet, and Robert Krimmer, "Success in eVoting – Success in eDemocracy? The Estonian Paradox," Electronic Participation: 8th IFIP WG 8.5 International Conference, pp. 55-66, https://doi.org/10.1007/978-3-319-45074-2_5.

J.-B. Jeangène Vilmer, A. Escorcia, M. Guillaume, J. Herrera, "Information Manipulation: A Challenge for Our Democracies," report by the Policy Planning Staff (CAPS) of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research (IRSEM) of the Ministry for the Armed Forces, Paris, August 2018.

Pie de Notas

1. En 2016, Bloomberg publicó una historia sobre un pirata informático colombiano, Andrés Sepúlveda, quien afirma que hackeó y espió en las elecciones en Colombia, Costa Rica, El Salvador, Guatemala, Honduras, México, Nicaragua, Panamá y Venezuela durante casi ocho años. 'Cómo hackear una elección'- https://www.bloomberg.com/features/2016-how-to-hack-an-election/

2. Antigua y Barbuda, Bahamas, Belice, Bolivia, Brasil, Colombia, Costa Rica, Dominica, República Dominicana, Ecuador, El Salvador, Granada, Guatemala, Guyana, Haití, Honduras, Jamaica, México, Nicaragua, Panamá, Paraguay, Perú, San Cristóbal y Nieves, San Vicente y las Granadinas, Santa Lucía, Surinam y Estados Unidos de América.

3. Consulte el sitio web del Departamento para la Cooperación y Observación Electoral de la OEA, disponible en https://www.oas.org/en/spa/deco/.

4. Por ejemplo, vea la colección de ensayos del sociólogo francés Jean Baudrillard, "La Guerra del Golfo no tuvo lugar".

5. CIDH, El marco jurídico interamericano sobre el derecho a la libertad de expresión. Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos. 2009, par. 8.

6. Ibid., par. 80

7. Ibid., par. 57

8. CIDH, Guía para garantizar la libertad de expresión frente a la desinformación deliberada en contextos electorales, cit., Pág. 17 – "En general, los poderes ejecutivos de la región controlan dimensiones del estado esenciales para el desarrollo de este tipo de campañas. Por ejemplo, desde la gestión del sistema educativo o los dispositivos de promoción cultural. En esos casos, resulta fundamental que las autoridades encargadas de esos departamentos aborden el problema de la desinformación mediante campañas de concientización, educación y capacitación. Las mismas deberían estar enfocadas en ofrecer a los ciudadanos herramientas para poder distinguir la información verdadera de la falsa, tomar conciencia de su propia participación en los procesos de réplica de la información, y alertar sobre el empobrecimiento del debate público que la desinformación genera. Si bien esta recomendación se dirige al poder ejecutivo, sería deseable que todos los actores involucrados en el fenómeno desarrollen campañas de educación y concientización".

9. Para los propósitos de este documento, se entiende por desinformación "la difusión masiva de información falsa (a) con la intención de engañar al público y (b) a sabiendas de su falsedad" - CIDH, Guía para garantizar la libertad de expresión frente a desinformación deliberada en contextos electorales, pág. 3

10. El gobierno francés ha descrito la manipulación de la información y quizás ha tomado la posición más dura en contra de lo anterior al introducir marcos regulatorios relacionados con la misma. Véase http://www.gouvernement.fr/en/against-information-manipulation. El gobierno canadiense también ha abordado el tema de las "noticias falsas" destacando la amenaza para su propia gente. Véase https://www.loc.gov/law/help/fake-news/canada.php.

11. En Trinidad y Tobago, las campañas electorales dirigidas llevaron a una parte específica del electorado a no molestarse en emitir su voto en papel el día de las elecciones, lo que afectó el resultado de las elecciones de una manera predeterminada. Véase https://www.opendemocracy.net/en/dark-money-investigations/they-were-planning-on-stealing-election-explosive-new-tapes-reveal-cambridg/

12. Ver, por ejemplo, CIDH, Libertad de expresión e Internet, cit, pars. 137-142; CIDH, Estándares para una Internet libre, abierta e incluyente, cit, cap. 4law updla.

13. Por ejemplo, intermediarios de Internet, proveedores de redes sociales, corredores de datos, motores de búsqueda, etc.

14. Los países representados en la encuesta incluyen: Antigua y Barbuda, las Bahamas, Brasil, Canadá, Chile, Colombia, Costa Rica, Ecuador, Granada, Guatemala, Haití, México, Panamá, Perú, San Vicente y las Granadinas, Trinidad y Tobago y Estados Unidos.

15. Cuanto más grande es el país, más probable es que haya introducido servicios en la nube.

16. Cabe señalar que dichas actualizaciones legislativas deben tener en cuenta las normas internacionales de derechos humanos vigentes

17. Según el Establecimiento de Seguridad de la Comunicación de Canadá, esto representa un aumento de tres veces desde 2015. Se espera que la tendencia al alza continúe. Ver https://cyber.gc.ca/en/cyber-threats-and-democracy.

18. Las instituciones que crean esos documentos originales tienden a ser organizaciones multilaterales o universidades y grupos de expertos de alto nivel. Algunos de los ejemplos más relevantes incluyen:
1. Promesa y problemas de la democracia electrónica por la OCDE
2.Manual sobre democracia electrónica. Publicación del tema Epace, por Reinasalu "Ciberseguridad y democracia" por el Instituto de Estudios de Seguridad de la Unión Europea (IESUE).

19. Entre las publicaciones de referencia destacadas que cubren el tema se incluyen: Manipulación de la información: un desafío para nuestras democracias, informe del Personal de Planificación de Políticas (CAPS) del Ministerio para Europa y de Asuntos Exteriores y el Instituto de Investigaciones Estratégicas de la Escuela Militar (IRSEM), Ciberseguridad en las elecciones por IFES, Transformando la Ciberseguridad Electoral por el Consejo de Relaciones Exteriores, El libro de campaña de la Ciberseguridad, edición europea. Defendiendo la Democracia Digital, del Centro Belfer para la Ciencia y Asuntos Internacionales, Harvard Kennedy School, Amenazas Cibernéticas al Proceso Democrático de Canadá por el Establecimiento de Seguridad en las Comunicaciones del gobierno canadiense o la "Guía para controlar la libertad de expresión frente a la desinformación deliberada en contextos electorales" por la Organización de los Estados Americanos.

20. CIDH, Guía para garantizar la libertad de expresión frente a la desinformación deliberada en contextos electorales, cit., Pág. 13.

21. Damien Bancal, un francés experto en crimen cibernético, analizó más de 30 sitios pertenecientes a 11 candidatos para la última campaña presidencial francesa, descubriendo más de 200 fallas, incluidas las inyecciones SQL y los sitios de WordPress que todavía usan el nombre de usuario y la contraseña originales en la cuenta del administrador.

22. Un ejemplo de un sitio web de verificación de hechos en Argentina - https://chequeado.com/

23. Un ejemplo de un sitio web de verificación de hechos en México - https://verificado.mx/

24. Para obtener fuentes adicionales y lecturas adicionales, las Directrices para revisar un marco electoral legislativo de la OSCE y las "Normas Electorales Internacionales: Directrices para revisar el marco legal de las elecciones" del Instituto Internacional para la Democracia y Asistencia Electoral (IDEA) ofrecen un análisis en profundidad sobre el Marco Legal para Elecciones Democráticas con requisitos y recomendaciones integrales como recurso clave.

25. Puede encontrar más información sobre el escándalo electoral de los Estados Unidos en 2000 en "Fact Check: The Florida Recount of 2000" https://www.factcheck.org/2008/01/the-florida-recount-of-2000 and y en el artículo de CNN Entonces, ¿quién ganó realmente? Lo que mostraron los estudios Bush vs. Gore. https://edition.cnn.com/2015/10/31/politics/bush-gore-2000-election-results-studies/index.html

26. Hemos visto esto en el Reino Unido, con el establecimiento del Centro Nacional de Ciberseguridad en 2016, que sigue siendo parte de la sede principal (GCHQ), con el mandato de ser la agencia responsable de los asuntos de ciberseguridad, respaldado con una capacidad muy sofisticada en GCHQ cuando sea necesario, pero también lo suficientemente independiente como para interactuar con el público en general.

27. Ver CIDH, Guía para garantizar la libertad de expresión frente a la desinformación deliberada en contextos electorales, cit., Página 15. "Una de las condiciones esenciales para combatir el fenómeno de la desinformación implica transparentar y dar mayor publicidad a todo el proceso electoral. La mayoría de los regímenes electorales de la región ya incluyen obligaciones de transparencia, especialmente en cabeza de partidos políticos. Asimismo, muchos también incluyen obligaciones especiales como, por ejemplo, señalar que ciertos mensajes o avisos son emitidos en el marco de campañas electorales, contratados por cierto partido político o alianza electoral o terceros, etcétera".

28. Según lo definido por el Diccionario Collins; ver https://www.collinsdictionary.com/dictionary/english/voter

29. Según lo definido por la Red de conocimientos electorales ACE; ver https://aceproject.org/ace-en/topics/em/ema/ema01

30. Sitio web de FIRST: https://www.first.org/

Consideraciones de Ciberseguridad del proceso democrático para América Latina y el Caribe

Consideraciones de Ciberseguridad del proceso democrático para América Latina y el Caribe

OEA | Más derechos para más gente