

	MANUAL DE SEGURIDAD PARA ACTORES POLÍTICOS EN LOS PROCESOS ELECTORALES	DNEECT-001
		Versión 01
		Página 1 de 16

MANUAL DE SEGURIDAD PARA ACTORES POLÍTICOS EN LOS PROCESOS ELECTORALES

CAPÍTULO I DISPOSICIONES GENERALES

Artículo 1.- Objeto

El presente Manual tiene por objeto establecer lineamientos técnicos y criterios orientadores para la prevención, identificación y gestión de riesgos que puedan afectar la integridad física y digital de los actores políticos, sus equipos de campaña, según corresponda, y su entorno, durante los procesos electorales, garantizando el respeto y protección de los derechos fundamentales, incluyendo los derechos a la participación política, la libertad de expresión y reunión pacífica, así como el de igualdad y no discriminación, conforme a estándares internacionales de derechos humanos.

Artículo 2.- Definición de actores políticos y ámbito de aplicación

Para efectos del presente documento, se consideran actores políticos a aquellas personas, candidatos/as, agrupaciones, observadores, instituciones que intervienen o influyen directa o indirectamente en el proceso electoral, antes, durante y después de la jornada electoral. Incluyen partidos políticos, instituciones públicas, sociedad civil e individuos que interactúan en el proceso electoral y/o en la toma de decisiones, así como aquellas expuestas a formas agravadas o específicas de violencia política.

Las disposiciones del presente Manual son aplicables a los actores políticos, así como a sus equipos, según corresponda. Su aplicación tiene carácter orientador y no sustituye ni limita las competencias de la Policía Nacional del Perú ni de otras autoridades conforme a la Constitución Política y la ley.

Artículo 3.- Principios

La implementación del presente Manual se rige por los siguientes principios:

Prevención. Los actores políticos deberán realizar evaluaciones anticipadas de riesgo antes del desarrollo de cada actividad pública durante el proceso

	MANUAL DE SEGURIDAD PARA ACTORES POLÍTICOS EN LOS PROCESOS ELECTORALES	DNEECT-001
		Versión 01
		Página 2 de 16

electoral, adoptando medidas razonables destinadas a evitar la ocurrencia de incidentes.

Proporcionalidad. Las medidas de seguridad deberán ser acordes al nivel de riesgo identificado, evitando tanto la insuficiencia de protección como restricciones indebidas de derechos fundamentales de los actores políticos involucrados.

Coordinación. La adopción e implementación de medidas deberá realizarse en articulación con la Policía Nacional del Perú y demás autoridades competentes, respetando sus atribuciones legales, para lo cual deberá establecerse un punto de contacto específico con cada entidad competente que debe permanecer actualizado durante todo el proceso electoral.

No discriminación. Las medidas de seguridad deberán aplicarse con criterios objetivos de evaluación de riesgo, garantizando la igualdad de trato a todos los actores políticos, sus equipos de campaña y su entorno.

Transparencia. Las decisiones adoptadas en materia de seguridad deberán quedar debidamente documentadas, incluyendo el registro material, fotográfico u otro de los incidentes y las acciones implementadas.

Confidencialidad y protección de datos. La gestión de la información relacionada con riesgos, amenazas o incidentes deberá garantizar la protección de los datos personales y la confidencialidad de las víctimas, acorde con la normativa de la materia.

CAPÍTULO II

EVALUACIÓN DEL RIESGO DE AFECTACIÓN A LA INTEGRIDAD DE ACTORES POLÍTICOS EN EL CONTEXTO ELECTORAL

Artículo 4.- Definición y niveles de riesgo electoral

La evaluación del riesgo electoral de afectación a la integridad de actores políticos es el proceso sistemático de identificación y análisis de factores que puedan afectar la seguridad, la integridad o el normal desarrollo de actividades político-electorales en una determinada circunscripción electoral. Se establecen los siguientes niveles de riesgo:

	MANUAL DE SEGURIDAD PARA ACTORES POLÍTICOS EN LOS PROCESOS ELECTORALES	DNEECT-001
		Versión 01
		Página 3 de 16

- **Nivel I – Riesgo leve.** Corresponde a contextos donde se identifican indicios iniciales de tensión o malestar social sin afectación directa del orden público. Incluye expresiones de descontento, tensiones menores entre simpatizantes o factores que podrían escalar si no son monitoreadas o atendidas oportunamente. Requiere vigilancia activa y medidas preventivas básicas.
- **Nivel II – Riesgo medio.** Se configura cuando existen hostigamientos, agresiones verbales, amenazas indirectas o alteraciones del orden público que ameritan coordinación con las autoridades competentes, especialmente con la Policía Nacional del Perú, responsable de contribuir al mantenimiento del orden y la seguridad durante las actividades electorales conforme a la normativa vigente.
- **Nivel III – Riesgo alto.** Comprende escenarios que representan una amenaza directa contra la integridad de los actores políticos, tales como amenazas directas, agresiones físicas, ataques a locales partidarios, sabotaje de materiales de campaña o impedimento deliberado de actividades políticas. También se considerará nivel alto la existencia de amenazas sistemáticas en entornos digitales que puedan traducirse razonablemente en agresiones físicas o afectación directa al proceso electoral. Estos supuestos requieren intervención inmediata de la Policía Nacional del Perú y comunicación al Ministerio Público cuando corresponda.
- También se considerará riesgo alto la existencia de amenazas reiteradas o ataques sistemáticos contra candidaturas o actores políticos pertenecientes a grupos históricamente discriminados.

Artículo 5.- Criterios para la evaluación del riesgo

La evaluación del riesgo deberá realizarse de manera objetiva, razonada y documentada. Para determinar el nivel aplicable podrán considerarse, entre otros, los siguientes criterios:

- Perfil, aforo y ubicación territorial del evento o actividad a desarrollarse.

	MANUAL DE SEGURIDAD PARA ACTORES POLÍTICOS EN LOS PROCESOS ELECTORALES	DNEECT-001
		Versión 01
		Página 4 de 16

- Análisis del contexto y antecedentes de violencia en la circunscripción electoral, incluyendo agresiones, disturbios o incidentes registrados en procesos electorales previos.
- Antecedentes de débil articulación interinstitucional en el territorio, que puedan afectar la capacidad de reacción coordinada frente a amenazas o incidentes.
- Existencia o antecedentes de conflictos sociales activos, tales como conflictos socioambientales, laborales o comunales que puedan incidir en las actividades políticas.
- Potencial generación de escenarios de tensión social asociados a la gestión del incidente, en la medida en que la presencia o visita de los actores políticos pueda dar lugar a acciones de hecho, protestas o reclamos dirigidos a autoridades responsables de la atención de la emergencia.
- Presencia de economías ilícitas o actores criminales que puedan interferir en el libre ejercicio de las actividades políticas.
- Cercanía a áreas de frontera, o que abarque más de un departamento del país, como VRAEM y/o territorios declarados en estado de emergencia.
- Análisis de discursos de odio o estigmatización persistente contra la candidatura, es decir, el nivel de polarización política.
- Riesgos diferenciados para candidatas y personas pertenecientes a grupos vulnerables y/o discriminados.
- Presencia de patrones de violencia política de género o violencia basada en prejuicios.
- Riesgo de criminalización indebida o uso abusivo del sistema judicial para hostigar candidaturas.
- Información proveniente de mecanismos de alerta temprana u observación electoral nacional o internacional.
- Información proporcionada por la Policía Nacional del Perú, el Ministerio Público, el Jurado Electoral Especial, la ODPE u otras autoridades competentes respecto de amenazas, alteraciones del orden o riesgos identificados.
- Información proporcionada por las Fuerzas Armadas, especialmente en regiones fronterizas, zonas declaradas en estado de emergencia u otras áreas donde su presencia operativa sea relevante, a efectos de contar con análisis situacionales, alertas de seguridad o información estratégica que contribuya a una evaluación integral del riesgo.

	MANUAL DE SEGURIDAD PARA ACTORES POLÍTICOS EN LOS PROCESOS ELECTORALES	DNEECT-001
		Versión 01
		Página 5 de 16

La evaluación del riesgo no tendrá carácter estático. Los actores políticos deberán actualizarla cuando se modifiquen las condiciones del entorno, se registren nuevos incidentes o se reciban alertas de autoridades competentes. Toda actualización deberá quedar documentada, señalando fecha, circunstancias que la motivan y medidas adoptadas como consecuencia de la nueva evaluación.

Se recomienda que la evaluación del riesgo se encuentre contenido un informe interno debidamente motivado y documentado, suscrito por la persona responsable de seguridad designada por la organización política, según corresponda, o por el actor político, quien dejará constancia expresa de los criterios considerados, el análisis efectuado y el nivel de riesgo determinado.

CAPÍTULO III

MEDIDAS DE SEGURIDAD FÍSICA

Artículo 6.- Planeamiento integral de actividades políticas

Los actores políticos deberán realizar un planeamiento previo y específico de seguridad para cada actividad pública en la que participen, con el fin de prevenir riesgos y proteger su integridad física y psicológica.

El planeamiento deberá sustentarse en la evaluación del nivel de riesgo aplicable y contemplar medidas proporcionales a la naturaleza, magnitud, ubicación y contexto de la actividad.

Cuando el actor político tenga alto nivel de exposición pública, antecedentes de amenazas, campañas de hostigamiento o se desenvuelva en zonas de riesgo identificado, deberán adoptarse medidas reforzadas de autoprotección, control de entorno y monitoreo permanente.

Cada organización política o actor político deberá designar un responsable de seguridad encargado de coordinar la implementación de las medidas de protección de los actores políticos y centralizar la información sobre riesgos, alertas e incidentes.

 JNE JURADO NACIONAL DE ELECCIONES	MANUAL DE SEGURIDAD PARA ACTORES POLÍTICOS EN LOS PROCESOS ELECTORALES	DNEECT-001
		Versión 01
		Página 6 de 16

Artículo 7.- Evaluación previa del lugar

Antes de realizar cualquier actividad política, deberá efectuarse una evaluación técnica del lugar con enfoque prioritario en la seguridad de la persona candidata o del actor político involucrado.

La evaluación deberá identificar riesgos específicos, tales como aglomeraciones previsibles, accesos limitados, puntos ciegos, proximidad de zonas conflictivas, vulnerabilidades logísticas o condiciones que dificulten una evacuación rápida.

Asimismo, sin perjuicio de otros aspectos, deberá verificarse lo siguiente:

- a) Tramitación oportuna ante las autoridades competentes de los permisos y/o autorizaciones que corresponden (por ejemplo, inspección de defensa civil).
- b) Rutas diferenciadas de ingreso y salida para los actores políticos, cuando sea posible.
- c) Verificación del aforo.
- d) Al menos dos rutas alternativas de evacuación previamente verificadas y libres de obstáculos.
- e) Un vehículo de traslado disponible para evacuación inmediata, con conductor identificado.
- f) Un punto de encuentro o refugio seguro previamente definido.
- g) Un plan de salida de la zona en caso de crisis grave o escalamiento del riesgo.
- h) Contar con los permisos de circulación del vehículo de traslado (por ejemplo: SOAT, revisión técnica y, licencia de conducir).
- i) Un kit de primeros auxilios.

Artículo 8.- Coordinación preventiva con la autoridad policial antes de la actividad política

Las organizaciones políticas y/o actores políticos deberán comunicar oportunamente a la Policía Nacional del Perú la realización de actividades que impliquen concentración de personas, e informar sobre la naturaleza de la actividad, aforo estimado, evaluación preliminar de riesgos y requerimientos de resguardo.

	MANUAL DE SEGURIDAD PARA ACTORES POLÍTICOS EN LOS PROCESOS ELECTORALES	DNEECT-001
		Versión 01
		Página 7 de 16

Artículo 9.- Plan de prevención y respuesta ante incidentes durante la actividad política

Tratándose de organizaciones políticas o actores políticos, toda actividad política deberá contar con un plan básico de prevención y respuesta ante incidentes, conocido por el equipo organizador y responsables designados. El plan incluirá responsables de seguridad, ingresos improvisados al escenario, salidas alternativas de evacuación, canales internos de comunicación, cadena de mando y procedimientos ante disturbios, amenazas, emergencias médicas (con o sin ingreso de ambulancias), evacuaciones u otras alteraciones del orden.

Asimismo, contemplará mecanismos de coordinación con servicios de emergencia y autoridades competentes. Cuando corresponda, podrá considerar recomendaciones de los Centros de Operaciones de Emergencia (COEN) u otras instancias especializadas.

El plan deberá contemplar protocolos específicos frente a amenazas de artefactos explosivos, disturbios masivos, intentos de ingreso forzado y situaciones de pánico colectivo.

El plan deberá incluir lineamientos para evitar el uso excesivo de la fuerza, tanto por parte de los equipos de seguridad privada como pública para garantizar el respeto de derechos fundamentales durante la gestión de incidentes.

Artículo 10.- Criterios para la adopción de medidas específicas

Las organizaciones políticas y/o actores políticos deberán considerar las recomendaciones de la Policía Nacional del Perú y los lineamientos de las autoridades electorales cuando la actividad se vincule directamente al proceso electoral.

En aplicación del principio de mínima intervención necesaria, las medidas no deberán afectar el libre ejercicio de los derechos de reunión pacífica, participación política y libertad de expresión.

Podrán adoptarse medidas adicionales -como controles de acceso, delimitación de áreas, soporte médico, seguridad privada o barreras físicas temporales- siempre que respondan a un riesgo específico, estén

	MANUAL DE SEGURIDAD PARA ACTORES POLÍTICOS EN LOS PROCESOS ELECTORALES	DNEECT-001
		Versión 01
		Página 8 de 16

debidamente justificadas y no vulneren derechos fundamentales ni la neutralidad electoral.

Artículo 11.- Registro y documentación de incidentes de seguridad

Culminado el evento o actividad política, las organizaciones políticas o actores políticos deberán llevar un registro interno de incidentes de seguridad ocurridos durante actividades de campaña, incluyendo fecha, lugar, descripción de los hechos, personas afectadas, medidas adoptadas y coordinación realizada con autoridades competentes. Este registro permitirá identificar patrones de riesgo, evaluar el nivel de riesgo que se enfrenta, fortalecer medidas preventivas y facilitar, cuando corresponda, la formulación de denuncias ante la autoridad competente.

Cuando el incidente pudiera constituir un delito, deberá preservarse la evidencia física o digital, respetando los principios básicos de la cadena de custodia, evitando su alteración o difusión innecesarias.

El registro deberá permitir la desagregación de datos por género, pertenencia étnica, edad y otros factores relevantes, a fin de identificar patrones diferenciados de violencia política.

Además, el responsable de seguridad designado por la organización política o el actor político deberá entre otras acciones, realizar la evacuación inmediata de los actores políticos a través de la ruta secundaria, previamente identificada, así como proceder a la revisión exhaustiva del vehículo previo al abordaje, y otras acciones tendientes a la protección y seguridad de los actores políticos.

Artículo 12.- Capacitación básica en autoprotección

Los actores políticos y/o las organizaciones políticas deberán promover sesiones informativas a sus integrantes dirigidas, sus equipos de campaña y su entorno, sobre medidas básicas de autoprotección, identificación de riesgos, manejo de situaciones de tensión y actuación ante emergencias.

La capacitación podrá incluir simulacros, recomendaciones prácticas de comportamiento en espacios públicos y pautas de coordinación inmediata con las autoridades en caso de incidente.

 JNE JURADO NACIONAL DE ELECCIONES	MANUAL DE SEGURIDAD PARA ACTORES POLÍTICOS EN LOS PROCESOS ELECTORALES	DNEECT-001
		Versión 01
		Página 9 de 16

La capacitación deberá incluir pautas de autoprotección durante los desplazamientos, el uso seguro del transporte, manejo prudente de la información sobre agendas públicas u otros temas sensibles, y prácticas para reducir riesgos previsibles sin restringir indebidamente la actividad política.

También deberá incorporar orientaciones prácticas para la identificación temprana de riesgos y la adopción de medidas razonables de autoprotección en actividades públicas y desplazamientos, incluyendo pautas para el manejo adecuado de situaciones de tensión y prevención de incidentes. Asimismo, podrá considerar recomendaciones específicas para candidaturas que, por su nivel de exposición o contexto territorial, enfrenten riesgos diferenciados, promoviendo siempre el ejercicio seguro y pleno de los derechos políticos.

CAPÍTULO IV

MEDIDAS CONTRA LA VIOLENCIA DIGITAL

Artículo 13.- Definición

Se entiende por violencia digital toda acción realizada mediante el uso de tecnologías de la información y comunicación incluyendo redes sociales, mensajería instantánea, servicios digitales, inteligencia artificial y herramientas automatizadas, que tenga como finalidad o efecto intimidar, amenazar, desacreditar, humillar, suplantar, vigilar, o interferir en el ejercicio de derechos políticos de cualquier actor político, integrante de organización política, afiliada, simpatizante o personal de campaña.

Entre estas acciones se incluyen, sin limitarse a:

- acoso individual o coordinado;
- discursos de odio o ataques basados en características personales, identidades o estereotipos (hate Speech);
- amenazas directas o veladas;
- suplantación de identidad;
- difusión indebida de datos personales (doxxing);
- manipulación de contenido audiovisual, incluyendo deepfakes;
- campañas de desinformación o manipulación algorítmica;
- ataques a cuentas, dispositivos o bases de datos;

	MANUAL DE SEGURIDAD PARA ACTORES POLÍTICOS EN LOS PROCESOS ELECTORALES	DNEECT-001
		Versión 01
		Página 10 de 16

- automatización o amplificación del acoso mediante bots, cuentas falsas o redes coordinadas;
- publicación de mensajes provocadores, ofensivos o fuera de tema en línea, con el objetivo de generar conflictos, descalificar o desviar discusiones (troll).

La violencia digital puede constituir una forma de violencia política basada en género cuando se dirige desproporcionadamente contra candidatas, por su condición de mujer, mediante ataques a su vida privada, su entorno familiar y personal, apariencia, roles de género o amenazas sexuales y que afecta el ejercicio de sus derechos políticos. Es un fenómeno de alto impacto, con capacidad de amplificación, permanencia y viralidad, que puede afectar de manera diferenciada a personas con mayor exposición pública.

Artículo 14.- Medidas mínimas de protección digital

Las organizaciones políticas y/o actores políticos deberán promover, como mínimo, las siguientes medidas:

- Implementación de autenticación multifactor en cuentas oficiales y personales vinculadas a la actividad política.
- Políticas internas de gestión segura de contraseñas y restricción de accesos administrativos.
- Actualización permanente de dispositivos y uso de software de protección.
- Limitación en la difusión de datos personales sensibles vía WhatsApp u otros aplicativos de comunicación, como por ejemplo, contraseñas.
- **Uso de copias de seguridad periódicas almacenadas en entornos seguros (discos cifrados, por ejemplo).**
- **Separación entre cuentas personales y cuentas oficiales de campaña.**
- **Capacitación básica en reconocimiento de intentos de phishing y suplantación.**
- Protección adecuada de bases de datos de simpatizantes y voluntariado.
- Monitoreo de menciones hostiles en redes sociales.

 JNE JURADO NACIONAL DE ELECCIONES	MANUAL DE SEGURIDAD PARA ACTORES POLÍTICOS EN LOS PROCESOS ELECTORALES	DNEECT-001
		Versión 01
		Página 11 de 16

Artículo 15.- Prevención y respuesta frente al acoso digital

Las organizaciones políticas y/o actores políticos deberán establecer mecanismos de monitoreo periódico de redes sociales y plataformas digitales para identificar:

- incrementos anómalos de comentarios negativos;
- patrones que indiquen coordinación o automatización de ataques;
- difusión de discursos de odio, estigmatización o desinformación;
- amenazas o contenido que pueda poner en riesgo la integridad de candidaturas o equipos.

El monitoreo deberá respetar la normativa de protección de datos personales y evitar prácticas de vigilancia indebida sobre la ciudadanía o que vulneren los derechos de otras personas.

Asimismo, deberán contar con un protocolo interno que contemple un canal de reporte inmediato, asistencia técnica para recuperación de cuentas, mitigación de ataques, resguardo de evidencia, orientación legal cuando existan indicios de infracción o delito y acompañamiento psicológico en casos graves.

Cuando corresponda, deberá gestionarse ante las plataformas digitales la remoción de contenido que constituya amenazas, suplantación, doxxing u otras formas de violencia digital severa, conforme a las políticas de contenido y privacidad de cada servicio. Para ello, los actores políticos y equipos deberán conocer las reglas específicas que aplican en cada plataforma, así como los canales formales de reporte. En casos de amenazas graves o campañas coordinadas que generen riesgo físico, se deberá evaluar la actualización del nivel de riesgo físico y activar medidas preventivas adicionales.

Artículo 16.- Protección de información estratégica de campaña

Los actores políticos y sus equipos deberán adoptar medidas razonables para proteger documentos estratégicos, bases de datos, planes territoriales y demás información sensible frente a accesos no autorizados, filtraciones o pérdida de información. Se recomienda el uso de almacenamiento seguro, control de accesos con niveles diferenciados, cifrado de información relevante y copias de respaldo periódicas.

	MANUAL DE SEGURIDAD PARA ACTORES POLÍTICOS EN LOS PROCESOS ELECTORALES	DNEECT-001
		Versión 01
		Página 12 de 16

En caso de pérdida o filtración de información sensible, deberá activarse un protocolo de contención que incluya evaluación de impacto, cambio inmediato de credenciales comprometidas y comunicación interna preventiva y documentación del incidente.

Artículo 17.- Actuación frente a desinformación grave, contenidos sintéticos y manipulación audiovisual (deepfakes)

Cuando se identifiquen campañas de desinformación o contenidos sintéticos manipulados que puedan afectar gravemente la integridad del proceso electoral o la seguridad de candidaturas, la organización política y/o el actor político deberá documentar el caso y activar su protocolo interno de respuesta inmediata.

Dicho protocolo incluirá la verificación técnica del contenido cuando corresponda, la emisión de un desmentido público claro y verificable, y el reporte oportuno a las plataformas digitales para su evaluación y eventual retiro. El desmentido público deberá priorizar información verificable y evitar la reproducción innecesaria del contenido manipulado, reduciendo su amplificación.

Si existieran indicios de delito o afectación grave de derechos, deberá comunicarse a las autoridades competentes y preservarse las evidencias digitales para fines legales.

Artículo 18.- Gestión y escalamiento de incidentes

Toda organización política y/o actor político deberá contar con un Protocolo de Gestión de Incidentes de Violencia Digital que establezca de manera clara y operativa, el conjunto de procedimientos para prevenir, detectar, contener, clasificar, documentar y escalar cualquier hecho que constituya o pueda constituir violencia digital.

El protocolo deberá incluir, como mínimo:

- **Medidas de contención inmediata**, orientadas a limitar el daño, asegurar cuentas comprometidas, preservar evidencia digital y proteger a la persona afectada.
- **Criterios uniformes de clasificación de incidentes** en categorías (leves, moderados y graves), considerando factores como:

	MANUAL DE SEGURIDAD PARA ACTORES POLÍTICOS EN LOS PROCESOS ELECTORALES	DNEECT-001
		Versión 01
		Página 13 de 16

- nivel de riesgo para la integridad física, psicológica o digital de la persona afectada;
 - alcance del contenido (viralización, replicación en múltiples plataformas);
 - presencia de amenazas, suplantación, doxxing, deepfakes u otras modalidades severas;
 - indicios de coordinación o automatización del ataque.
- **Lineamientos detallados de documentación técnica**, que incluyan pautas para capturas, enlaces, metadatos, fecha y hora, registro de cuentas involucradas y cualquier otro elemento necesario para investigaciones posteriores.
- **Procedimientos de comunicación y escalamiento**, que contemplen:
 - Reporte inmediato a las plataformas digitales a través de sus canales oficiales cuando el incidente implique amenazas, suplantación, exposición de datos personales o contenidos manipulados;
 - Notificación a organismos electorales competentes cuando el incidente pueda afectar el ejercicio de derechos políticos o la integridad del proceso electoral;
 - Comunicación a autoridades penales cuando existan indicios de la presunta comisión de un delito.
- **Tiempos máximos de respuesta** para cada fase del incidente (detección, contención, documentación, escalamiento y cierre), diferenciados según la gravedad del caso, garantizando una actuación oportuna y continua.
- **Asignación de roles y responsabilidades**, identificando claramente a las personas u órganos internos responsables de recibir alertas de incidentes, ejecutar medidas de contención, resguardar evidencia, activar comunicaciones externas, brindar apoyo técnico, legal y psicosocial a la persona afectada y realizar el seguimiento hasta el cierre del caso.
- **Mecanismos de seguimiento y evaluación**, que aseguren la revisión periódica del protocolo, la actualización ante nuevas tecnologías y la retroalimentación basada en incidentes previos.

	MANUAL DE SEGURIDAD PARA ACTORES POLÍTICOS EN LOS PROCESOS ELECTORALES	DNEECT-001
		Versión 01
		Página 14 de 16

El protocolo deberá ser conocido por todas las personas candidatas, equipos de campaña, personal de comunicación y responsables de seguridad digital, garantizando su aplicación efectiva y uniforme.

Artículo 19.- Protección reforzada

Las organizaciones políticas y/o actores políticos deberán adoptar medidas reforzadas de protección digital para personas con mayor exposición a violencia política digital, incluyendo candidatas, jóvenes activistas, voceras y defensoras de derechos humanos, periodistas vinculadas a la campaña y equipos de comunicación expuestos a ataques sistemáticos.

Estas medidas podrán comprender monitoreo ampliado, capacitación específica en autoprotección digital y mecanismos de escalamiento prioritario ante plataformas y autoridades competentes.

Artículo 20.- Mejora continua

Las organizaciones políticas y/o actores políticos deberán promover una cultura institucional de prevención mediante programas de capacitación periódica en seguridad digital, violencia digital, IA, desinformación y protección de datos; participación en talleres especializados y coordinación con organismos electorales y entidades competentes, revisión y actualización anual de sus protocolos conforme avancen las tecnologías y aparezcan nuevos riesgos.

CAPÍTULO V MEDIDAS POSTERIORES A LA JORNADA ELECTORAL

Artículo 21.- Continuidad de medidas de protección

Las medidas de seguridad no cesan automáticamente con la culminación de la jornada electoral. Las organizaciones políticas y/o los actores políticos deberán mantener vigilancia razonable durante el periodo de cómputo oficial de resultados y eventuales controversias electorales, especialmente en contextos de alta polarización. La evaluación de riesgo deberá actualizarse durante el periodo postelectoral inmediato, especialmente en contextos de resultados estrechos o conflictividad social.

 JNE JURADO NACIONAL DE ELECCIONES	MANUAL DE SEGURIDAD PARA ACTORES POLÍTICOS EN LOS PROCESOS ELECTORALES	DNEECT-001
		Versión 01
		Página 15 de 16

Artículo 22.- Atención y seguimiento a víctimas de incidentes

En caso los actores políticos o integrantes del equipo de campaña hayan sido víctimas de agresiones físicas o digitales, la organización política deberá brindar acompañamiento institucional, orientación para la formulación de denuncias y seguimiento del caso ante las autoridades competentes. La organización política deberá evitar cualquier forma de revictimización y garantizar confidencialidad en la gestión del caso.

Artículo 23.- Evaluación y mejora posterior al proceso electoral

Concluido el proceso electoral, las organizaciones políticas deberán realizar una evaluación interna del funcionamiento de sus medidas de seguridad y autoprotección, identificando lecciones aprendidas y oportunidades de mejora para futuros procesos.

CAPÍTULO VI COORDINACIÓN INTERINSTITUCIONAL

Artículo 24.- Canales de alerta temprana

Las organizaciones políticas y/o actores políticos podrán establecer responsables de seguridad que mantengan canales de comunicación directa con la Policía Nacional del Perú y otras autoridades competentes para la activación de alertas tempranas ante situaciones de riesgo.

Podrán articularse con mecanismos de monitoreo de derechos humanos o instancias especializadas en protección del espacio cívico, cuando la situación lo amerite.

Artículo 25.- Coordinación interinstitucional

El Jurado Nacional de Elecciones promoverá mecanismos de coordinación y articulación con la Policía Nacional del Perú y demás entidades competentes, a fin de facilitar el intercambio oportuno de información, el seguimiento de situaciones de riesgo y la adopción de acciones preventivas en el marco del proceso electoral.

Dicha coordinación podrá incluir canales de comunicación directa, protocolos de actuación conjunta y mecanismos de alerta temprana frente a

	MANUAL DE SEGURIDAD PARA ACTORES POLÍTICOS EN LOS PROCESOS ELECTORALES	DNEECT-001
		Versión 01
		Página 16 de 16

hechos que puedan afectar la seguridad de candidaturas o la integridad del proceso electoral.

La coordinación podrá incluir intercambio de buenas prácticas, capacitaciones conjuntas y participación en mesas técnicas de prevención de violencia electoral.