



MODELO DE PLANEACIÓN INSTITUCIONAL DEL INE

COMPONENTE
Continuidad de Operaciones

2019

Contenido

I. INTRODUCCIÓN	3
II. SUSTENTO JURÍDICO	4
III. DIAGNÓSTICO INSTITUCIONAL RELATIVO AL COMPONENTE	4
III.1 Respuestas principales sobre el grupo que dice conocer el tema de continuidad de operaciones:.....	4
III.2 Respuestas principales sobre el grupo que señala desconocer el tema de continuidad de operaciones.....	6
IV. COMPONENTE DE CONTINUIDAD DE OPERACIONES	8
IV.1. Objetivo.....	8
IV.2. Objetivos específicos.....	8
IV.3. Alcance	8
V. EJES RECTORES DEL COMPONENTE	8
V.1 Plan de Continuidad de Operaciones y Protocolos.....	8
VI. PLAN DE CONTINUIDAD DE OPERACIONES.....	9
VI.1 Glosario de abreviaturas y definiciones.....	9
VI.2 Prioridades y Principios.....	9
VI.3 Actores involucrados y funciones	10
Nivel 1. Titular de la Secretaría Ejecutiva.....	10
Nivel 2. Coordinador del Plan de Continuidad de Operaciones.....	10
Nivel 3. Titular de la UR.....	11
Nivel 4. Enlace de Continuidad de Operaciones	11
Nivel 5. Funciones del responsable para la aplicación del protocolo	12
Nivel 6. Dirección Jurídica	12
Nivel 7. Unidad Técnica de Servicios de Informática	13
VI.4 De los Protocolos	13
Protocolos de nueva creación	14
Protocolos Existentes	14
Pruebas, revisión y actualización.....	14
VI.5 SICOOPER.....	15
VI.6 Protocolos externos al Plan	15
VII. ADMINISTRACIÓN DE RIESGOS	15

I. INTRODUCCIÓN

El Instituto Nacional Electoral tiene como objetivos estratégicos organizar procesos electorales con efectividad y eficacia; fortalecer la confianza y la participación ciudadana en la vida democrática y política del país, así como garantizar el derecho a la identidad. Tres pilares sustanciales para la democracia mexicana, en la cual la ocurrencia de incidentes siempre es latente.

Esta posibilidad conlleva el reto de garantizar mecanismos de recuperación y continuidad de operaciones oportunos, que permitan, por una parte, cumplir con las encomiendas emanadas de la Constitución Política y, por otra, con las expectativas de la ciudadanía y los actores políticos.

Así, el 29 de mayo de 2019 mediante el acuerdo INE/CG270/2019, se aprobó el Modelo de Planeación Institucional en el cual, se integró el Componente de “Continuidad de Operaciones” como marco general para responder organizadamente a la ocurrencia de eventos inesperados en los procesos sustantivos que podrían poner en riesgo el cumplimiento de la misión y objetivos estratégicos del Instituto en cuestión.

De esta forma el diseño prospectivo de planes de acción para la atención de posibles eventos no deseados es de vital importancia para el Instituto, ya que de materializarse pudieran afectar el desarrollo de las elecciones y las actividades asociadas al fortalecimiento democrático.

El presente componente considera el análisis de diversas metodologías relativas a la gestión de planes de continuidad de operaciones, el uso de buenas prácticas, normas internacionalmente aprobadas y basadas en la gestión de riesgos como ISO 22301 e ISO2700.

Al ser un marco metodológico del Modelo de Planeación Institucional, el componente de Continuidad de Operaciones se encuentra estructurado a partir de dos ejes rectores divididos en dos niveles, el primero, corresponde al “Plan de Continuidad de Operaciones”, que pertenece al actual documento y es de carácter permanente y contiene directrices institucionales generales para su funcionamiento, mientras que el segundo nivel es de carácter “protocolario”, que será temporal y específico.

Asimismo, este documento incluye el resultado de un diagnóstico institucional, que se realizó entre el personal de diferentes niveles y unidades responsables, para identificar el grado de conocimiento en la materia, así como el estado actual de los planes y protocolos de continuidad de operaciones que coexisten en el Instituto Nacional Electoral y la forma en que son gestionados.

II. SUSTENTO JURÍDICO

Acuerdo INE/CG270/2019	Acuerdos Segundo y Tercero
------------------------	----------------------------

III. DIAGNÓSTICO INSTITUCIONAL RELATIVO AL COMPONENTE

Con el propósito de conocer la información que tiene el personal del INE en sus diferentes unidades y vocalías, en materia de continuidad de operaciones, la Coordinación de Planeación Institucional elaboró un breve cuestionario para aplicar al personal del Instituto a través de una muestra aleatoria.

El cuestionario se estructuró en dos apartados, el primero se diseñó para las personas que indicaran conocer el tema de continuidad de operaciones; mientras que el segundo apartado, se elaboró para el personal que señalará no conocer el tema en cuestión, en este contexto los resultados obtenidos en la primera pregunta reflejan que el 41% de los encuestados conoce sobre la continuidad de operaciones, mientras que el 59% lo desconoce.

Derivado de lo anterior, a continuación, se exponen los resultados obtenidos en cada apartado:

III.1 Respuestas principales sobre el grupo que dice conocer el tema de continuidad de operaciones:

- Dentro del grupo de personas que señalaron conocer sobre el tema de continuidad de operaciones, el 39% mencionó que en su unidad o vocalía se cuenta con un análisis de impacto para la continuidad de operaciones; el 34% dijo que no cuentan con un análisis de impacto, y el 26% lo desconoce.
- El 80% de las personas dicen conocer sobre los potenciales riesgos que pueden repercutir en la continuidad de operaciones dentro de su unidad o vocalía, mientras que el 15% mencionó que desconocía sobre los potenciales riesgos.
- Sobre el tema de contar con alguna estrategia de recuperación de continuidad de operaciones en su unidad o vocalía, el 40% mencionó que sí cuentan con una estrategia, el 36% señaló que no, y el 24% lo desconoce.
- La mayoría de los encuestados, el 70% señaló que el INE cuenta con un plan de continuidad de operaciones; el 24% lo desconoce, y el 5% indicó que el INE no cuenta con un plan.

- Sobre la existencia de una clasificación de riesgos en sus unidades o vocalías, el 37% mencionó que sí existe una clasificación de riesgos que impactan en la continuidad de operaciones; el 34% dijo que no, y el 26% lo desconoce.
- El 36% mencionó que se administran los riesgos en su unidad o vocalía, mientras que el 64% señaló que no se administran los riesgos en su área.
- La mayoría de los encuestados, con un 73%, señaló no tener responsabilidad en la administración de algún protocolo, y el 27% dijo que sí. De las personas que mencionaron que sí, la gran mayoría pertenecen a Juntas Distritales y Locales Ejecutivas.
- El 47% mencionó que nunca ha participado en pruebas frecuentes para asegurar la continuidad de operaciones en su unidad o vocalía; el 22% una vez al año ha participado en pruebas; mientras que el 18% participó una vez al semestre.
- El 55% señaló conocer poco sobre las características de la continuidad de operaciones; mientras que el 29% y el 8% indicaron respectivamente conocer bien y muy bien las características de la continuidad de operaciones.
- El 55% señaló conocer poco sobre metodologías de identificación y administración de riesgos para la continuidad de operaciones; el 30% y el 6% mencionaron respectivamente conocer bien y muy bien sobre las metodologías.
- El 81% mencionó que los riesgos para la continuidad de operaciones se presentan durante los procesos electorales y en las operaciones cotidianas; mientras que el 13% indicaron que los riesgos sólo se presentan durante los procesos electorales, y el 6% mencionó que los riesgos se presentan únicamente en las operaciones cotidianas.
- El 44% señaló que los responsables de asegurar la continuidad de operaciones son los mandos medios, operativos y la alta dirección; mientras que el 27% mencionó que la responsabilidad es de la alta dirección; el 25% señala que los responsables son los mandos medios, y el 5% le deja la responsabilidad al nivel operativo.
- El 30% indica que el tipo de riesgo más frecuente que afecta las operaciones en su unidad o vocalía son el administrativo; seguido del humano con el 29%; el financiero con el 27%; el normativo con el 11%, y al final mencionan la imagen institucional con el 4%.
- En general, los tipos de riesgo más identificados por los encuestados son: Protocolos en Sistemas de Información; Protocolos de Protección Civil; Marco de Actuación para la Continuidad de Operaciones; Protocolo de Continuidad de Operaciones de los Procesos Electorales Locales 2019; Protocolo para Prevenir,

Atender y Sancionar el Hostigamiento y Acoso Sexual o Laboral; Marco de Actuación para la Continuidad de Operaciones del PEF; Protocolo para la Continuidad de Operaciones de la DEA; Protocolo de Seguridad de Módulos de Atención Ciudadana; Protocolo para Prevenir la Discriminación.

En conclusión la gran mayoría (con alrededor de 70%) de los encuestados reconoce que los riesgos pueden repercutir en la continuidad de operaciones en sus respectivas unidades o vocalías, señalan que los riesgos para la continuidad de operaciones se pueden presentar durante los procesos electorales y durante las operaciones cotidianas, y también parten de la idea de que el INE cuenta con un Plan de Continuidad de Operaciones, al tiempo que señalan no tener responsabilidades sobre la administración de algún protocolo.

Con respecto al tema de la existencia de clasificación de riesgos, su administración y estrategia para recuperar la continuidad de operaciones en sus unidades o vocalías, los encuestados se muestran divididos entre quienes reconocen la presencia de esos elementos en sus áreas y quienes dicen que no existen.

Por otro lado, la mayoría (con al rededor del 55%) conoce poco sobre las características de la continuidad de operaciones, la metodología de identificación y administración de riesgos.

Por lo tanto, la mayoría del primer grupo de encuestados demuestra tener nociones generales sobre la continuidad de operaciones, situación que va disminuyendo cuando se les pregunta de manera más particular sobre los principales elementos que componen la continuidad de operaciones. Además, las respuestas de la mayoría de los encuestados reflejan que no se sienten parte de los procesos de continuidad de operaciones tomando en cuenta que un número significativo señaló no tener responsabilidad o haber participado en pruebas referentes a la continuidad de operaciones.

III.2 Respuestas principales sobre el grupo que señala desconocer el tema de continuidad de operaciones

- El 31% de los encuestados señalaron que las situaciones de riesgo más frecuentes que han interrumpido sus actividades laborales en su unidad o vocalía son los sismos; mientras que un 19% indicó que son las interrupciones eléctricas; seguido de la interrupción de sistemas informáticos con un 15%, y el 8% destaca que el riesgo más frecuente son las inundaciones. El resto de los encuestados mencionaron otros elementos como la toma de instalaciones, falta de recursos humanos y económicos.
- El 53%, señala que ha recibido algún tipo de información ante riesgos de sismos para saber cómo actuar bajo esos eventos en su área de trabajo; mientras que el 18% ha recibido información con respecto a riesgos de incendios; seguido de un 11% que recibió información sobre riesgos de inundaciones. La interrupción eléctrica y de sistemas informáticos, fueron mencionados por un 5% de los encuestados.

- Conforme a la pregunta anterior, el 55% indica que la información recibida para responder ante determinados riesgos proviene del área técnica especializada dentro de su unidad o vocalía; el 14% apunta que la información proviene de la alta dirección; el 9% de mandos medios y 22% destaca que proviene de otras áreas.
- El 89% de los encuestados indica que ha participado en algún tipo de simulacro para saber cómo actuar bajo determinados riesgos; mientras que el 11% dice que no ha participado.
- Los simulacros más mencionados, en los cuales han participado los encuestados son referentes a los sismos e incendios.
- El 86% sabe a qué persona o autoridad dirigirse en caso de presentarse un riesgo en su unidad o vocalía, y el 14% señala que no identifica a la persona o autoridad.

En consecuencia, del grupo de personas que mencionaron no conocer sobre el tema de continuidad de operaciones, la mayoría reconoce que ha estado expuesto a un tipo de riesgo que interrumpe sus actividades laborales, destacando como riesgos más comunes los sismos, las interrupciones eléctricas, de sistemas informáticos y las inundaciones. La mayoría señala que ha recibido algún tipo de información para saber cómo actuar ante la presencia de un riesgo, principalmente relacionados con sismos, incendios e inundaciones, en donde además han participado en simulacros de sismos e incendios. También la mayoría de los encuestados sabe a qué persona o autoridad dirigirse ante situaciones de riesgo y señala que la información proporcionada en materia de riesgos proviene de un área técnica especializada.

Por lo tanto, si bien es cierto que un grupo de encuestados señalaron no conocer sobre el tema de continuidad de operaciones, también es cierto que en sus respectivas unidades y vocalías han sido participes y cuentan con información referente a la continuidad de operaciones, sobre todo en lo referente a riesgos externos como desastres naturales, seguido de riesgos internos asociados a la tecnología de la información.

Finalmente, la información obtenida como producto de la aplicación del cuestionario, permite acercarnos a la posición que los empleados del INE tienen con respecto a la continuidad de operaciones, de tal forma que nos lleve, entre otras cosas, a identificar áreas de oportunidad para el fortalecimiento de la continuidad de operaciones, un tema que es de vital importancia para el logro de la misión y objetivos estratégicos de la institución.

IV. COMPONENTE DE CONTINUIDAD DE OPERACIONES

IV.1. Objetivo

Contar con un Modelo de actuación institucional de Continuidad de Operaciones a través de la definición de un plan y por medio de protocolos específicos, para hacer efectivo el desarrollo de los procesos sustantivos del instituto ante la amenaza latente de riesgos o eventos no deseados.

IV.2. Objetivos específicos

- Prevenir que los riesgos sucedan y minimizar el impacto de los que no puedan ser prevenidos;
- Impulsar la preparación institucional frente a la materialización de riesgos que permita la óptima administración de crisis;
- Diseñar un esquema general de continuidad de operaciones homogéneo, permanente, dinámico y accesible, y
- Establecer los criterios de coordinación institucional para la pronta recuperación de los procesos afectados por la materialización de riesgos o eventos no deseados.

IV.3. Alcance

La Continuidad de Operaciones es el componente metodológico del Modelo de Planeación Institucional que dará sustento a las actividades del Instituto orientadas a prevenir y garantizar el desarrollo de sus procesos ante la ocurrencia de eventos no deseados, poniendo en práctica estrategias previamente definidas para la administración de crisis, planes y protocolos de recuperación y retorno a la operación normal.

V. EJES RECTORES DEL COMPONENTE

V.1 Plan de Continuidad de Operaciones y Protocolos

El Componente se divide en los siguientes ejes rectores:

1. Plan de Continuidad de Operaciones. Es de carácter permanente el cual será desarrollado en el presente documento y busca establecer la coordinación, funciones y canales de comunicación de los actores clave del componente metodológico, así como un esquema general de continuidad de operaciones.
2. Protocolos. Es de carácter temporal y específico, en el cual se definen los criterios y las directrices generales para su ejecución.

Los ejes rectores tienen como propósito orientar la actuación del personal del Instituto ante la materialización de eventos no deseados que puedan afectar la continuidad de operaciones. Serán de observancia obligatoria para las Unidades Responsables, las cuales

deberán de integrarlo e implementarlo en los procesos que conforme a su experiencia se consideren de mayor impacto y riesgo, bajo la coordinación de la Secretaría Ejecutiva.

VI. PLAN DE CONTINUIDAD DE OPERACIONES

VI.1 Glosario de abreviaturas y definiciones

Amenaza: Fenómeno o actividad que puede ocasionar daños al patrimonio, a la estabilidad o a la operación institucional.

Componente: Componente de Continuidad de Operaciones.

Impacto: Las consecuencias negativas que se generarían en el Instituto, en el supuesto de materializarse un riesgo.

Instituto: Instituto Nacional Electoral

Plan: Plan de Continuidad de Operaciones

Protocolos de Continuidad de Operaciones: Conjunto de acciones que describen secuencialmente los procedimientos y la forma de utilización de los recursos necesarios para recuperar la continuidad de operaciones en caso de interrupción.

Procesos Sustantivos: Conjunto de actividades que interactúan directamente con las funciones relevantes de la institución, es decir, con el cumplimiento de su misión, objetivos y proyectos estratégicos institucionales y el cumplimiento de sus metas.

Riesgo: Posibilidad de que ocurra un acontecimiento o evento no deseado que impacte de forma negativa el logro de los objetivos institucionales.

UR: Unidades Responsables o Unidad Responsable en el Instituto.

SICOOPER: Sistema de la Continuidad de Operaciones.

Vulnerabilidad: Se define como la debilidad o grado de exposición de un sujeto, institución o sistema a los efectos negativos de una amenaza.

VI.2 Prioridades y Principios

El Plan está orientado a las siguientes prioridades:

- a) La integridad física de las personas;
- b) La protección de los bienes del Instituto;
- c) El restablecimiento de la operación de los procesos sustantivos, y
- d) La recuperación de servicios e infraestructura ante la ocurrencia de eventos no deseados.

Principios Básicos del Plan:

- a) Participativo, formativo e incluyente con el personal; para lo cual los involucrados deberán integrarse a programas de capacitación y realización de simulacros para conocer el funcionamiento del Plan y probar la vigencia y funcionalidad de los protocolos, la capacitación deberá ser continua y extenderse a temas relacionados con programas de administración de riesgos que garanticen una cultura institucional en la materia;
- b) Interactivo, por lo cual las UR deberán utilizar los mecanismos de comunicación establecidos en el Plan y en el nivel protocolario;
- c) Jerárquicamente flexible, en el sentido que cada UR deberá ejecutar las acciones y etapas de los protocolos a su cargo en coordinación con las demás unidades involucradas y con la guía de la Secretaría Ejecutiva, y
- d) Dinámico, lo que significa que es susceptible a cambios y mejoras permanentes.

VI.3 Actores involucrados y funciones

El Plan se integrará por actores clave para la continuidad de operaciones con funciones diferenciadas según los siguientes niveles:

Nivel 1. Titular de la Secretaría Ejecutiva

- a) Impulsará la implementación y el funcionamiento del Componente;
- b) Conocerá y dará seguimiento al Componente;
- c) Conocerá, conforme a los lineamientos de funcionamiento del Comité de Planeación Institucional, los informes del estado del Componente, y
- d) Nombrará y dará a conocer a las UR la designación del coordinador, quien deberá tener un nivel jerárquico inmediato inferior.

Nivel 2. Coordinador del Plan de Continuidad de Operaciones

- a) Conducirá los trabajos para que las UR diseñen y alineen los protocolos vigentes y nuevos al Plan;
- b) Revisará, en conjunto con los responsables de aplicación de protocolos, el programa de simulacros para la revisión de operatividad y vigencia de los protocolos;
- c) Dará seguimiento a las acciones para la implementación de los simulacros;
- d) Conocerá las áreas de oportunidad identificadas en los simulacros para los diferentes protocolos;
- e) Impulsará la mejora de los protocolos y las modificaciones que en su caso se hicieran;
- f) Administrará el directorio de los enlaces y titulares de las UR;
- g) Vigilará el correcto funcionamiento, actualización y operatividad del SICOOPER;
- h) Recibirá los informes y reportes de las UR para integrarlos y presentarlos al Titular de la Secretaría Ejecutiva e instancias competentes, e

- i) Impulsará bianualmente un diagnóstico general del estado que guarda el Plan a nivel institucional.

Nivel 3. Titular de la UR

- a) Nombrará al enlace de Continuidad de Operaciones de la UR, el cual deberá ser de nivel jerárquico inmediato inferior;
- b) Enviará, por los medios electrónicos de que dispone el Instituto a la Dirección Jurídica, para su revisión y dictaminación los protocolos que se actualicen y los de nueva creación 5 días hábiles previos a su autorización;
- c) En el supuesto de protocolos que atiendan a causas de fuerza mayor o caso fortuito y se requiera su aplicación inmediata, no será necesaria dicha dictaminación, a fin de salvaguardar los intereses institucionales y garantizar la atención expedita de la contingencia que se presente, en cuyo caso únicamente se deberá remitir a la Dirección Jurídica para que ésta emita, en su caso, observaciones relevantes;
- d) Autorizará el alcance y contenido de los protocolos que requiera la UR, para lo cual cada instrumento deberá contener su nombre, cargo y firma; y
- e) Remitirá al Titular de la Secretaría Ejecutiva, a través del Coordinador del Plan de Continuidad de Operaciones, los protocolos autorizados debidamente firmados, así como los informes del estado y vigencia de protocolos.

Nivel 4. Enlace de Continuidad de Operaciones

- a) Fungirá como canal permanente de comunicación entre la UR y el Coordinador del Plan de Continuidad de Operaciones;
- b) Coordinará el diseño y actualización de los protocolos de su UR, así como la elaboración del informe que se presente a la Secretaría Ejecutiva;
- c) Remitirá para validación de la Dirección Jurídica, en el plazo establecido, los protocolos actualizados o de nueva creación, acción que deberá informarse al Coordinador del Plan de Continuidad de Operaciones;
- d) Supervisará la realización de pruebas periódicas para verificar la vigencia y funcionalidad de los protocolos de su UR;
- e) Transferirá el conocimiento al personal involucrado en el funcionamiento de los protocolos de su UR;
- f) Verificará la integración a la plataforma informática de los protocolos validados por la Dirección Jurídica;
- g) Coordinará al personal involucrado en el funcionamiento de los protocolos de su UR;

- h) Informará de forma expedita al Coordinador del Plan de Continuidad de Operaciones y al titular de la UR, de la activación y puesta en marcha de algún protocolo hasta su conclusión, indicando sus causas y estado;
- i) Presentará al Coordinador del Plan de Continuidad de Operaciones, un informe respecto de las acciones implementadas y los resultados sobre el protocolo activado, mencionando el tiempo requerido para la recuperación normal de actividades y,
- j) Alimentará el SICOOPER con los informes generados de la atención a contingencias y sus resultados, conforme a las lecciones aprendidas.

Nivel 5. Funciones del responsable para la aplicación del protocolo

- a) Diseñará el protocolo relativo al proceso sustantivo bajo su responsabilidad, conforme a los criterios previstos en el presente documento;
- b) Realizará el monitoreo y pruebas para verificar la vigencia y aplicabilidad del protocolo a su cargo;
- c) Propondrá al titular de la UR y enlace de Continuidad de Operaciones, los ajustes pertinentes a los protocolos, y
- d) Activará los protocolos a su cargo cuando sea necesario y dará seguimiento de su desarrollo hasta lograr la recuperación de la continuidad de operaciones.

Nivel 6. Dirección Jurídica

- a) Prestará, cuando se requiera, asesoría jurídica a la Secretaría Ejecutiva, respecto del Plan y los protocolos, a fin de asegurar el respeto y apego del Instituto al marco normativo aplicable y con ello lograr una adecuada coordinación con la UR involucrada en la implementación del Plan;
- b) Revisará la viabilidad jurídica de los protocolos, emitirá recomendaciones a las UR para su mejora, por los medios electrónicos de que dispone el Instituto en un plazo máximo de 5 días hábiles, y, en su caso, dictaminará que se apegan al marco normativo aplicable;
- c) Cuando se trate de protocolos que atiendan a causas de fuerza mayor o caso fortuito, recibirá la información que le remita la UR y observará, en su caso, aspectos relevantes para su atención, y
- d) Comunicará de las acciones mencionadas en el inciso anterior, al Coordinador del Plan de Continuidad de Operaciones, a través de copia de conocimiento de las recomendaciones que remita a la UR, o bien, de la dictaminación correspondiente, por los medios electrónicos de que dispone el Instituto.

Nivel 7. Unidad Técnica de Servicios de Informática

- a) Apoyará en el desarrollo y operación del SICOOPER.

VI.4 De los Protocolos

El nivel protocolario se desarrollará por las UR, guardando los canales de comunicación y las formalidades establecidas en el Plan.

Cada UR deberá generar sus propios protocolos de continuidad de operaciones, tanto para periodo de proceso electoral como ordinario. En la generación y gestión de protocolos podrán participar varias unidades.

Dichos protocolos deberán contar al menos con los siguientes elementos:

- a) Determinar el nombre del protocolo y clave, la cual llevará la siguiente nomenclatura:
 - Iniciales PCO (Protocolo de Continuidad de Operaciones) - iniciales de la Dirección Ejecutiva o Unidad Técnica/ año completo/número consecutivo;¹
- b) Definir el objetivo del protocolo, el cual deberá redactarse de forma sucinta y en tiempo infinitivo;
- c) Señalar el marco jurídico de aplicación, en donde deberán establecerse las disposiciones legales que sustenten la ejecución del protocolo;
- d) Integrar el diagnóstico, identificación y análisis de riesgos a la continuidad de operaciones;
- e) Clasificar el protocolo de acuerdo con el catálogo previsto;
- f) Definir el flujo de trabajo en el que se establezcan las acciones secuenciales para atender la contingencia y lograr la continuidad de operaciones;
- g) Especificar periodo para la aplicación de las pruebas de mantenimiento y revisión, y
- h) La firma del titular de la UR, la firma del enlace y la firma del responsable de aplicar el protocolo.

Los protocolos podrán considerar la inclusión de los elementos de activación siguientes:

- a) Condiciones de activación del protocolo;
- b) Medios para la declaración de activación;
- c) Personal responsable de activar y gestionarlo;
- d) Contactos del personal involucrado en la activación, gestión y operación;
- e) Niveles de priorización en la recuperación, y
- f) Los recursos humanos, financieros y materiales necesarios para atender las contingencias.

¹ A modo de ejemplo: PCO-DESPEN/2019/01

Protocolos de nueva creación

En el diseño y elaboración de protocolos, las UR deberán realizar un diagnóstico tomando en cuenta las siguientes acciones:

1. Determinar los procesos que sean sustantivos, considerando su impacto en el logro de los objetivos y proyectos estratégicos del Plan Estratégico Institucional 2016-2026, así como de sus objetivos particulares.
2. Experiencias recabadas de riesgos o amenazas materializadas con anterioridad.
3. Analizar sus procesos sustantivos para identificar los riesgos susceptibles de afectarles conforme a la administración del riesgo.

El diagnóstico permitirá identificar los protocolos de nueva creación para cada UR.

La creación de protocolos tiene carácter preventivo y busca reducir la incertidumbre en la materialización de riesgos e impactos, por lo que las UR no están obligadas a generar protocolos en todos los procesos sustantivos ni en todos los posibles riesgos.

En caso de amenazas, impactos y riesgos materializados, las UR, una vez que se retome la operación, deberán analizar la creación de un protocolo.

Protocolos Existentes

Los protocolos existentes antes de la aprobación del presente Plan deberán registrarse en el SICOOPER y se les asignará un responsable de la aplicación del protocolo.

Los responsables de la aplicación del protocolo y el enlace de continuidad de operación determinarán los plazos para las pruebas, mantenimiento y revisión de los mismos. Y en caso de actualización de protocolos, las UR procurarán alinearlos al presente Plan.

Los protocolos existentes a los cuales se alude en los párrafos anteriores tienen que ver con una diversidad de temáticas, por ejemplo, con protocolos de Protección Civil; Protocolos de Actuación para la Continuidad de Operaciones de los Procesos Electorales; Protocolos para Prevenir la Discriminación, para Prevenir el Acoso Sexual o Laboral, Protocolos referentes a los Recursos Financieros, Materiales, de Obras Públicas, Personal, entre otros.

Pruebas, revisión y actualización

Como parte del Plan, los protocolos deberán someterse por las UR a un proceso preventivo para revisar su vigencia y, en su caso, determinar su actualización atendiendo a las siguientes acciones:

- a) Verificar su aplicabilidad y vigencia y, en su caso, determinar su actualización, mínimo anualmente;
- b) Recordar al personal implicado la existencia del protocolo, funcionamiento y su rol en la implementación;

- c) Remitir al Coordinador del Plan de Continuidad de Operaciones, previo conocimiento del titular de la UR, un informe en el que se especifiquen los resultados de la revisión y prueba de los protocolos vigentes, y
- d) Los enlaces de las UR deberán informar al Coordinador del Plan de Continuidad de Operaciones, de aquellos protocolos que hubieren perdido vigencia y funcionalidad que en consecuencia requieran ser dados de baja. Estos protocolos permanecerán en la herramienta informática SICOOPER por un periodo de 3 años para su consulta.

VI.5 SICOOPER

Es la plataforma informática que servirá como repositorio de los protocolos de Continuidad de Operaciones.

Los protocolos registrados en el SICOOPER deberán contar cuando menos con los siguientes elementos:

- a) Protocolos autorizados;
- b) Flujo de trabajo en el que se establezcan las acciones secuenciales para atender la contingencia y lograr la continuidad de operaciones;
- c) Elementos de activación;
- d) Informes de atención de contingencias y resultados, y
- e) Protocolos no vigentes.

VI.6 Protocolos externos al Plan

En caso de que el Consejo General y/o sus comisiones determinen la generación de protocolos, las UR deberán atender las instrucciones de dichas comisiones y procurarán alinear dichos protocolos a los presentes criterios.

Los protocolos deberán estar registrados en el SICOOPER.

VII. ADMINISTRACIÓN DE RIESGOS

La correcta clasificación y valoración de riesgos, vulnerabilidades y amenazas permitirá la homologación institucional de los diagnósticos necesarios para el diseño de protocolos, facilitando así la administración y gestión del Plan de Continuidad de Operaciones.

La administración de riesgos se realizará con base en la Metodología de Administración de Riesgos del Marco Normativo de Control Interno del Instituto Nacional Electoral, tomando en cuenta los siguientes elementos:

- a) Identificación;
- b) Evaluación;
- c) Criterios;

- d) Clasificación, y
- e) Priorización

El apartado de riesgos de los protocolos podrá realizarse, considerando la metodología del control de control.