OPLE Veracruz
ORGANISMO PÚBLICO LOCAL ELECTORAL

Comisión Especial de Sistemas Informáticos

GUÍA PARA LA GENERACIÓN DE PLANES DE SEGURIDAD Y CONTINUIDAD DE LOS SISTEMAS INFORMÁTICOS

del

Organismo Público Local Electoral del Estado de Veracruz

Diciembre 2023

CONTENIDO

I. INTRODUCCIÓN

El Organismo Público Local Electoral del Estado de Veracruz (OPLEV) se encuentra inmerso en el Proceso Electoral 2023-2024 para renovar los poderes Ejecutivo y Legislativo en la Entidad. En ese sentido, para la correcta ejecución del mismo, se deben de realizar una serie de acciones tendientes a garantizar el desarrollo de las actividades de cara a la jornada electoral, los actos posteriores a las elecciones y los resultados electorales.

En este contexto, los sistemas informáticos electorales se han convertido en herramientas indispensables para ejecutar de forma eficiente las actividades que se llevan a cabo durante un proceso electoral. Asimismo, el OPLEV cuenta con diversos sistemas informáticos que dan soporte a las actividades ordinarias del Organismo, y que tienen alcances al interior o exterior del mismo.

A pesar de los esfuerzos del OPLEV por desarrollar y continuar perfeccionando diversos sistemas informáticos, es importante destacar que éstos no están exentos de sufrir amenazas tanto en el ámbito externo como interno, que podrían poner en riesgo su correcto funcionamiento o incluso llevar al colapso total de los mismos.

En la actualidad, los ataques cibernéticos se han incrementado en número y complejidad, tornándose más difíciles de detectar y contener. Como ya se ha mencionado, cualquier institución puede convertirse en blanco de ciberdelincuentes.

Un Plan para la Continuidad y la Seguridad de los Sistemas Informáticos, es un conjunto de medidas y procedimientos diseñados para garantizar la operación continua y adecuada de los sistemas de información, incluso en situaciones adversas o de crisis. Este plan busca minimizar los riesgos y las interrupciones que puedan afectar la disponibilidad, integridad y confidencialidad de la información y los servicios proporcionados por los sistemas informáticos

Por lo expuesto anteriormente, y en vista de la creciente dependencia de los procesos electivos al funcionamiento ininterrumpido de los sistemas informáticos, es que la Comisión Especial de Sistemas Informáticos en colaboración con la Unidad Técnica de Servicios Informáticos (UTSI) y en cumplimiento de la actividad 10 del Programa Anual de Trabajo ha elaborado esta guía.

Es importante tener en cuenta que esta guía se realizó con el fin de dotar de mayores herramientas además de las existentes a la UTSI para el desarrollo de las estrategias en materia de seguridad y continuidad exclusivamente relacionadas con el software utilizado en los sistemas del OPLE Veracruz.

II. PROCESO DE ANÁLISIS

La siguiente guía pretende establecer un enfoque integral para el desarrollo de planes de continuidad y seguridad informática en el contexto del Organismo Público Local Electoral del Estado de Veracruz, para uso interno de la UTSI en la que la Unidad en coordinación con la Comisión detallan un procedimiento de análisis sobre la información que se necesita generar al interior del área, con el fin de definir estrategias de seguridad y continuidad exclusivas del software.

El procedimiento se inicia con la comprensión de los conceptos fundamentales de seguridad informática, siendo crucial para la generación de información que respalde la elaboración de planes de continuidad. En esta etapa, se realiza una recopilación de información donde se identifican y catalogan los activos críticos vinculados a los sistemas. Posteriormente, se lleva a cabo un análisis detallado de riesgos e impacto, categorizando las posibles amenazas y creando una matriz que evalúa tanto la probabilidad de ocurrencia como el impacto asociado.

Basándose en este análisis, la UTSI puede desarrollar un Plan de Continuidad, estableciendo estrategias proporcionales a la criticidad de los activos identificados. La implementación del plan, junto con la documentación de cualquier desviación, y las pruebas consecuentes aseguran su eficacia en situaciones críticas. Este enfoque dinámico reconoce la naturaleza cambiante de los entornos tecnológicos, permitiendo actualizaciones periódicas para adaptarse a nuevas amenazas y garantizar la solidez de las medidas de seguridad implementadas.

Por otro lado, para la generación de información y documentación sobre seguridad informática, se inicia con un análisis de las amenazas más comunes, seguido del desarrollo del plan y su implementación. Esta información debe ser gestionada mediante la elaboración primigenia de un plan de trabajo que incluya la planificación detallada de las fases y actividades relacionadas o secundarias.

Por lo tanto, las fases clave del proceso de análisis incluyen:

a. CONCEPTOS BÁSICOS DE SEGURIDAD INFORMÁTICA

En esta sección, se presentan una serie de conceptos esenciales para comprender los temas abordados en este documento.

I. Términos de seguridad informática

Activo: Cualquier dato, dispositivo u otro componente del entorno que interviene en las actividades relacionadas con la información y los sistemas informáticos.

Amenaza: Es una circunstancia con el potencial de ocasionar daños o pérdidas en los sistemas informáticos.

Ataque: Acción organizada con intención de causar daños o problemas a un sistema informático o red.

Control: Es una medida implementada para prevenir la materialización de un riesgo.

Impacto: Efecto económico, operativo o reputacional causado por la materialización del riesgo.

Riesgo: Es la probabilidad que una amenaza pueda aprovechar una vulnerabilidad y causar daños a los activos

Vulnerabilidad: Debilidad del sistema informático que puede ser utilizada para causar daño.

II. Principios básicos de la seguridad informática

Mínimo privilegio: El usuario debe contar únicamente con los permisos estrictamente necesarios para efectuar las acciones requeridas, sin otorgar más ni menos de lo estrictamente necesario. Un atacante primero identifica este punto y concentra sus esfuerzos en esa área de debilidad.

Proporcionalidad: Las medidas de seguridad deben ser correspondientes con la importancia de lo que se protege y con el nivel de riesgo conocido.

Dinamismo: La seguridad informática no es un producto estático, sino un proceso continuo que requiere supervisión y mantenimiento constante.

Participación Universal: Todos los usuarios deben estar comprometidos en respaldar el sistema de seguridad establecido, colaborando activamente en su implementación y cumplimiento.

III. Los tres pilares de la seguridad informática

Confidencialidad. - Requiere que la información solo sea accesible para las personas con una autorización y control específicos. Este principio busca ocultar o mantener secreto determinada información o recursos, previniendo así la divulgación no autorizada sobre la organización.

Integridad. -Implica que la información permanezca inalterada ante posibles accidentes o intentos maliciosos. Sólo se podrá modificar la información mediante autorización. Este principio tiene como objetivo prevenir modificaciones no autorizadas en la información.

Disponibilidad. - Asegura que el sistema informático continúe funcionando sin experimentar degradaciones en cuanto a accesos. Es esencial proporcionar los recursos necesarios a los usuarios autorizados cuando los requieran. La información debe permanecer accesible para los elementos autorizados. El objetivo es prevenir interrupciones no autorizadas en los recursos informáticos.

b. MÉTODOS PARA DESARROLLAR PLANES DE CONTINUIDAD INFORMÁTICA

El plan de continuidad es una herramienta vital para identificar las potenciales amenazas sobre los activos y establecer controles estratégicos para minimizar su impacto en el caso de materializarse.

A continuación, se citan diversas metodologías como puntos de referencia para el análisis y la gestión de riesgos en sistemas, con el propósito de facilitar la elaboración de las etapas de evaluación de riesgos. Es relevante enfatizar que cada una de estas metodologías presenta sus propias fortalezas, ofreciendo así opciones que pueden ser elegidas y ajustadas según las necesidades particulares de la Unidad.

1. **ISO/IEC 27005**: Este tipo de método, establece límites del SGSI[1] al identificar los activos críticos de información como unidades de información, ubicación, departamentos, así como los riesgos internos o externos asociados.
2. **COBIT:** Esta metodología se basa en el ciclo de Deming, consiste en planificar, implementar, verificar y corregir. El proceso 9 de COBIT define el riesgo como cualquier amenaza que afecta a las metas u objetivos de la organización, causada por un evento no planificado.
3. **COSO:** Organización americana dedicada a la creación de guías y marcos de trabajo en el ámbito de la gestión de riesgos empresariales.
4. **MAGERIT**: Esta es una metodología española desarrollada por el Ministerio de Administraciones Públicas. Su objetivo es proporcionar criterios válidos en materia de TICs y se divide principalmente en 3 etapas:
    - **A.** La planificación del proyecto
    - **B.** Análisis de riesgos
    - **C.** Gestión de riesgos y tratamiento de riesgos

Estas metodologías se presentan como procedimientos sistemáticos y ordenados para materializar un conjunto de métodos, técnicas y herramientas. Aunque no contienen métodos específicos, detallan los procesos que conforman el marco de gestión de riesgo. Se eligen como referencia debido a su reconocimiento en el ámbito de la gestión de riesgos informáticos y su capacidad para adaptarse a contextos diversos, brindando así un enfoque integral y probado en la materia.

c. FASES PARA GENERAR INFORMACIÓN PARA LA EMISIÓN DE PLANES DE CONTINUIDAD

Tomando como base los conceptos generales utilizados como la identificación de activos, riesgos, amenazas e impacto, se detallan las siguientes fases:

1. Recopilación de información

La recopilación de información se basa en la generación de un inventario detallado de los activos indispensables para funcionamiento de los sistemas informáticos utilizados en el OPLEV, y que pudieran ser susceptibles de estar comprometidos en su funcionamiento durante el proceso electoral o en actividades ordinarias. Este inventario permitirá un análisis exhaustivo para identificar los componentes cruciales para el funcionamiento efectivo de los sistemas.

Los activos pueden incluir, entre otros: códigos fuente, bases de datos, espacios de almacenamiento, claves de usuarios, servidores, conexiones a internet, procesos técnicos operativos aprobados, documentación de los sistemas y recursos humanos.

Tabla 1. Inventario de activos con ejemplos:

[1] Sistema de Gestión de la Seguridad de Información.

No	Nombre del activo	Descripción	Responsable	Tipo	Ubicación
1	Sistema	Código fuente	Área de desarrollo de software	Intangible	Servidor ubicado en site de comunicaciones del edificio central
2	Base de datos	Base de datos	Área de desarrollo de software	intangible	Servidor ubicado en site de comunicaciones del edificio central
3	Servidor	Equipo servidor donde se aloja el sistema	Área de infraestructura	Equipo informático	Site de comunicaciones del edificio central

2. Análisis de riesgo e impacto

El objetivo de esta fase es proporcionar y analizar la información necesaria para la toma de decisiones en la estrategia de continuidad. Esto se logra identificando y clasificando los riesgos según su probabilidad de ocurrencia y su impacto potencial.

Para lograr lo anterior es necesario construir una **matriz de riesgos, considerando la experiencia y pericia de la UTSI, con el apoyo técnico de las áreas responsables.** En este proceso, se pueden seguir las consideraciones detalladas a continuación:

- **Identificación de amenazas.** Enumerar las amenazas potenciales que podrían afectar los sistemas informáticos. Estas amenazas pueden incluir ataques cibernéticos, malware, acceso no autorizado, fallas en el hardware, errores humanos, entre otros.
- **Categorización de las amenazas.** Clasificar las amenazas según su gravedad y probabilidad de ocurrencia. Para estimar la probabilidad, se pueden utilizar datos históricos, tendencias de seguridad y conocimiento experto.
  Esto ayudará a priorizar los riesgos y concentrarse en los más críticos, para lo anterior se propone las siguientes tablas de ponderación:

Tabla 2. Ejemplo de ponderación de la probabilidad de que se materialice una amenaza.

Probabilidad de materializarse una falla		
Grado	Descripción	Valor
Bajo	probabilidad < 20 %	1
Medio	probabilidad > 21% < 60 %	2
Alto	probabilidad > 61%	3

Tabla 3. Ejemplo de ponderación de impacto que tenga una amenaza en activo.

Impacto		
Grado	Descripción	Valor
Bajo	No compromete la funcionalidad del sistema	1
Medio	El fallo genera retrasos o pausas que son tolerables por un cierto tiempo	2

Alto	Fallo que genera la imposibilidad de funcionamiento del sistema, divulgación de información indebida, accesos no autorizados.	3

- **Evaluación de riesgos.** Calcular el nivel de riesgo para cada amenaza, sumando la probabilidad de ocurrencia más el impacto potencial. Esto permite una comparación cuantitativa y priorización de los riesgos.

- **Elaboración de la matriz de riesgos.** Esta matriz evalúa los riesgos asociados a los activos inventariados, priorizando aquellos de mayor criticidad para concentrar recursos económicos y humanos.

Tabla 4. Ejemplo de una matriz de riesgos.

No	Amenaza	Activo comprometido	Probabilidad de materializarse Tabla 2 (A)			Impacto Tabla 3 (B)			RIESGO (A + B)
			Bajo	Medio	Alto	Bajo	Medio	Alto	Nivel de riesgo
1	Daño irreversible	Base de datos	1					3	4

3. Desarrollo del plan de continuidad con sus estrategias

Basándose en la matriz de riesgo, las áreas responsables establecerán las estrategias de continuidad tomando en consideración la proporcionalidad, es decir, el activo involucrado y su impacto en los sistemas, analizados por la UTSI.

Asimismo, es importante que el plan de continuidad contemple un mecanismo de comunicación interna de crisis, lo anterior atendiendo a que la rapidez y transparencia en dar a conocer la información es clave en una situación de crisis. En ese sentido el mecanismo comunicación de crisis deberá contener al menos la siguiente información:

- Problema que está teniendo lugar, la causa y las consecuencias que puede tener.
- Alcance de la crisis y la ciudadanía o funcionariado que pueden verse afectados.
- Plan de acción y continuidad que se esté llevando a cabo o se vaya a implementar por las personas involucradas.
- Definir el canal adecuado para transmitir la información y la o el funcionario de la UTSI que debe realizar el comunicado y ante qué instancia.
- Establecer el proceso de comunicación entre la UTSI y la Comisión correspondiente o área responsable, de acuerdo al plan de acción y continuidad establecido.

También hay que hacer notar que los procedimientos establecidos en el Plan de continuidad deberán estar sujetos a una revisión periódica, debido a que los avances continuos en las tecnologías permiten ir

mejorando los enfoques de seguridad para minimizar las amenazas, y de igual manera dichas amenazas evolucionan con el tiempo.

En el contexto anterior, el Plan de continuidad deberá contener por lo menos los siguientes rubros o información:

I. Portada
II. Presentación
III. Glosario
IV. Objetivos y alcances
V. Inventario de activos
VI. Matriz de riesgos con sus tablas de ponderación
VII. Procedimientos de control
    a. Amenaza materializada.
    b. Activo comprometido
    c. Tiempo de respuesta esperado
    d. Acción a implementar
    e. Responsable de llevar a cabo la acción

VIII. Mecanismo de comunicación interna de crisis.
IX. Periodicidad para revisiones y actualización del plan de continuidad.
X. En su caso, un esquema de capacitación para personal de UTSI y/o personal del Organismo sobre los temas del plan que resulten pertinentes.

4. Implementación del plan de continuidad

Durante esta fase, la UTSI debe llevar a cabo la implementación del plan de continuidad establecido, documentando cualquier desviación de la estrategia acordada, indicando la razón y la versión del plan resultante. Al final de esta fase se deberá contar con el **Plan de continuidad**, especificando su versión correspondiente.

5. Pruebas del Plan de continuidad

Durante esta fase se deben realizar ejercicios, simulacros o cualquier otra actividad que tenga como fin validar que el Plan de continuidad funciona adecuadamente. Es importante señalar que el Plan de continuidad es un documento dinámico, sujeto a actualizaciones debido a la naturaleza cambiante de los activos, tecnologías y técnicas informáticas.

d. FASES PARA DESARROLLAR EL PLAN DE SEGURIDAD INFORMÁTICA

Los planes de seguridad informática son un conjunto de políticas y prácticas destinadas a proteger los datos y sistemas informáticos de una institución. Éstos se basan en tres pilares fundamentales de la seguridad informática: confidencialidad, integridad y disponibilida; las fases para su desarrollo son:

1. Análisis de las amenazas más comunes

Las amenazas a la seguridad se refieren a la explotación de una vulnerabilidad o fallo que se utilizan para afectar la operatividad de un sistema informático, con la intención de sacar algún provecho. Las amenazas informáticas pueden clasificarse, según su origen y a grandes rasgos, en dos categorías:

1. Amenazas informáticas externas:

Se trata de amenazas que provienen de fuera de la institución y que escapan al control de la UTSI. Estas amenazas incluyen virus, gusanos, troyanos, etc.

2. Amenazas informáticas internas:

Son amenazas que se originan en la propia institución y pueden ser controladas, hasta cierto punto, por la UTSI. Éstas incluyen el acceso no autorizado a los sistemas informáticos, el robo de datos, etc. En esta fase se debe identificar y evaluar las amenazas y vulnerabilidades potenciales a las que están expuestos los sistemas informáticos del OPLE Veracruz. También se debe determinar las posibles consecuencias y el impacto que podrían tener para la institución de verse comprometido algún activo detectado para el desarrollo del plan de continuidad.
Para facilitar el análisis a continuación se plantea un ejemplo de cómo puede desarrollarse una matriz de las amenazas más comunes para los sistemas informáticos. Aunque se sugiere utilizar los criterios de las Tablas 2 y 3, cabe destacar que esta matriz puede ser modificada para mejorar su utilidad y adaptarse mejor a las necesidades específicas a la valoración de los sistemas e infraestructura del Organismo.

Tabla 5. Matriz de análisis de amenazas de seguridad

No	Amenaza	Descripción	Probabilidad de ocurrir (A)			Impacto (B)			RIESGO (A + B)
			Bajo	Medio	Alto	Bajo	Medio	Alto	Ponderado
1	Malware	Programas maliciosos como virus, gusanos, troyanos, ransomware, etc., que pueden afectar negativamente el sistema y los datos.							
2	Ataques de hackers	Intentos de acceder ilegalmente a un sistema para robar información confidencial, dañar los datos o interrumpir el funcionamiento normal.							
3	Ataques de denegación de servicio (DoS)	Inundar un sistema con exceso de solicitudes, sobrecargándolo y dejándolo inaccesible para los usuarios legítimos.							

No	Amenaza	Descripción	Probabilidad de ocurrir (A)			Impacto (B)			RIESGO (A + B)
			Bajo	Medio	Alto	Bajo	Medio	Alto	Ponderado
4	Ataques de ingeniería social	Manipulación o engaño psicológico a través de técnicas como el phishing, el spear phishing o el pharming para obtener información confidencial.							
5	Fugas de información	Divulgación accidental o intencional de información sensible o confidencial, ya sea por parte de empleados, socios o hackers externos.							
6	Acceso no autorizado	Intento de acceso a sistemas o datos sin la debida autorización o permiso.							
7	Fallos de seguridad física	Robo de equipos, cableado dañado o accesibilidad no autorizada a áreas restringidas.							
8	Fallos en el software	vulnerabilidades o debilidades en el código o diseño del software que pueden ser explotados por atacantes.							
9	Ataques a dispositivos móviles	Robo de información o control remoto de dispositivos móviles, como smartphones o tablets, mediante el uso de malware o aplicaciones maliciosas.							
10	Intercepción de datos	Robo de información en tránsito a través de redes no seguras o captura de paquetes de datos.							

Estas son solo algunas de las amenazas más comunes, pero la lista es amplia y continúa evolucionando con nuevas técnicas y tecnologías.

2. Desarrollo del Plan de seguridad informática con sus estrategias

Teniendo en consideración los tres pilares de la seguridad informática, la UTSI elaborará las políticas de seguridad que construirán el Plan de seguridad informática para los sistemas electorales.

En esta fase basándose en la matriz de la Tabla 5, la UTSI establecerá las políticas de seguridad tomando en consideración la proporcionalidad, es decir, el activo involucrado y su impacto en los sistemas.

El plan de seguridad informática deberá contener por lo menos la siguiente información para cada política o estrategia de control desarrollado para cada amenaza:

a) Amenaza
b) Activos susceptibles de la amenaza
c) Política o estrategia de seguridad para mitigar la amenaza
d) Responsable de ejecutar la acción
e) En su caso, mecanismo de comunicación de crisis

Como se mencionó anteriormente, comunicar la información oportunamente es una de las mejores acciones a llevar a cabo al enfrentar una crisis, es por esto que el plan de seguridad deberá prever un mecanismo de comunicación de crisis cuando una amenaza esté generando un impacto en algún activo.

A final de esta fase, se deberá contar con el **Plan de seguridad informática**, especificando su versión. Es importante subrayar que, dada su naturaleza de seguridad, el plan no debe contener contraseñas, direcciones electrónicas o cualquier otro elemento que pueda comprometer la seguridad de los sistemas.

3. Implementación del Plan de seguridad informática

Durante esta etapa, la UTSI llevará a cabo la implementación del Plan de seguridad informática establecido. En caso de que alguna política o estrategia no haya sido posible implementarla según lo acordado, se deberá documentar el motivo, en su caso la nueva política o estrategia que sustituya.

Es crucial destacar que el Plan de seguridad informática es un documento que puede estar sujeto a actualizaciones continuas, debido a la naturaleza dinámica de los activos, tecnologías y técnicas informáticas.

En este sentido, se recomienda que cualquier modificación subsiguiente al plan sea debidamente comunicada al área responsable. Esta precaución se basa en la necesidad de mantener una coordinación eficiente entre las y los responsables de la seguridad informática y demás partes interesadas, asegurando que las actualizaciones sean coherentes con los objetivos estratégicos y los requisitos normativos establecidos.

Para garantizar el éxito de los planes de seguridad y continuidad, es esencial involucrar a las áreas responsables de los sistemas en su ejecución. Esto no solo facilita la comprensión de las medidas, sino que también posibilita la realización de observaciones y evaluaciones para asegurar su efectividad.

Adicionalmente, la UTSI deberá establecer un mecanismo eficiente para comunicar las estrategias que se proyecten implementar.

e. ELABORACIÓN DEL PLAN DE TRABAJO PARA LA ELABORACIÓN DEL PLAN DE SEGURIDAD DEL OPLE VERACRUZ.

El plan de trabajo es un documento esencial que permite llevar un seguimiento y control adecuado del proyecto y garantizar su éxito, tomando en cuenta tanto las limitaciones como las capacidades disponibles de cara a los futuros procesos electorales. Además, facilita la identificación y planeación de actividades; sus fechas de ejecución y los posibles desafíos que pueden surgir; lo que resulta en una gestión más eficaz de los recursos, incluyendo los financieros, materiales y humanos.

Lo anterior, asegura que las metas y objetivos sean realistas y alcanzables dentro del marco de recursos y condiciones existentes.

En este sentido, la UTSI deberá generar un Plan de trabajo para proyectar el desarrollo del Plan de continuidad y seguridad, en el que debe contemplar al menos la siguiente información:

- Presentación
- Objetivo general
- Objetivos específicos
- Organigrama de la UTSI
- Alcances y limitaciones del plan de trabajo
- Inventario de sistemas informáticos del OPLEV, tanto de desarrollo por la UTSI cómo desarrollado por un proveedor
- Planificación temporal de la fases y actividades adicionales o secundarias
- Programación de los informes a emitir a la Secretaría Ejecutiva, o en su caso la Comisión que dé seguimiento al o los sistemas.

El Plan de trabajo deberá ser presentado para su aprobación en la Comisión que dé seguimiento al o los sistemas e informado a la Secretaría Ejecutiva.

III. NUEVAS SOLUCIONES TECNOLÓGICAS PARA GARANTIZAR LA CONTINUIDAD Y SEGURIDAD

Por otra parte, en el marco del estudio de la información que colabore a aumentar el nivel de continuidad en los servicios y seguridad de los sistemas informáticos, es crucial evaluar la viabilidad de migrar los sistemas informáticos críticos hacia la computación en la nube.

Esta estrategia implica la adquisición de capacidad informática, almacenamiento de bases de datos, aplicaciones y otros recursos de tecnologías de la información a través de una plataforma de servicios en la nube accesible por Internet.

Dicha migración ofrece diversas ventajas, entre las cuales se destacan:

- Contratar servicios en la nube solo durante el tiempo necesario para el proceso electoral, evitando inversiones que no se utilizaran de forma permanente.

- Flexibilidad para ajustar la capacidad de cómputo contratada, a medida que sea necesario o conforme el proyecto avance en fases críticas.
- Mayor velocidad para incrementar la capacidad de cómputo y responder rápidamente a la demanda de usuarios y procesos.
- Adherencia a estándares internacionales de disponibilidad de servicios e infraestructura.
- Garantía de redundancia en los servicios y acceso a servicios de seguridad gestionados de clase mundial.
- Externalización del soporte técnico de la infraestructura de cómputo a un proveedor, permitiendo que el personal de UTSI se enfoque en los temas tecnológicos específicos de los programas del Organismo.

La migración de cómputo a la nube se presenta como una estrategia proactiva para mejorar la seguridad, fortalecer la continuidad operativa y optimizar la gestión de recursos tecnológicos, contribuyendo así a mejorar los servicios ofrecidos por la UTSI al Organismo, Partidos Políticos y la ciudadanía en general.

Cualquier decisión relacionada con esta migración deberá ajustarse a las políticas presupuestales previamente aprobadas por el OPLE Veracruz. Asimismo, se sugiere llevar a cabo un análisis más exhaustivo mediante un estudio FODA, considerando a fondo las fortalezas, oportunidades, debilidades y amenazas asociadas a este proceso. Este enfoque permitirá una evaluación integral y fundamentada, respaldando así las determinaciones que se adopten en este contexto.

CONCLUSIONES

En conclusión, la guía propuesta para la generación de información destinada a la elaboración de planes de continuidad y seguridad informática en los sistemas electorales del Organismo Público Local Electoral del Estado de Veracruz constituye un marco integral y estratégico. A través de un proceso analítico que abarca desde la comprensión de los conceptos fundamentales hasta la implementación y prueba de los planes resultantes, la guía proporciona una estructura sólida y dinámica para fortalecer la seguridad y garantizar la continuidad operativa.

La importancia de identificar y catalogar activos críticos, analizar riesgos e impactos, y desarrollar estrategias proporcionales a la criticidad de los sistemas se destaca como un enfoque proactivo y necesario en un entorno tecnológico cada vez más desafiante. Asimismo, la consideración de la migración a la nube se presenta como una medida estratégica para potenciar la seguridad y la flexibilidad operativa.

El énfasis en la actualización periódica de los planes, la documentación de desviaciones y la realización de pruebas contribuyen a un enfoque dinámico que reconoce la naturaleza cambiante de las amenazas y tecnologías.

En última instancia, la guía no solo se posiciona como una herramienta técnica, sino como un marco que promueve la conciencia y el compromiso de todas las partes involucradas, subrayando la necesidad de la seguridad informática y la continuidad operativa como componentes esenciales para la integridad de los sistemas en el contexto de un proceso electoral.

Basándonos en los alcances mencionados, la Comisión presenta esta guía destinada a generar información para la elaboración de planes de continuidad y seguridad en los sistemas informáticos, para uso interno de la UTSI.