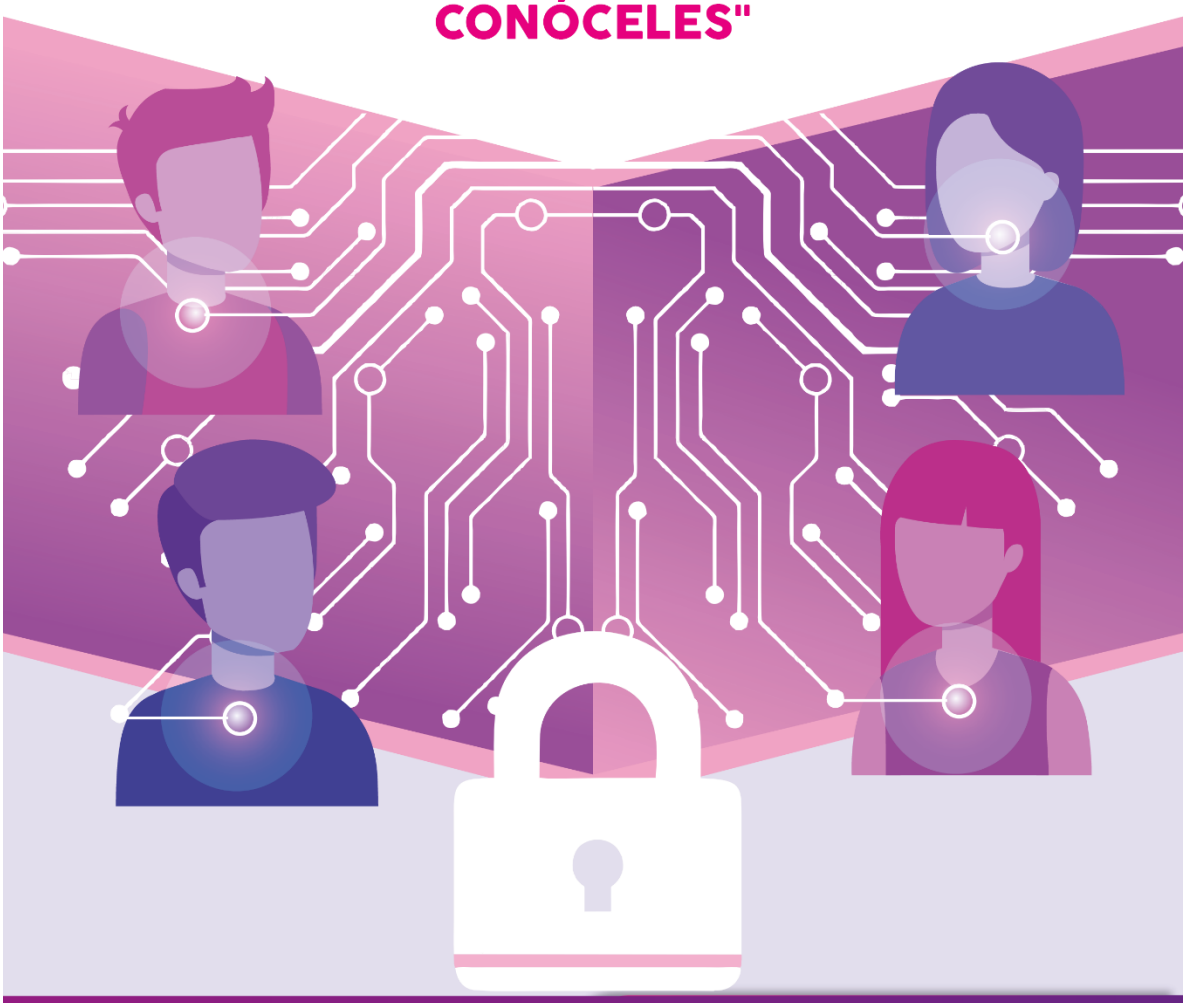
OPLE Veracruz
ORGANISMO PÚBLICO LOCAL ELECTORAL

Proceso Electoral 2023 2024

Mi voz, mi voto, mi elección Veracruz

PLAN DE CONTINUIDAD DEL SISTEMA "CANDIDATAS Y CANDIDATOS, CONÓCELES"



Presentación

El Consejo General del Instituto Nacional Electoral aprobó el siete de septiembre de dos mil veintidós el Acuerdo INE/CG616/2022, mediante el cual incorporó la obligatoriedad de la publicación de información curricular y de identidad de las candidaturas en elecciones federales y locales, así como la aprobación de los Lineamientos para el uso del sistema "Candidatas y Candidatos, Conóceles" para los procesos electorales federales y locales.

El treinta de agosto del dos mil veintitrés, el Consejo General del Organismo Público Local Electoral del Estado de Veracruz, mediante Acuerdo OPLEV/CG108/2023 aprobó la creación e integración de la Comisión Temporal del Sistema de referencia y designó a la Unidad Técnica de Transparencia como la instancia interna responsable de la coordinación del mismo y a la Dirección Ejecutiva de Prerrogativas y Partidos Políticos y a la Unidad Técnica de Servicios Informáticos, como unidades responsables de apoyo en los trabajos relacionados con éste.

El treinta de octubre de dos mil veintitrés, el Consejo General de este Organismo a través del Acuerdo OPLEV/CG141/2023, aprobó el Plan de Trabajo para la implementación y operación del Sistema de mérito, para el proceso electoral local ordinario 2023-2024. En este documento se determinó la elaboración del Plan de Continuidad del Sistema.

El artículo 8 fracciones II y IV de los Lineamientos para el Uso del Sistema "Candidatas y Candidatos, Conóceles" para los procesos electorales locales, prevén que este Sistema informático cuente con diversas especificaciones de cada uno de los componentes, así como de los procesos, tomando en cuenta aspectos de funcionalidad, capacidad, continuidad y seguridad. Mientras que, en la fase de pruebas, se deberá cubrir, entre otros, los aspectos de continuidad y seguridad del mismo.

Es de resaltarse que, el treinta de diciembre de dos mil veintitrés el Consejo General de este Organismo emitió el Acuerdo OPLEV/CG218/2023, por el que se aprueba la Guía para la generación de Planes de continuidad y seguridad de los sistemas informáticos del Organismo Público Local Electoral del Estado de Veracruz.

Si bien en el antepenúltimo párrafo del considerando 11 y en el Acuerdo segundo del documento antes indicado se estipuló que el Plan debe centrarse especialmente en los Sistemas de Cómputos, Seguimiento de Paquetes y de Registro de Candidaturas Locales, ello no es impedimento para que la Guía de referencia constituya un documento rector de aplicación análoga para otros sistemas informáticos que el Organismo Público Local Electoral debe implementar para el Proceso Electoral Local Ordinario 2023-2024.

Lo anterior, dado que en el considerando 10 del referido Acuerdo, también se estableció que "la Guía tiene como objetivo establecer un modelo de trabajo que permita al OPLE Veracruz documentar la información esencial. La metodología propuesta busca minimizar riesgos y garantizar el correcto desempeño de los sistemas informáticos, considerando directrices ante situaciones previsibles derivadas del uso continuo de dichos sistemas".

Ahora bien, el Plan de Continuidad del Sistema "Candidatas y Candidatos, Conóceles" tiene como propósito garantizar la operación continua y adecuada del sistema de información, incluso en situaciones adversas o de crisis, mediante el establecimiento de un conjunto de medidas y procedimientos diseñados para tal efecto.

Glosario

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

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

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

IV. **Confidencialidad:** Este principio de seguridad informática busca ocultar o mantener secreto determinada información o recursos, previniendo la

divulgación no autorizada sobre la organización. Requiere que la información solo sea accesible para las personas con autorización y control específicos.

V. **Control:** Medida implementada para prevenir la materialización de un riesgo.

VI. **DEPPP:** Dirección Ejecutiva de Prerrogativas y Partidos Políticos del Organismo Público Local Electoral del Estado de Veracruz.

VII. **Disponibilidad:** Busca prevenir interrupciones no autorizadas en los recursos informáticos, por lo que la información debe permanecer accesible para los elementos autorizados. Asegura que el sistema informático continúe funcionando sin experimentar degradaciones en cuanto a accesos.

VIII. **Impacto:** Efecto económico u operativo causado por la materialización de un riesgo.

IX. **Instancia Interna**: Unidad Técnica de Transparencia del Organismo Público Local Electoral del Estado de Veracruz.

X. **Integridad:** Este principio de seguridad informática tiene como objetivo prevenir modificaciones no autorizadas en la información e implica que ésta permanezca inalterada ante posibles accidentes o intentos maliciosos. Sólo se podrá modificar la información mediante autorización.

XI. **Riesgo:** Probabilidad que una amenaza pueda aprovechar la vulnerabilidad y causar daños a los activos.

XII. **Sistema:** Sistema de "Candidatas y Candidatos, Conóceles."

XIII. **UTSI:** Unidad Técnica de Servicios Informáticos del Organismo Público Local Electoral del Estado de Veracruz.

XIV. **Vulnerabilidad:** Debilidad del Sistema informático que puede ser utilizada para causar daño.

Objetivo General

Establecer los procedimientos para salvaguardar la disponibilidad, confidencialidad e integridad de la información, así como la continuidad de la operación del Sistema de "Candidatas y Candidatos, Conóceles" para el Proceso Electoral Local Ordinario 2023-2024.

Alcance

El plan de continuidad implementará los procedimientos que atenderán los procesos de operación del Sistema de "Candidatas y Candidatos, Conóceles": captura, validación y publicación de la información para el Proceso Electoral Local Ordinario 2023-2024.

Procedimientos de control

Procedimiento 1.

I. Amenaza materializada

A) Falla en el servicio de internet de la instancia interna o de la DEPPP por parte del proveedor.

II. Acto comprometido

Se compromete la revisión de la información publicada efectuada por parte de la Instancia Interna del sistema. Es indispensable para la operación diaria del sistema, toda vez que puede incidir en que se encuentre visible información que contenga alguna de las prohibiciones estipuladas en el artículo 18 de los Lineamientos para el Uso del Sistema "Candidatas y Candidatos, Conóceles" para los procesos electorales locales.

Se compromete, en su caso, el proceso de sustitución de las candidaturas por parte de la DEPPP. Es indispensable para la operación diaria del Sistema, toda vez que puede incidir en que no se cuente visible información obligatoria.

III. Tiempo de respuesta esperado

2 horas

IV. Acción a implementar

- **En primer nivel, la Instancia Interna** solicitará soporte técnico a la UTSI para que revise la conectividad de los equipos destinados a la operación del Sistema.
- **En segundo nivel, la UTSI** solicitará soporte técnico al proveedor del servicio de internet en dicha área.

  De persistir la falla, se buscará una sede alterna para realizar la revisión de la información o realizar el proceso de sustitución.

Procedimiento 2.

I. Amenaza materializada:

A) Combustión espontánea o corto circuito de algún elemento que forme parte de algún equipo de cómputo o dispositivo.

II. Acto comprometido

Se compromete la revisión de la información publicada efectuada por parte de la instancia interna del sistema. Es indispensable para la operación diaria del sistema, toda vez que puede incidir en que se encuentre visible información que contenga alguna de las prohibiciones estipuladas en el artículo 18 de los Lineamientos para el Uso del Sistema "Candidatas y Candidatos, Conóceles" para los procesos electorales locales.

Así mismo, también se compromete la atribución que tiene la DEPPP de suprimir aquella información en el Sistema de una candidatura sustituida una vez que así lo apruebe el Consejo General.

III. Tiempo de respuesta esperado

2 horas

IV. Acción a implementar

- **En primer nivel, la Instancia Interna o la DEPPP** solicitará soporte técnico a la UTSI para que revise el equipo de cómputo y determine el grado del daño del equipo y, en su caso, si se puede reparar o es pérdida total.
- **En segundo nivel,** en caso de no tener reparación el equipo de cómputo dañado, la Instancia Interna o la DEPPP solicitará a la UTSI la instalación de un nuevo equipo de cómputo.

Procedimiento 3.

I. Amenaza materializada:

A) Cortocircuito en la instalación eléctrica que alimenta los equipos instalados en el área de servidores.

II. Acto comprometido

Se compromete los equipos de almacenamiento y procesamiento de datos, así como el equipo de telecomunicaciones y de alimentación de respaldo. Es indispensable para la operación diaria del sistema.

III. Tiempo de respuesta esperado

Inmediata, una vez detectado el siniestro.

IV. Acción a implementar

- Se cuenta con una instalación eléctrica con tierra física apropiada con la correcta polaridad de los contactos para evitar contratiempos relacionados con el suministro eléctrico.
- Se tienen instaladas dos fuentes de alimentación ininterrumpida (UPS) con regulador integrado, de manera que, ante una posible variación en el suministro eléctrico, el equipo de cómputo esté debidamente protegido y pueda continuar su operación.

- Se cuentan con extintores (basados en CO_2 y polvo químico seco) distribuidos estratégicamente en toda la unidad.

Procedimiento 4.

I. Amenaza materializada:

A) Acceso no permitido al área de servidores.

II. Acto comprometido

Se compromete la integridad de los equipos de almacenamiento y procesamiento de datos, así como el equipo de telecomunicaciones. Es indispensable para la operación diaria del sistema.

III. Tiempo de respuesta esperado

1 hora

IV. Acción a implementar

- El acceso a los servidores está bajo llave y solo personal autorizado puede tener acceso.
- Se cuenta con contraseñas en los servidores y su acceso solo es de forma local además de establecer el bloqueo automático de pantalla en todas las computadoras.
- Se cuenta con seguridad en la entrada del edificio en dado caso que no se encuentre personal de la UTSI es informado al área correspondiente para verificar el acceso.
- Monitoreo por video CCTV en el edificio del OPLE Veracruz, teniendo acceso en cualquier momento el personal autorizado tanto a las imágenes en tiempo real, como a las grabaciones.

Procedimiento 5.

I. Amenaza materializada:

A) Problemas y exposiciones en aplicación y componentes del sistema, tales como: código malicioso en el software, ataques externos para obtención indebida de claves asignadas, ataques externos para obtención o modificación indebida de información.

II. Acto comprometido

Se compromete la integridad de la información en los equipos de almacenamiento. Es indispensable para la operación diaria del sistema.

III. Tiempo de respuesta esperado

1 hora

IV. Acción a implementar

- Se cuenta con un programa Oracle VM Manager el cual genera respaldo del sistema operativo, base de datos y configuraciones. En caso de pérdida o alteración indebida de la información se utilizará el respaldo creado por el programa antes citado.
- Se cuenta con un sistema operativo de uso empresarial basado en Linux el cual brinda alto nivel de seguridad para las aplicaciones, contando con las últimas actualizaciones, mismas que contienen comprobaciones periódicamente en sus vulnerabilidades y creando parches de seguridad.
- Se cuenta con un firewall físico con los siguientes servicios: Prevención de intrusos (IPS), antivirus, Filtros DNS, Filtros de correos, firewall de aplicaciones web, control de aplicaciones y control de usuarios.
- Los servidores donde se almacenen programas y datos, tienen cuentas con diferentes privilegios disponible en el sistema operativo teniendo en particular restringida la instalación de software o modificación de la información.

- Protección de seguridad del Framework Laravel contra vulnerabilidades comunes, como el cross-site scripting (XSS) y los ataques de inyección de código.
- Uso de tokens temporales para verificar la autenticidad de los usuarios.
- Rutas seguras (Certificado SSL).
- Contraseñas cifradas.

Procedimiento 6.

I. Amenaza materializada:

A) Fuga de información de claves de usuarios.

II. Acto comprometido

Se compromete el acceso al sistema, la alteración de la información en particular de la o las cuentas afectadas.

III. Tiempo de respuesta esperado

Media hora después del reporte de la pérdida de las contraseñas.

IV. Acción a implementar

- Se deberá reportar de manera inmediata a la Instancia Interna y esta a su vez solicitar el apoyo de la Unidad Técnica de Servicios Informáticos para deshabilitar las cuentas comprometidas y realizar el restablecimiento de las contraseñas.
- Será responsabilidad de la o el propietario de la cuenta vulnerada la verificación y, en su caso, la solicitud de rectificación de la información que hubiera sido alterada.

Procedimiento 7.

I. Amenaza materializada:

A) El sistema informático de captura y validación, así como el sitio de publicación no está disponible.

II. Acto comprometido

Se compromete el acceso al sistema y al sitio de publicación.

III. Tiempo de respuesta esperado

2 horas.

IV. Acción a implementar

- Se analizará la viabilidad de tener en todo momento disponible en equipos redundantes tanto los servidores de aplicación, bases de datos y sitio de publicación. Lo anterior permitirá que, ante la caída o pérdida de alguno de estos activos, se puedan recuperar y restablecer con los respaldos con los que se cuenten.
- Se analizará la viabilidad considerando la fecha límite para la captura, instalar en un espacio dentro de las instalaciones del OPLE Veracruz una red local con el sistema para dar continuidad a la operación del sistema.
- Se analizará la viabilidad de contar con un respaldo en la nube de las bases de datos y del sitio de publicación para que la información se encuentre disponible en caso de pérdida de la infraestructura del OPLE Veracruz.
- Se analizará la posibilidad de contar con un servidor en la nube que permite alojar de forma temporal el sistema de captura y verificación para dar continuidad a la operación del sistema.

Procedimiento 8.

I. Amenaza materializada:

A) La base de datos se corrompió.

II. Acto comprometido

Se compromete la información capturada y por lo tanto el sitio de publicación no mostrará información.

III. Tiempo de respuesta esperado

1 hora.

IV. Acción a implementar

- Se cuenta con un programa Oracle VM Manager el cual genera un respaldo del sistema operativo, base de datos y configuraciones. En caso de pérdida o alteración indebida de la información se utilizará el respaldo creado por el programa antes citado.
- Se analizará la viabilidad de tener en todo momento disponible en equipos redundantes tanto los servidores de aplicación, bases de datos y sitio de publicación. Lo anterior permitirá que, ante la caída o pérdida de alguno de estos activos, se puedan recuperar y restablecer con los respaldos con los que se cuenten.

Tabla de amenazas materializadas

Num.	Descripción	Acciones a implementar	Tiempo de respuesta
1	Falla en el servicio de internet de la instancia interna o de la DEPPP por parte del proveedor.	**En primer nivel, la Instancia Interna** solicitará soporte técnico a la UTSI para que revise la conectividad de los equipos destinados a la operación del Sistema. **En segundo nivel, la UTSI** solicitará soporte técnico al proveedor del servicio de internet en dicha área. De persistir la falla, se buscará una sede alterna para realizar la revisión de la información o realizar el proceso de sustitución.	**2 hrs**
2	Combustión espontánea o corto circuito	**En primer nivel, la Instancia Interna o la DEPPP** solicitará soporte técnico a la UTSI para que revise el equipo de cómputo y	**2 hrs**

	de algún elemento que forme parte de algún equipo de cómputo o dispositivo.	determine el grado del daño del equipo y, en su caso, si se puede reparar o es pérdida total. **En segundo nivel,** en caso de no tener reparación el equipo de cómputo dañado, la Instancia Interna o la DEPPP solicitará a la UTSI la instalación de un nuevo equipo de cómputo.	
3	Cortocircuito en la instalación eléctrica que alimenta los equipos instalados en el área de servidores.	Se cuenta con una instalación eléctrica con tierra física apropiada con la correcta polaridad de los contactos para evitar contratiempos relacionados con el suministro eléctrico. Se tienen instaladas dos fuentes de alimentación ininterrumpida (UPS) con regulador integrado, de manera que ante una posible variación en el suministro eléctrico, el equipo de cómputo esté debidamente protegido y pueda continuar su operación. Se cuentan con extintores (basados en CO_2 y polvo químico seco) distribuidos estratégicamente en toda la unidad.	Inmediata, una vez detectado el siniestro.
4	Acceso no permitido al área de servidores.	El acceso a los servidores está bajo llave y solo personal autorizado puede tener acceso. Se cuenta con contraseñas en los servidores y su acceso solo es de forma local además de establecer el bloqueo automático de pantalla en todas las computadoras. Se cuenta con seguridad en la entrada del edificio en dado caso que no se encuentre personal de la UTSI es informado al área correspondiente para verificar el acceso. Monitoreo por video CCTV en el edificio del OPLE Veracruz, teniendo acceso en cualquier momento el personal autorizado tanto a las imágenes en tiempo real, como a las grabaciones.	1 hr.
5	Problemas y exposiciones en aplicación y componentes del sistema, tales como: código	Se cuenta con un programa Oracle VM Manager el cual genera respaldo del sistema operativo, base de datos y configuraciones. En caso de pérdida o alteración indebida de la información se utilizará el respaldo creado por el programa antes citado. Se cuenta con un sistema operativo de uso empresarial basado en Linux el cual brinda alto nivel de seguridad para las aplicaciones, contando con las últimas actualizaciones, mismas que contienen	1 hr

	malicioso en el software, ataques externos para obtención indebida de claves asignadas, ataques externos para obtención o modificación indebida de información.	comprobaciones periódicamente en sus vulnerabilidades y creando parches de seguridad. Se cuenta con un firewall físico con los siguientes servicios: Prevención de intrusos (IPS), antivirus, Filtros DNS, Filtros de correos, firewall de aplicaciones web, control de aplicaciones y control de usuarios. Los servidores donde se almacenen programas y datos, tienen cuentas con diferentes privilegios disponibles en el sistema operativo teniendo en particular restringida la instalación de software o modificación de la información. Protección de seguridad del Framework Laravel contra vulnerabilidades comunes, como el cross-site scripting (XSS) y los ataques de inyección de código. Uso de tokens temporales para verificar la autenticidad de los usuarios. Rutas seguras (Certificado SSL). Contraseñas cifradas.	
6	Fuga de información de claves de usuarios.	Se deberá reportar de manera inmediata a la Instancia Interna y esta a su vez solicitar el apoyo de la UTSI para deshabilitar las cuentas comprometidas y realizar el restablecimiento de las contraseñas. Será responsabilidad de la o el propietario de la cuenta vulnerada la verificación y, en su caso, la solicitud de rectificación de la información que hubiera sido alterada.	30 min. después del reporte de la pérdida de las contraseñas.
7	El sistema informático de captura y validación, así como el sitio de publicación no está disponible.	Se analizará la viabilidad de tener en todo momento disponible en equipos redundantes tanto los servidores de aplicación, bases de datos y sitio de publicación. Lo anterior permitirá que, ante la caída o pérdida de alguno de estos activos, se puedan recuperar y restablecer con los respaldos con los que se cuenten. Se analizará la viabilidad de tener la posibilidad, considerando la fecha límite para la captura, instalar en un espacio dentro de las instalaciones del OPLE Veracruz una red local con el sistema para dar continuidad a la operación del sistema.	2 hrs.

		Se analizará la viabilidad de contar con un respaldo en la nube de las bases de datos y del sitio de publicación para que la información se encuentre disponible en caso de pérdida de la infraestructura del OPLE Veracruz. Se analizará la viabilidad de contar con un servidor en la nube que permite alojar de forma temporal el sistema de captura y verificación para dar continuidad a la operación del sistema.	
8	La base de datos se corrompió.	Se cuenta con un programa Oracle VM Manager el cual genera un respaldo del sistema operativo, base de datos y configuraciones. En caso de pérdida o alteración indebida de la información se utilizará el respaldo creado por el programa antes citado. Se contemplará tener en todo momento disponible en equipos redundantes tanto los servidores de aplicación, bases de datos y sitio de publicación. Lo anterior permitirá que, ante la caída o pérdida de alguno de estos activos, se puedan recuperar y restablecer con los respaldos con los que se cuenten.	1 hr.

Mecanismos de comunicación

Durante la etapa de captura de datos de la información, el capturista del Partido Político, supervisor, sus candidaturas y personas candidatas independientes cuando se presente alguna incidencia derivada de la ejecución del Sistema, esta deberá establecer de manera inmediata la comunicación con el personal de la Instancia Interna, para que esta a su vez pueda estar en condiciones de poder requerir a la UTSI de este Organismo la solución correspondiente a la incidencia presentada.

De igual forma, cualquier situación podrá ser reportada por las representaciones de los Partidos Políticos y en su caso representaciones de candidaturas independientes acreditadas ante el Consejo General.

Los reportes que, en su caso, se generen serán dirigidos al correo electrónico siguiente: incidenciasconoceles@oplever.org.mx de la Instancia Interna, con la finalidad de dejar constancia del reporte realizado.

El reporte enviado por correo electrónico debe contener al menos los siguientes datos: nombre de la persona que reporta, usuario del Sistema que ocupa, descripción de la falla, de ser posibles imágenes gráficas del error (capturas de pantalla) y un número telefónico para contactar a la persona.

Una vez que la incidencia sea reportada y se tenga la posible solución por parte de la UTSI, el personal de la Instancia Interna comunicará a la persona capturista del Partido Político, supervisor, sus candidaturas y personas candidatas independientes que la misma ha sido solventada, para los efectos que haya lugar.

En el caso en que la falla reportada no sea atendida y solucionada por parte de la UTSI, la Instancia Interna dará aviso inmediato al Consejo General a través de su Presidencia para que sea este órgano colegiado quien determine lo conducente.

Conclusión

La continuidad en las operaciones de todo Sistema informático es de vital importancia para el cumplimiento del objetivo para el que fue desarrollado.

Por lo anterior, el seguimiento y aplicación de los procedimientos establecidos en este Plan de Continuidad del Sistema de "Candidatas y Candidatos, Conóceles" permitirá que las y los usuarios del mismo cuenten con mecanismos que garanticen la continuidad operativa en las etapas del Sistema.