

Plan de Continuidad y Seguridad de la Información e Infraestructura

Octubre 2025, Versión 1.0

Unidad de Tecnologías
de la Información y Comunicaciones

Contenido

Glosario	2
Introducción	3
Objetivo	4
Alcance	4
Continuidad de las Operaciones	5
Escenarios	5
Procedimientos de Continuidad	6
Indisponibilidad de los Recursos Humanos	6
Indisponibilidad de Infraestructura Tecnológica	7
Indisponibilidad de Software	10
Indisponibilidad de Servicios	11
Indisponibilidad de Instalaciones	12
Activación del plan de continuidad	12
Identificación de la contingencia	13
Recuperación y reanudación de operaciones	14
Seguridad de la información e infraestructura	17
Recursos Humanos	18
Infraestructura Tecnológica	19
Software e información	19
Servicios	20
Instalaciones del Instituto	21
Pruebas al Plan de Continuidad y Seguridad de la Información e Infraestructura	21

Glosario

Activo crítico	Recurso, sistema o información cuya interrupción o destrucción causaría un daño grave a la operación del Instituto.
ADSL	Acrónimo en inglés de Asymmetric Digital Subscriber Line, es un tipo de tecnología de línea telefónica para transmitir Voz y Datos.
Contingencia	Situación de riesgo o un suceso inesperado que puede interrumpir el funcionamiento normal de los sistemas informáticos.
DDR	Dispositivo que graba video en formato digital, normalmente usando un disco duro.
EDR	"Endpoint Detection and Response" (Detección y respuesta de puntos de conexión) y es una tecnología de ciberseguridad que protege los dispositivos (endpoints) como computadoras, teléfonos y servidores de amenazas.
IEEH / Instituto	Instituto Estatal Electoral de Hidalgo.
Incidencia	Evento inesperado que interrumpe o degrada el funcionamiento normal de un sistema, red o servicio, afectando la productividad.
Riesgo	Amenaza o vulnerabilidad que puede comprometer la seguridad de los sistemas y datos digitales, desde errores humanos hasta ataques de ciberdelincuentes y desastres naturales.
Seguridad de la información	Prácticas y herramientas para proteger la confidencialidad, integridad y disponibilidad de la información, tanto en formatos digitales como físicos
Site	Espacio físico donde se alojan equipos informáticos y de telecomunicaciones.
UPS	Uninterruptable Power Supply, Sistema de Alimentación Ininterrumpida, es un dispositivo permite tener flujo de energía eléctrica mediante baterías, cuando el suministro eléctrico falla.
UTIC	Unidad de Tecnologías de la Información y Comunicaciones.
XDR	Plataforma unificada de ciberseguridad que integra y correlaciona datos de múltiples fuentes, como endpoints, redes, correo electrónico y la nube, para detectar amenazas de manera más efectiva.

Introducción

El presente Plan de Continuidad y Seguridad de la Información e Infraestructura se ha desarrollado como consecuencia del Análisis de Riesgos de Seguridad de la Información en Infraestructura Tecnológica, del Instituto Estatal Electoral de Hidalgo. Incorpora los métodos y acciones para garantizar el cumplimiento de los aspectos normativos y regulatorios.

Los daños provocados por fenómenos naturales y, de lo organizacional y social (parte de errores o conducta humana premeditada), que derivan en desastres o situaciones de crisis representan un factor de desaceleración para la actividad y los objetivos del Instituto, ello implica altos costos socioeconómicos y de presencia a consecuencia de una abrupta interrupción de operaciones en las distintas áreas.

Actividades como garantizar la instalación y mantenimiento de software de forma segura, poco tienen que ver con las actividades de capacitación; sin embargo, todas ellas se enmarcan en un mismo marco de la ciberseguridad.

En este contexto, el Plan de Continuidad y de Seguridad de la información e Infraestructura del Instituto Estatal Electoral del Hidalgo actúa como orientación y soporte, es capaz de dar coherencia a todas las actividades relacionadas con la continuidad de las operaciones del Instituto ante contingencias y la protección de activos críticos ante ataques de físicos y de ciberseguridad; con la perspectiva de prevención de incidentes o su mitigación, que es esencial, para evitar los enormes costes económicos, a menudo vinculados a las contingencias y ataques. En este sentido, este Plan representa una inversión estratégica para ahorrar costos y prevenir problemas de presentación del Instituto.

Este plan deberá ser comunicado al personal involucrado en su ejecución y formar parte de la estrategia de capacitación, a fin de garantizar su cumplimiento.

Objetivo

Establecer las acciones necesarias para garantizar el restablecimiento de las operaciones críticas del Instituto Estatal Electoral de Hidalgo ante la ocurrencia de una contingencia, asegurando la integridad, confidencialidad y disponibilidad de la información institucional, así como la operatividad continua de los sistemas y la infraestructura tecnológica que pudieran verse afectadas.

Alcance

- Este documento está dirigido a todo el personal con acceso a las Tecnologías de la Información y Comunicaciones del IEEH, ya sea por la responsabilidad que tienen asignada con relación a los bienes informáticos o por los beneficios que de ellos obtienen.
- Garantizar la confidencialidad, integridad y disponibilidad de la información electrónica o digital sensible del Instituto.
- Sentar las bases para la recuperación en caso de compromiso en la operación.
- Asegurar la disponibilidad de sistemas frente a ataques de denegación de servicio u otros fallos.
- Proteger la infraestructura de Tecnologías de la Información y Comunicaciones.
- Controlar y verificar identidades para los usuarios en los accesos a recursos informáticos del Instituto.
- Garantizar el cumplimiento de las Políticas y Lineamientos de Gestión de Sistemas de Información y Comunicaciones.
- Implementar planes de concientización y capacitación al personal sobre las Políticas y Lineamientos de Gestión de Sistemas de Información y Comunicaciones, fomentando una cultura de ciberseguridad.
- Preservar la reputación del Instituto y garantizar la continuidad de operación incluso tras sufrir un incidente de ciberseguridad.

Es así que, el presente plan está dividido en dos partes: la continuidad de las operaciones ante contingencias y la seguridad de la información e infraestructura.

Continuidad de las Operaciones

El Plan de Continuidad es la guía estratégica que asegura que el Instituto pueda seguir operando sus funciones críticas durante y después de una interrupción, utilizando protocolos para la respuesta a emergencias y la protección de activos.

Escenarios

Situación o Evento	Escenarios				
	Recursos Humanos	Infraestructura tecnológica	Software	Servicios	Indisponibilidad de instalaciones
Enfermedades infecciosas	✓				
Indisponibilidad de los recursos humanos	✓				
Fallas o incapacidad en la infraestructura (Infraestructura tecnológica o Telecomunicaciones)		✓	✓	✓	
Interrupciones de energía eléctrica		✓		✓	
Ataques cibernéticos		✓	✓	✓	
Toma de instalaciones por grupos.		✓		✓	✓
Factores ambientales y Desastres naturales	✓	✓		✓	✓

De acuerdo con la clasificación y calificación de los Activos Críticos y de los riesgos identificados en el “Análisis de Riesgos de Seguridad de la Información en Infraestructura Tecnológica”, se generan los siguientes procedimientos para aplicarse en caso de presentarse alguna incidencia o contingencia:

Procedimientos de Continuidad

Con el objetivo de conocer las actividades a realizar en caso de que se presente algún evento que altere en la operación de las actividades del Instituto, se establecen estrategias y acciones documentadas a implementar para asegurar la operación de funciones y la recuperación de procesos después de una interrupción o desastre.

De los riesgos identificados, se generan los procedimientos de continuidad que implican identificar los riesgos, evaluar su impacto en el Instituto, establecer mecanismos de respuesta y recuperación; definiendo los recursos y responsabilidades necesarios para mantener la continuidad de las operaciones y la confianza del personal. Estos, están basados en las Políticas y Lineamientos de Gestión de Sistemas de Información y Comunicaciones, en caso de que se presente alguna incidencia o evento.

Indisponibilidad de los Recursos Humanos

Procedimiento específico	Aplica a:	Tratamiento
Continuidad de Recursos Humanos	Consejerías Electorales	Mitigar
	Dirección Ejecutiva	Mitigar
	Subdirección de área	Mitigar
	Jefatura de Departamento	Mitigar
	Personal Operativo	Mitigar
	Personal Técnico	Mitigar

Procedimiento específico Continuidad de Recursos Humanos

La estrategia para la continuidad de Recursos Humanos se basa en la mitigación por la sustitución del personal indispuerto por otro que tenga el mismo conocimiento o habilidades para la ejecución de procesos de información digital u operación técnica afectados. Implica que cada proceso tenga una persona responsable y, por lo menos, una persona suplente.

Consejería Electoral. - Si bien las personas integrantes de los órganos de decisión del Instituto, como el Consejo General y los Consejos Distritales Electorales, desempeñan funciones fundamentales en la organización, desarrollo y fiscalización de los procesos electorales locales, así como en la supervisión institucional y la garantía de los principios rectores del IEEH, su

ausencia no representa un riesgo directo para la continuidad de los servicios tecnológicos. Esto se debe a que sus atribuciones están orientadas principalmente a la toma de decisiones, emisión de acuerdos y validación de resultados, sin intervenir en la operación técnica o administrativa de los sistemas informáticos, redes, infraestructura o servicios digitales que sustentan la actividad tecnológica del Instituto.

Dirección Ejecutiva o Titular de área. – Es el responsable de los procedimientos y actividades en el área, por lo que en caso de presentarse alguna contingencia implementará las medidas pertinentes para su atención inmediata. En caso de indisponibilidad de alguna persona que labora en el área, en conjunto con el personal de la misma, realizará el plan para los ajustes de personal requeridos. En caso de que se deba ausentar de sus funciones, la subdirección o Jefatura de Departamento, previamente capacitados para ello, lo suplirán de las mismas.

Subdirección o Jefatura de Departamento. – En caso de indisponibilidad para ejercer sus funciones, otra subdirección o jefatura de departamento o personal operativo disponible suplirá esta eventualidad.

Personal operativo. - En caso de indisponibilidad para ejercer sus funciones, otra persona operativa disponible o su jefe(a) inmediato deberá suplir sus funciones.

Personal Técnico. – Personal especializado en la supervisión y operación de la infraestructura del Instituto. En caso de indisponibilidad para ejercer sus funciones, otra persona técnica disponible deberá suplir sus funciones.

Indisponibilidad de Infraestructura Tecnológica

Procedimiento específico	Aplica a:	Tratamiento
Continuidad de equipamiento	Computadoras Personales	Mitigar
	Ruteadores	Transferir
	Switches	Mitigar
	Telefonía análoga	Mitigar / transferir
	Telefonía IP	Mitigar / Transferir
	Videovigilancia	Mitigar
	Equipo satelital	Mitigar
	Servidores	Transferir

Procedimiento específico	Aplica a:	Tratamiento
	Escáneres	Mitigar
	Impresoras	Mitigar
	UPS	Mitigar
	Reguladores	Mitigar
	Planta de energía	Mitigar
	Red cableada	Mitigar

Procedimiento específico Continuidad de Infraestructura Tecnológica

Computadoras personales. - Si se detectan fallas en una computadora, la persona responsable del equipo deberá realizar el proceso de levantar una solicitud mediante el Sistema de Gestión de Servicios (SGS), para su revisión. En caso de que el equipo no tenga una solución pronta, se deberá sustituir el equipo temporal para continuar con la operación.

Ruteadores. - En caso de falla, se deberá levantar una incidencia mediante el Sistema de Gestión de Servicios (SGS), y el técnico responsable del equipo deberá comunicarse con el proveedor para su atención inmediata.

Switches. - En caso de detección de falla, se deberá mitigar la incidencia al sustituir por un equipo de respaldo.

Telefónica IP. - En caso de presentarse falla en el equipo o interrupción en el servicio, la persona responsable del equipo telefónico deberá realizar el proceso de levantar una solicitud mediante el Sistema de Gestión de Servicios (SGS), para su atención. Personal técnico determinará si la falla radica en la infraestructura tecnológica del Instituto o externa. En caso de ser externa deberá comunicarse con el proveedor para que sea atendida por este, por el contrario, si se trata de infraestructura de cableado, se deberá atender con forme al procedimiento aplicable.

Telefónica analógica. - En caso de presentarse falla en el equipo o interrupción en el servicio, la persona responsable del equipo telefónico deberá realizar el proceso de levantar una solicitud mediante el Sistema de Gestión de Servicios (SGS), para su atención. Personal técnico determinará si la falla radica en la infraestructura tecnológica del Instituto o externa. En caso de ser externa deberá comunicarse con el proveedor para que sea atendida por este, por el contrario, si se trata de infraestructura de cableado, se deberá atender con forme al procedimiento aplicable.

Videovigilancia. - Aunque el equipo de videovigilancia no interviene directamente en la operación tecnológica, su funcionamiento es esencial para proteger la infraestructura crítica del Instituto. Permite detectar accesos no autorizados y prevenir incidentes que podrían comprometer la continuidad operativa, por lo que su riesgo debe ser mitigado mediante mantenimiento, respaldo energético y monitoreo constante.

Equipo Satelital. - El equipo se emplea en caso de no contar con infraestructura de comunicaciones para Enlace ADSL. En caso de falla en la señal Satelital se contará como medio de respaldo con Banda Ancha Móvil.

Servidores. - Esto deberán tener unidades de almacenamiento redundantes o respaldo en otros servidores, fuentes de energía de respaldo. Para los datos críticos del Instituto se recomienda tener Servidores en la Nube para el procesamiento, comunicación y almacenamiento de información. En caso de fallo, se deberá restablecer de manera inmediata.

Escáneres. - Si se detecta fallas en un equipo, el usuario responsable del equipo deberá realizar el proceso de levantar una solicitud mediante el Sistema de Gestión de Servicios (SGS), para su revisión. En caso de que el equipo no tenga una solución pronta, se deberá sustituir el equipo para continuar con la operación.

Impresoras. - Si se detecta fallas en un equipo, la persona responsable del equipo deberá realizar el proceso de levantar una solicitud mediante el Sistema de Gestión de Servicios (SGS), para su revisión. En caso de que el equipo no tenga una solución pronta, se deberá sustituir el equipo para continuar con la operación.

UPS. - Si se detecta fallas en un equipo, la persona responsable del equipo deberá realizar el proceso de levantar una solicitud mediante el Sistema de Gestión de Servicios (SGS), para su revisión. En caso de que el equipo no tenga una solución pronta, se deberá sustituir el equipo para continuar con la operación.

Reguladores. - Si se detecta fallas en un equipo, la persona responsable del equipo deberá realizar el proceso de levantar una solicitud mediante el Sistema de Gestión de Servicios (SGS), para su revisión. En caso de que el equipo no tenga una solución pronta, se deberá sustituir el equipo para continuar con la operación.

Planta de energía. - Equipo que provee respaldo de energía eléctrica en caso de que la energía pública falte. Deberá ser rehabilitado a la brevedad o ser sustituida por otro equipo de energía auxiliar.

Red Cableada. – En caso de presentarse falla por conexión la persona responsable del equipo deberá realizar el proceso de levantar una solicitud mediante el Sistema de Gestión de Servicios (SGS), para su revisión. Al verificarse que la falla procede de la Red cableada; deberá ser corregido o sustituido el cable, en su totalidad donde se encuentra la falla.

Indisponibilidad de Software

Procedimiento específico	Aplica a:	Tratamiento
Continuidad de Software	Sistemas operativos	Mitigar
	De productividad	Mitigar
	Desarrollo del propio Instituto	Mitigar
	Gestión de tareas	Mitigar
	Uso en línea	Mitigar
	Almacenamiento de archivos	Mitigar
	De bases de datos	Mitigar
	Sitios de internet	Mitigar
	Correos electrónicos	Mitigar
	Videoconferencia	Mitigar

Procedimiento específico Continuidad de Software

La estrategia para la continuidad de software se basa la mitigación en la reinstalación del sistema o aplicación afectada, la cual incluye:

- Reinstalación del software afectado.
- Configuración.
- Restauración de los datos o información de acuerdo con el último corte de respaldo del sistema afectado.
- Realizar pruebas de funcionalidad.
- Comunicar a las áreas afectadas de la reanudación dl servicio.

En el caso de que se encuentren defectos en el Software, se deberá tener comunicación con el fabricante a fin de reportar la falla y solicitar su corrección. Si el Software fue desarrollado por el propio Instituto se notificará a la UTIC y esa deberá hacer la corrección de la falla o defecto de manera inmediata.

Indisponibilidad de Servicios

Procedimiento específico	Aplica a:	Tratamiento
Continuidad de Servicios	Líneas Telefónicas	Transferir
	Servicios de Internet	Transferir
	Energía eléctrica	Transferir
	Servidores	Transferir

Procedimiento específico Continuidad de Servicios

La estrategia para la continuidad de Servicio se encuentra basada en la transferencia del riesgo o contingencia. Implica que para cada Servicio se tendrá a un proveedor, el cual deberá dar atención conforme a los términos del contrato.

Líneas Telefónicas. – En caso de fallo en líneas telefónicas, se llamará al proveedor para que este atienda la incidencia de forma inmediata.

Servicios de Internet. – En caso de fallo del servicio de Internet, se llamará al proveedor para que este atienda la incidencia de forma inmediata. También se podrá hacer uso del servicio redundante con un proveedor de respaldo diferente.

Energía eléctrica. - En caso de fallo en energía eléctrica, se activará la planta de energía auxiliar, adicionalmente se llamará al proveedor para que este atienda la incidencia de forma inmediata.

Servidores. - En caso de fallo en servidores arrendados, se llamará al proveedor para que este atienda la incidencia en los plazos establecidos.

Indisponibilidad de Instalaciones

Las contingencias que pueden presentarse en este apartado consisten en la toma de instalaciones del Instituto por parte de grupos activistas, vandalismo, incendios o por contingencias ambientales como terremotos, tormentas o inundaciones, por lo que en caso de presentarse se deberá evaluar la situación y, de ser el caso, hacer la declaratoria de emergencia.

Procedimiento específico	Aplica a:	Tratamiento
Continuidad de instalaciones	Instalaciones del IEEH	Mitigar
	Instalaciones alternas del IEEH	Mitigar

Procedimiento específico Continuidad de instalaciones

Instalaciones del IEEH. – En caso de toma de instalaciones o vandalismo se deberá esperar (aceptar) a que los grupos o personas abandonen las instalaciones, en tanto se podrán llevar las actividades de manera remota. Una vez recuperadas las instalaciones se llevará un diagnóstico de los daños a la infraestructura tecnológica y se actuará de acuerdo con el plan de continuidad de la misma. En caso de que fuera por contingencias ambientales se deberá realizar las actividades desde las casas del personal, en tanto persista la contingencia, posteriormente se llevará el diagnóstico de los daños y, si los daños fueron severos, se deberá considerar la ocupación de sedes o instalaciones alternas temporales para las actividades críticas, así como el continuar realizando las operaciones remotamente hasta el restablecimiento de la infraestructura tecnológica y Servicios para las operaciones en las instalaciones afectadas.

Activación del plan de continuidad

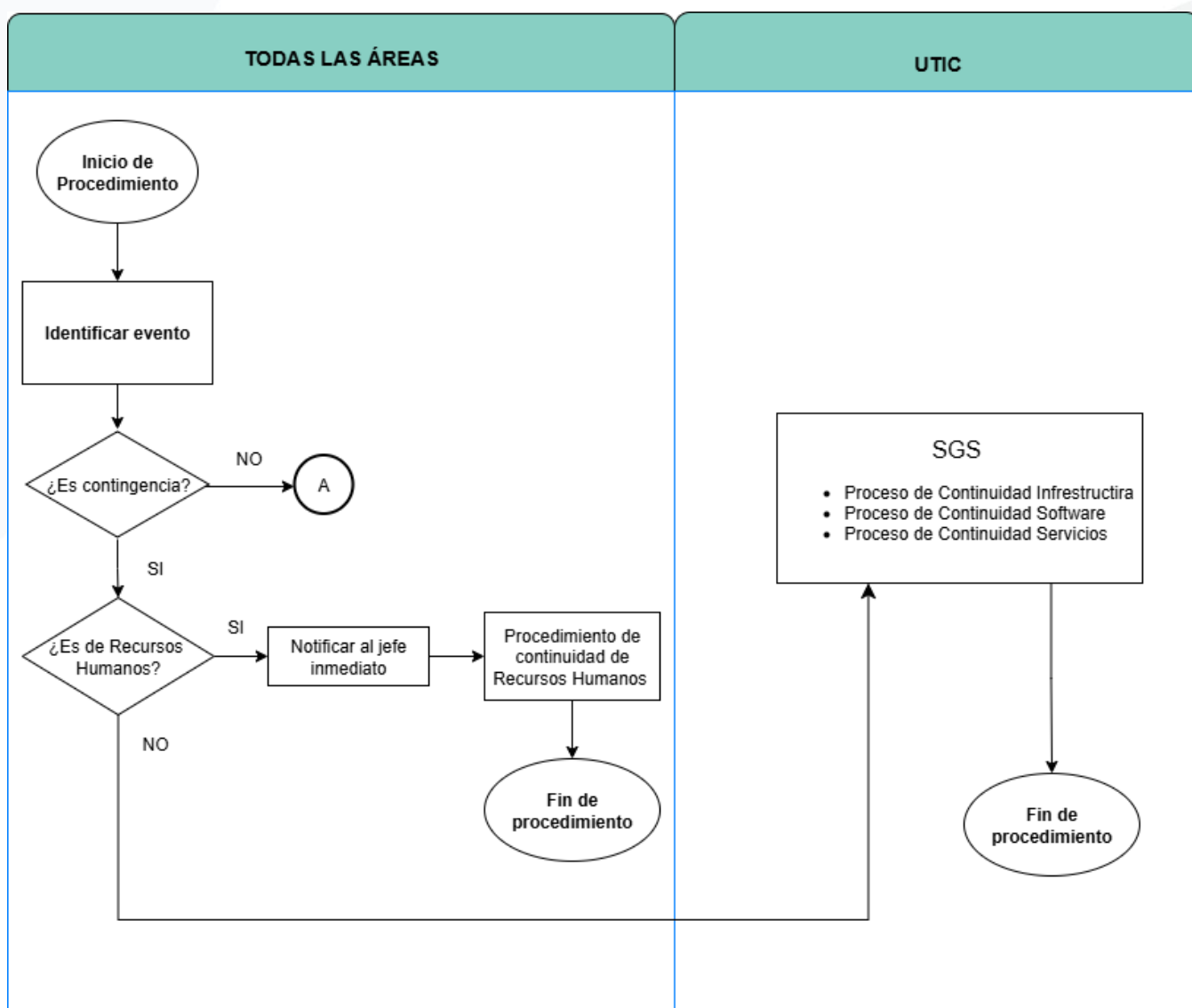
Una vez identificado el riesgo y el procedimiento específico por utilizar, es importante conocer los tiempos promedios de respuesta una vez que se ha notificado la contingencia.

Dicha información se muestra en la tabla siguiente de acuerdo con el nivel e impacto del evento:

Nivel de Impacto	Recursos Humanos	Infraestructura Tecnológica	Software	Servicios
ALTO	N/A	2 horas	2 horas	1 hora
MEDIO	30 min.	4 horas	4 horas	2 horas
BAJO	1 hora	6 horas	6 horas	4 horas

* Estos tiempos están estimados con base a los tiempos de atención de incidentes presentados en el Instituto.

Identificación de la contingencia

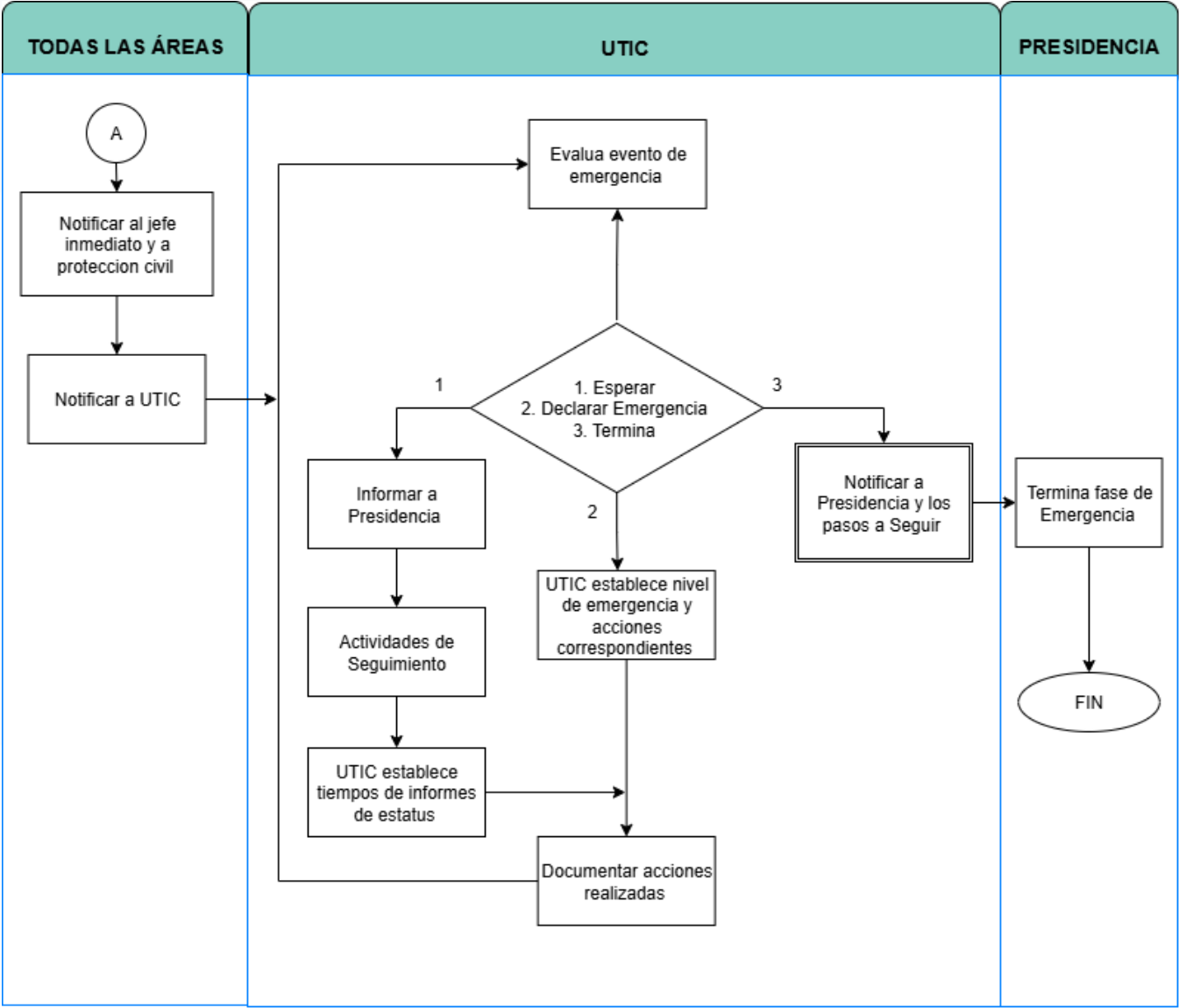


RESPONSABLE	ACTIVIDAD	ÁREAS PARTICIPANTES
Cualquier persona del IEEH	1. Identifica el evento que puede obstaculizar la operación. 2. Distingue que el evento sea una contingencia o una emergencia. 2.1. Un evento de contingencia se caracteriza por la falta de personal, falla en equipo tecnológico, software o servicios tecnológicos. 2.2. Un evento de emergencia se caracteriza por incendios, humo, amenazas de bombas, inundaciones, sismo, bloqueo o toma de instalaciones.	Todas las áreas del IEEH
Cualquier persona del IEEH	3. De ser el caso 2.1, la persona debe identificar que el evento sea de falta de personal de su área; de ser así, debe notificar a su jefe(a) inmediato superior. 4. El jefe(a) inmediato debe activar el “Procedimiento específico Continuidad de Recursos Humanos”. 5. Termina el procedimiento	Área afectada
Cualquier persona del IEEH	6. De ser el caso 2.1 por falla de equipo tecnológico, software o servicios tecnológicos, la persona debe levantar un reporte por medio del Sistema de Gestión de Servicios (SGS).	Área afectada
Personal Técnico	7. La UTIC asigna a personal técnico para resolver el reporte. 8. Termina el procedimiento	UTIC
Cualquier persona del IEEH	9. De ser el caso 2.2, la persona debe referirse al proceso de específico de eventos de emergencia.	Todas las áreas del IEEH

Recuperación y reanudación de operaciones

Seguimiento de solicitudes por SGS. - La UTIC designará a personal técnico para dar seguimiento a la solicitud del SGS, de acuerdo con los Procedimientos Específicos de Continuidad de Infraestructura Tecnológica, Continuidad de Software y Continuidad de Servicios.

Evaluación de emergencia. – El Titular de la UTIC deberá realizar el procedimiento de identificación descrito anteriormente, para evaluar la contingencia. El cual, se llevará a cabo la evaluación del evento y su nivel de impacto en las operaciones del Instituto. De ser declarada la contingencia como una emergencia, informará inmediatamente a la Presidencia del IEEH; además, se activarán los planes de continuidad establecidos para los activos del Instituto.



RESPONSABLE	ACTIVIDAD	ÁREAS PARTICIPANTES
Cualquier persona del IEEH	10. Notifica al jefe inmediato y/o a protección civil.	Todas las áreas del IEEH
Jefe(a) inmediato y/o a protección civil	11. Notifica a la UTIC.	Todas las áreas del IEEH
Titular de la UTIC	12. Evalúa el evento de emergencia y los hechos relevantes del evento, considerando como mínimo: <ul style="list-style-type: none"> • Descripción del evento. • Activos afectados. • Estimación de la duración del evento. • Posibles soluciones. 	UTIC / Protección civil
Titular de la UTIC	13. Decide entre esperar, declarar emergencia o terminar el evento. 13.1. Si es esperar, todavía no se determina si la infraestructura tecnológica o los servicios se verán afectadas por el evento. 13.2. Si es declarar emergencia - Es claro que el evento impacta directamente a la operación del Instituto y es necesario establecer el nivel de afectación. 13.3. Si es terminar - El evento de emergencia ha terminado y el IEEH tiene la capacidad de operar normalmente.	UTIC
Titular de la UTIC	14. De ser el caso 13.1, Notifica a la Presidencia respecto al evento identificado, así como los pasos a seguir.	UTIC / Presidencia
Titular de la UTIC	15. Asigna actividades de seguimiento para monitorear el evento al Personal Técnico.	UTIC
Personal Técnico	16. Establece el tiempo para el siguiente informe del estatus del evento. (Se recomienda de ser posible sea cada 30 minutos, la ejecución del paso 2 - Evaluar el evento de emergencia y los hechos relevantes del evento).	UTIC
Titular de la UTIC	17. Se documentan las actividades realizadas y realiza la actividad 12 nuevamente.	UTIC
Titular de la UTIC	18. Establece el nivel de la emergencia que se va a declarar: Nivel 1: <ul style="list-style-type: none"> • Se mantienen las operaciones en las instalaciones afectadas • Se monitorea el impacto 	UTIC

RESPONSABLE	ACTIVIDAD	ÁREAS PARTICIPANTES
	<ul style="list-style-type: none"> Se identifican los posibles pasos a seguir Se preparan para una posible contingencia Nivel 2 <p>Nivel 2: Se da aviso de que se ha presentado un evento de emergencia y se mantendrá la continuidad de acuerdo al procedimiento específico Continuidad de instalaciones, en tanto se procede con la restauración de instalaciones, infraestructura tecnológica y servicios para la reanudación de operaciones.</p>	
Titular de la UTIC	19. Se documentan las actividades realizadas y realiza la actividad 12 nuevamente.	UTIC
Titular de la UTIC	<p>20. En caso de terminar, realiza la evaluación la disposición de la infraestructura tecnológica y los Servicios para verificar la capacidad de operar normalmente.</p> <ul style="list-style-type: none"> Servicios en las instalaciones Energía eléctrica Líneas telefónicas. Acceso a la nube (Internet) Personal suficiente para operar normalmente. <p>21. Notifica a la Presidencia respecto al evento de emergencia.</p>	UTIC
Persona que preside	22. Termina la fase de emergencia	Presidencia
	23. Fin del procedimiento.	

Seguridad de la información e infraestructura

Las siguientes medidas de seguridad se enfocan en proteger los activos de información y la infraestructura tecnológica que son vitales para el Instituto, mediante medidas preventivas para controlar los riesgos identificados y garantizar la seguridad de los Activos y la continuidad en las operaciones del Instituto.

Recursos Humanos

- La UTIC deberá realizar un catálogo de puestos del Instituto con la finalidad de establecer de forma predeterminada la asignación y acceso a infraestructura tecnológica del Instituto que incluirá:
 - Nombre completo
 - Puesto
 - Área de adscripción
 - Tipo de contratación (permanente o temporal)
 - Lista de equipos de cómputo que utilizará
 - Lista de servicios informáticos que utilizará
 - Acceso y niveles para aplicaciones que utilizará
- Los Contratos del personal deberán incluir cláusulas de confidencialidad de información y señalar la responsabilidad sobre el manejo de información e infraestructura tecnológica.
- El departamento de Recursos Humanos será el responsable de notificar a la UTIC del personal de nuevo ingreso o de su reasignación, señalando: nombre completo, área de adscripción, puesto, tipo de contratación (de ser temporal, señalar el periodo de contratación) y localización física para laborar.
- La Dirección Ejecutiva de Administración a través del departamento de Recursos Humanos será responsable de notificar a la UTIC sobre el personal que deje de laborar para el Instituto, con la finalidad de proceder con la baja de la cuenta institucional de acuerdo con la normativa establecida. Una vez que deje su puesto de trabajo, la persona tendrá acceso a su correo y drive hasta el momento de efectuar el procedimiento de entrega-recepción.
- La UTIC elaborará y mantendrá una base de datos de los usuarios activos en el Instituto.
- El personal que requiera equipo de cómputo (computadora, laptop, impresora, escáner, UPS, u otro) se le asignará bajo resguardo y responsabilidad directa de su buen uso y manejo.
- Personal que deba tener acceso a infraestructura tecnológica; la UTIC proporcionará un correo institucional y, dependiendo de sus funciones, un drive en la nube para resguardo de información.
- Los usuarios y contraseñas proporcionadas para el uso de infraestructura tecnológica son de uso personal e intransferible.
- La persona titular del área administrativa deberá tener disponible al personal de su área la información de uso común en un repositorio en la nube.
- Se deberán capacitar por lo menos a dos personas para cada función o perfil de trabajo.

Infraestructura Tecnológica

- Contar con UPS para computadoras personales de escritorio. No deberán conectarse a este equipo impresoras, escáneres, ventiladores, cafeteras y equipo de proyección, o cualquier otro que por sus características hagan un alto consumo de energía eléctrica.
- Tener una planta de energía auxiliar para las instalaciones del Instituto.
- El personal deberá identificarse para tener acceso a la infraestructura tecnológica. Esto implica contraseñas de acceso a equipo de cómputo asignado y servicios en la nube.
- Las computadoras personales y laptop del personal deberán tener bloqueos automáticos después de 5 minutos como máximo.
- Se deberá incluir en los inventarios de infraestructura tecnológica, ciclos de vida; a fin de hacer la planeación correcta para su sustitución o actualización.
- Antes de renovar infraestructura tecnológica, se deberá realizar un estudio para investigar nuevas tecnologías con el fin de actualizar los procesos del Instituto.
- La UTIC será la responsable de proporcionar la capacitación acerca del manejo de equipo de cómputo y Seguridad.

Software e información

- Llevar a cabo el Mantenimiento y Actualización de Sistemas Operativos, navegadores web y aplicaciones de oficina a fin de proteger contra vulnerabilidades.
- Respaldo de aplicaciones desarrolladas por el Instituto.
- Las unidades administrativas deberán tener una base de datos de usuarios y contraseñas de Administrador de las aplicaciones que sean responsables.
- Instalación de EDR y XDR
- Tener firewall instalado.
- Limitar la ejecución de software procedente de Internet o de medios extraíbles como son memorias USB.
- Procedimientos de identificación, autenticación para acceder a software desarrollado por el Instituto a personal del Instituto.
- Utilizar contraseñas de alta seguridad para evitar ataques de directorio.
- Se llevará un inventario de licencias de software con la finalidad de tener control para la renovación de estas.
- El personal deberá guardar la información importante que genera o procesa, en medios de almacenamiento externos o en la nube, mediante réplicas o copias de respaldo; así como proporcionar la persona titular del área la información crítica para su adecuado resguardo.
- El envío de información reservada deberá viajar por la nube de forma encriptada (archivos de texto, hojas de cálculo, digitalizaciones, etc).
- Los correos electrónicos que envía el personal del Instituto deberán tener leyendas de confidencialidad de información.

- Se tendrá un procedimiento de replicación de datos y copias de seguridad encriptadas información relevante como documentos, contabilidad digital, archivos, expedientes, digitalizaciones, comunicados, seguimientos a temas y bases de datos de aplicaciones en drives de la nube del instituto; observando los tiempos establecidos para el resguardo y disponibilidad de información.
- Antes de renovar licencias de software, se deberá hacer un estudio para investigar las nuevas tecnologías de aplicaciones y su compatibilidad con las que se encuentren en uso.
- Las unidades administrativas serán las responsables de proporcionar la capacitación del manejo y respaldo de información que esté a su cargo; en casos de nuevo ingreso de personal, reasignación de puestos de trabajo o actualización de las Aplicaciones Informáticas.
- La UTIC será la responsable de proporcionar la capacitación del manejo y respaldo de información de aplicaciones informáticas de uso general en casos de nuevo ingreso de personal, reasignación de puestos de trabajo o actualización de las Aplicaciones Informáticas.

Servicios

- El contrato con la empresa proveedora del servicio de energía eléctrica deberá contemplar la atención inmediata en el caso de una interrupción eléctrica.
- Celebrar instrumentos jurídicos que incluyan cláusulas de confidencialidad y de atención inmediata con las empresas proveedoras de Servicios de Internet, hospedaje de páginas, dominios, servidores en la nube, etc.; a fin de, resguardar la información y en el caso de una interrupción del servicio, esta sea atendida inmediatamente.
- Contar por lo menos con dos proveedores de Internet a fin de contar con un respaldo del servicio.
- Contratar servicios de servidores para respaldo de datos y resguardo de aplicaciones y aplicaciones en línea.
- Para la adquisición de equipo de cómputo (PC, laptop, impresoras, escáneres, UPS, etc.) deberán incluirse pólizas de garantía de 3 años, por lo menos. La atención deberá ser “en sitio” de las instalaciones del Instituto.
- Llevar control o calendario de pagos de servicios a proveedores de servicio, con la finalidad de evitar cortes de servicios.

Instalaciones del Instituto

- El área crítica del Site de comunicaciones deberá contar con equipo de emergencia: teléfono con acceso a otras áreas administra y llamadas al exterior, detectores de humo, extintor especializado en equipo electrónico, luces de emergencia y otras medidas que apliquen.
- El área del Site deberán contar con equipo de aire acondicionado independiente.
- Toda persona deberá identificarse para tener acceso a las instalaciones del Instituto y portar el gafete de identificación correspondiente en todo momento.
- Accesos a áreas de Site, servidores, racks de derivación y DDR serán de uso restringido y de acceso solo a personal técnico de la UTIC.
- El acceso a personal de proveedores a áreas restringidas deberá ser autorizado previamente por el Titular de la UTIC y estar acompañados por personal de la UTIC en todo momento.
- Personas externas al Instituto deberán estar acompañas en todo momento por personal del IEEH en las Instalaciones del mismo.
- Se vigilarán las áreas críticas y administrativas con cámaras de videovigilancia.

Las fallas de seguridad que resulten en el desarrollo de la operación del Instituto deberán analizarse de manera proactiva a fin de detectar su origen e incorporar su tratamiento a este Plan.

Pruebas al Plan de Continuidad y Seguridad de la Información e Infraestructura

Las pruebas se llevarán a través de un simulacro, estos deberán ser diseñados por la UTIC. Para su implementación deberán ser acordados y aprobados por la Presidencia o, en su caso, por la CPTIC. Esto simulacros deberán involucrar al menos evento en los escenarios identificados e incluir al menos una unidad administrativa del Instituto.