PLAN DE CONTINGENCIA EN MATERIA DE TIC´s APLICABLE A LAS OFICINAS DE LA AGENCIA DE PROYECTOS ESTRATÉGICOS DEL ESTADO DE QUINTANA ROO.

-ACCIONES INTERNAS-

Versión: 2.0: _____

Fecha de aprobación: _____

OBJETIVO

El objetivo del plan de contingencia en Tecnologías de la Información y las Comunicaciones (TIC) es garantizar la continuidad operativa de los servicios y procesos institucionales ante incidentes que afecten la infraestructura tecnológica, tales como fallas de sistemas, ciberataques, desastres naturales o errores humanos. Asimismo, busca proteger la información, minimizar tiempos de interrupción y reducir el impacto operativo y económico de la Agencia.

ALCANCES

El plan de contingencia en TIC abarca la identificación de riesgos tecnológicos, la definición de procedimientos de respuesta ante incidentes, la asignación de responsabilidades y la implementación de medidas preventivas y correctivas. Incluye la protección de sistemas informáticos, redes de comunicación, bases de datos, equipos tecnológicos y servicios digitales críticos. Además, contempla mecanismos de respaldo y recuperación de información, pruebas periódicas del plan, capacitación del personal.

Para lograr mejores resultados, el presente plan es aplicable a todos los usuarios que hagan uso de equipos de cómputo y a los *administradores de la infraestructura de telecomunicaciones propiedad de la Agencia de Proyectos Estratégicos del Estado de Quintana Roo para el cumplimiento de sus funciones, de acuerdo a lo siguiente:

VARIACIONES EN EL SUMINISTRO DE ENERGÍA ELÉCTRICA

-Acciones preventivas-

- Contar con un No-break (Equipo de protección con inclusión de baterías dentro de su mecanismo) con capacidades necesarias (60% superiores) para cada uno de los equipos de cómputo de la Agencia.
- Conocer el procedimiento para reportar fallas en el suministro de energía eléctrica
- Conocer el funcionamiento de los UPS y No-Break.
- Conocer el procedimiento para reportar detección de un mal funcionamiento en los UPS y No-break.
- Conocer los procedimientos para reportar problemas de los servicios de telecomunicación.
- Solicitar revisión periódica (mensualmente) del estado y óptimo funcionamiento de los No-Break.
- Realizar respaldos de la información almacenada en los equipos de cómputo.
- Contar con medios o unidades externas de almacenamiento para realizar respaldos de información.

-Acciones durante fallos en suministro de energía eléctrica-

- Reportarlo a sus superiores y al área responsable del mantenimiento de la instalación eléctrica de la Agencia.
- Apagar y desconectar el No-break al primer indicio de variación de voltaje.
- Si el equipo de cómputo o el No-break se apagan ante una variación de voltaje, no volver a encenderlos y reportarlo a la Unidad de Tecnologías.
- Esperar a que personal de la Unidad de Tecnologías revise los equipos que han sido reportados para que emitan un dictamen en caso de ser necesario.
- Esperar a que personal del área responsable del mantenimiento de la instalación eléctrica de la Agencia emita un reporte o comunicado sobre los fallos en el suministro de la energía eléctrica.
- Encender los equipos hasta que el suministro de energía eléctrica se regularice.
- *Realizar recorridos en las áreas para verificar que se hayan apagado y desconectado los equipos de forma adecuada.

-Acciones posterior al restablecimiento del suministro de la energía eléctrica-

- Encender los equipos (Computadoras, no-break, ups, impresoras, teléfonos, etc.)
- En caso de identificar algún mal funcionamiento en los equipos y/o sistemas, deberá de levantar el reporte en el sistema de Soporte Técnico.
- *Notificar a los usuarios afectados el restablecimiento de los servicios de TIC´s.
- *Identificar y evaluar los daños de la infraestructura de telecomunicaciones.

INCENDIOS

-Acciones preventivas-

- Todo el personal deberá conocer los protocolos de seguridad señalados por el comité de protección civil de la AGEPRO.
- Contar con respaldos de la información institucional del disco duro de cada equipo de cómputo.
- Tener a la mano la unidad de almacenamiento que contiene los respaldos de cada usuario.
- *Contar con respaldos internos de seguridad del equipamiento de telecomunicaciones de la Agencia.
- *Tener a la mano la unidad de almacenamiento que contiene los respaldos del equipo de telecomunicaciones, siempre y cuando sea de dimensiones que permitan un traslado sin complicaciones.

-Acciones durante el incendio-

- Todo el personal deberá apegarse a los protocolos de seguridad señalados por el comité de protección civil de la AGEPRO.
- *Salvaguardar la unidad de unidad de almacenamiento que contiene los respaldos del equipo de telecomunicaciones, siempre y cuando sea de dimensiones que permitan un traslado sin complicaciones.

-Acciones posterior del incendio-

- *Realizar un reporte de los daños causados en la infraestructura de telecomunicaciones de la Agencia.
- *Realizar las acciones pertinentes para el restablecimiento del servicio de Telecomunicaciones.
- Solicitar la revisión de sus equipos y esperar a que el personal de la UTIC emita un dictamen.

TORMENTAS TROPICALES / HURACANES

-Acciones preventivas-

- Todo el personal deberá conocer los protocolos de seguridad señalados por el comité de protección civil de la AGEPRO.
- Contar con respaldos de la información institucional del disco duro de cada equipo de cómputo.
- Tener a la mano la unidad de almacenamiento que contiene los respaldos de cada usuario.
- *Contar con respaldos internos de seguridad del equipamiento de telecomunicaciones de la Agencia.
- *Tener a la mano la unidad de almacenamiento que contiene los respaldos del equipo de telecomunicaciones, siempre y cuando sea de dimensiones que permitan un traslado sin complicaciones.
- Apagar y desconectar equipos de cómputo y telecomunicaciones, incluyendo impresoras, scanner y no-break cuando el área responsable de la seguridad lo indique.
- Colocar los equipos de cómputo y telecomunicaciones, impresoras, scanner y no-break dentro de bolsas de plástico, etiquetarlos y resguardarlos en lugares seguros.

-Acciones durante el la tormenta o huracán-

- Mantenerse en sus domicilios atentos a los boletines emitidos por la Coordinación Estatal de Protección Civil del Estado de Quintana Roo.
- En caso de no poder abandonar las instalaciones de la Agencia a tiempo, deberá de apegarse a las indicaciones de las Brigadas Internas de Protección Civil de la AGEPRO.

-Posterior de la tormenta tropical / huracán-

- *Realizar un reporte de los daños causados en la infraestructura de telecomunicaciones de la Agencia.
- *Realizar las acciones pertinentes para el restablecimiento del servicio de Telecomunicaciones.
- Solicitar la revisión de sus equipos y esperar a que el personal de la UTIC emita un dictamen.

DELITO INFORMATICO

Incorporar un apartado específico sobre delito informático dentro del Plan de Contingencia permite establecer lineamientos claros para la identificación, prevención, detección y respuesta ante incidentes derivados de actividades ilícitas en el entorno digital. Asimismo, fortalece la capacidad institucional para mitigar riesgos, asegurar la resiliencia tecnológica y garantizar que las acciones de recuperación se ejecuten de manera coordinada, oportuna y conforme al marco normativo aplicable.
Este segmento busca proporcionar las bases para una actuación integral frente a amenazas informáticas, promoviendo una cultura de seguridad que contribuya a la protección de los activos tecnológicos y a la correcta operatividad y accesibilidad de la infraestructura de telecomunicaciones.

- El/la Titular de la Unidad de Tecnologías de Información y Comunicaciones será quien autoriza la activación del plan de contingencia.
- Los/las titulares de los departamentos de Soporte Técnico y Telecomunicaciones (Chetumal y Cancún) y del Departamento de Tecnología de Software, serán las personas encargadas de ejecutar el plan de contingencia con apoyo de todo el personal adscrito a la UTIC.

-Acciones preventivas-

- Detectar y revisar todas las alertas o incidentes que arrojen parámetros sobre la contingencia.
  Por ejemplo:
  - Mensajes de error durante la ejecución de programas.
  - Lentitud en el acceso a las aplicaciones.

- Falla general en el equipo (sistema operativo, aplicaciones).
- Denegación de servicios informáticos, entre otros.

- Implementar autenticación multifactor (MFA) en los sistemas y/o plataformas que lo permitan.
- Mantener políticas de respaldos periódicos.
- Aplicar controles de acceso basados en roles, en los sistemas y/o plataformas que lo permitan.
- Realizar auditorías y pruebas de penetración, siempre y cuando sea factible realizar la contratación de un servicio de terceros para la aplicación.
- Capacitar continuamente a los usuarios sobre phishing y seguridad digital

-Acciones durante-

- Detección e identificación del incidente

- Monitorear constantemente la infraestructura de telecomunicaciones de la agencia mediante herramientas de seguridad (SIEM, IDS/IPS, antivirus, logs, etc).
- Identificar comportamientos anómalos en la red, servidores o equipos de usuario.
- Verificar alertas de seguridad generadas por los sistemas.
- Determinar el tipo de incidente (intrusión, malware, phishing, robo de información, ransomware, etc.).
- Evaluar el alcance del incidente: sistemas afectados, usuarios comprometidos y posible impacto.

- Contención inmediata

- Desconectar o retirar de la red de datos de la Agencia
- Aislar los equipos comprometidos de la red para evitar propagación
- Desactivar cuentas de usuario comprometidas o sospechosas.
- Bloquear direcciones IP o dominios maliciosos en firewall o sistemas de filtrado.
- Suspender temporalmente servicios vulnerables si representan un riesgo.
- Aplicar reglas de seguridad adicionales en los dispositivos de red.

- Preservación de evidencia digital

- Realizar copias memoria y registros del sistema.
- Guardar logs de servidores, firewalls, aplicaciones y sistemas de autenticación.
- Documentar cronológicamente todos los eventos detectados.
- Mantener cadena de custodia de la evidencia digital.
- Evitar modificar o eliminar archivos que puedan servir como prueba.

- Análisis del incidente

- Identificar el vector de ataque (phishing, vulnerabilidad explotada, acceso indebido, etc.).
- Determinar cómo se comprometió el sistema.
- Analizar malware o herramientas utilizadas por el atacante.
- Evaluar la información comprometida o filtrada.
- Determinar la magnitud del daño y los sistemas afectados.

- Erradicación de la amenaza

- Eliminar malware o accesos no autorizados.
- Aplicar parches de seguridad y actualizaciones pendientes.
- Reconfigurar sistemas comprometidos.
- Cambiar credenciales comprometidas.
- Reinstalar sistemas afectados si es necesario.

- Recuperación de sistemas

- Restaurar información desde respaldos seguros.
- Verificar integridad de los sistemas antes de volver a conectarlos a la red.
- Monitorear de manera intensiva los sistemas recuperados.
- Reanudar operaciones gradualmente.

- Comunicación y notificación

- Notificar a la dirección de la organización.
- Informar a las autoridades competentes si el incidente constituye un delito.
- Comunicar a los usuarios afectados si hubo compromiso o pérdida de datos e información.
- Elaborar reportes técnicos del incidente.

- Documentación y lecciones aprendidas.

- Elaborar un informe detallado del incidente.
- Analizar fallas en controles de seguridad.
- Actualizar políticas y procedimientos de seguridad.
- Implementar medidas preventivas para evitar incidentes similares.
- Capacitar al personal en ciberseguridad.

-

-Acciones posterior del ataque-

- Efectuar las pruebas necesarias con el usuario final de los equipos y/o sistemas de información afectados.
- Restaurar el correcto funcionamiento de la infraestructura de telecomunicaciones de la Agencia y reanudar con las actividades de forma cotidiana.
- Comunicar el restablecimiento del servicio.

IMPREVISTOS

Los casos que se presenten y que estén vinculados al trabajo y no estén contemplados en este Manual de Políticas, serán atendidos o resueltos por la Unidad de Tecnologías de la Información y Comunicaciones.

VIGENCIA

Este Manual entrará en vigencia a partir de la aprobación del mismo por parte del Director General, y socialización con los encargados de las Unidades Administrativas, permanecerá por tiempo indefinido introduciéndosele las revisiones y las mejoras que amerite el mismo.

CHETUMAL QUINTANA ROO, A 27 DE MARZO DEL AÑO 2026

FORMALIZACIÓN DEL
PLAN DE CONTINGENCIA EN MATERIA DE TIC´s APLICABLE A LAS OFICINAS DE LA AGENCIA DE PROYECTOS ESTRATÉGICOS DEL ESTADO DE QUINTANA ROO.

-ACCIONES INTERNAS-

C. CARLOS FLORES HIDALGO

DIRECTOR GENERAL DE LA AGENCIA DE PROYECTOS ESTRATÉGICOS DEL ESTADO DE QUINTANA ROO.

C. VANESSA GUADALUPE RAMIREZ ORTIZ

TITULAR DE LA UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES DE LA AGENCIA DE PROYECTOS ESTRATÉGICOS DEL ESTADO DE QUINTANA ROO.

LCDA. MARÍA NEYDI ESCAMILLA QUIJANO

JEFA DEL DEPARTAMENTO DE TECNOLOGÍA DE SOFTWARE

LCDO. JOSÉ ROMÁN RÍO ARCEO

JEFE DEL DEPARTAMENTO DE SOPORTE TÉCNICO Y TELECOMUNICACIONES