PROGRAMA DE RESULTADOS ELECTORALES PRELIMINARES (PREP)
PLAN DE CONTINUIDAD

ANEXO. II

Contenido

1.-Antecedentes

Dentro de la Gestión de la Seguridad de la Información en una compañía es importante contar con un plan alternativo que asegure la continuidad de la actividad del Negocio en caso de que ocurran incidentes graves.

Tradicionalmente, los Planes de Continuidad, denominados Planes de Contingencia en sus orígenes, están asociados a grandes compañías que necesitan reaccionar de forma inmediata ante cualquier evento que interrumpa sus servicios. La realidad es que cualquier compañía puede sufrir un incidente que afecte a su continuidad y, dependiendo de la forma en que se gestione dicho incidente, las consecuencias pueden ser más o menos graves.

A la velocidad con la que operan los negocios actuales un incidente de unas pocas horas de duración puede tener un impacto catastrófico en los resultados y en la imagen de la organización que lo sufra.

La íntima dependencia que existe entre el negocio y los sistemas de información exige que éstos estén preparados para afrontar las múltiples amenazas que ponen en riesgo su operatividad y, en consecuencia, la continuidad del negocio. El incendio ocurrido en el Edificio Windsor en Madrid en el mes de febrero de 2005 o el Huracán Katrina en agosto de ese mismo año, son dos ejemplos que vienen a sumarse a sucesos, como los atentados del 11-S del año 2001. Sin embargo, en no pocas ocasiones no es necesario un desastre de dimensiones parecidas a las de los mencionados anteriormente para poner en peligro no sólo la buena marcha del negocio sino su misma supervivencia; eventos como la irrupción de un virus o la instalación de un parche de seguridad pueden conducir a la inoperabilidad temporal de los sistemas, la pérdida de información crítica o, en última instancia, la inutilización de las infraestructuras

http://www.criptored.upm.es/guiateoria/gt_m001r.htm

2.- Generales

Un plan de continuidad se compone de varias fases que comienzan con un análisis de los procesos que componen la organización. Este análisis servirá para priorizar qué procesos son críticos para el negocio y establecer una política de recuperación ante un desastre.

Por cada proceso se identifican los impactos potenciales que amenazan la organización, estableciendo un plan que permita continuar con la actividad empresarial en caso de una interrupción.

Beneficios de contar con un plan de continuidad:

- Identifica los diversos eventos que podrían impactar sobre la continuidad de las operaciones y su impacto sobre el negocio.
- Obliga a conocer los tiempos críticos de recuperación para volver a la situación anterior al desastre sin comprometer al negocio.
- Previene o minimiza las pérdidas para el negocio en caso de desastre.
- Clasifica los activos para priorizar su protección en caso de desastre.
- Aporta una ventaja competitiva frente a la competencia.

El **objetivo final** es mantener el negocio, por lo que se deberán priorizar las operaciones de negocio críticas necesarias para continuar en funcionamiento después de un incidente no planificado.

http://www.soyentrepreneur.com/que-es-un-plan-de-continuidad-de-negocio.html

3.- Objetivo

Elaborar el programa denominado "Plan de Continuidad" para determinar acciones que garanticen las ejecuciones de los procesos de acopio, digitalización, captura, verificación y publicación, en caso de que se suscite una situación adversa o de contingencia, dentro de este plan estará involucrado el personal involucrado en la operación del sistema y deberá formar parte de los ejercicios y simulacros referido en el Capítulo VI de los Lineamientos del Programa de Resultados Electorales Preliminares.

4.- Plan de Continuidad.

4.1 - PREREQUISITOS:

- Elaborar un directorio de las personas que toman parte en el proceso **PREP** (teléfono de trabajo y residencia, celular, busca, correo electrónico tanto de trabajo como personal, y cualquier otra forma posible de contactarlos en una situación de emergencia), así como de las personas que podrían sustituirlos
- Todo el personal participante en la **Jornada Electoral** para el **PREP** deberá estar debidamente identificado con credenciales que acrediten su personalidad y su rol tanto en los **CATD** como en el **Recinto Central.**
- Todo material informático deberá de estar debidamente identificado y aprobado para su utilización así como respaldados para su rápida recuperación en caso de desastre
- Elaborar una lista de contactos especial que incluya una descripción de la institución o persona y cualquier otra información que sea absolutamente crítica sobre ellos, incluyendo información de contacto:
    - personal de emergencias,
    - policía, bomberos,
    - suministro de agua,
    - suministro luz,
    - hospitales
    - personal técnico computo, aires acondicionados
- Contar con equipos de computo, scanner, respaldo de energía , comunicaciones y enlaces de respaldo 1 a 1 en sus respectivos **CATD** o **Recinto Central**.
- Los **CATD** y el **Recinto Central** deberán contar con instalaciones eléctricas adecuadas y suficientes para la operación de toda la infraestructura, así como también de generadores de energía eléctrica para suministrar una fuente de energía alterna en caso de falla de la red eléctrica publica.
- Todo el personal del **PREP** deberá contar con una copia del plan de Continuidad

4.2 - GUÍA DE "CÓMO HACER"

Debe incluir instrucciones paso por paso de que hacer, quien tiene que hacerlo y cómo hacerlo en caso de una eventualidad.

- Prepara una lista de cada responsabilidad y escribe el nombre de la persona a la que está asignada. También, hazlo al contrario: Para cada persona, enlista las responsabilidades. De esa forma,, si quieres saber quien se supone que debe llamar a la compañía de seguros, puedes buscar "Seguro". Si quieres saber que está haciendo Joe Doe, puedes buscar bajo "Joe", y así obtener esa información.

EVENTUALIDAD	ACCIÓN A REALIZAR	RESPONSABLE
El personal contratado no llego	Consultar el directorio del personal Localizar a quien pueda sustituirlo Sustituirlo	Coordinador PREP
Equipo informático no arranca	Sustituir con equipo de respaldo	Por definir
Equipo informático no enlaza	• Checar conexiones • Sustituir cableado • Sustituir con equipo de respaldo	Por definir
Equipo de respaldo de energía no funciona	Sustituir con equipo de respaldo	Por definir
Scanner no trabaja correctamente	Sustituir con equipo de respaldo	Por definir
Enlace de comunicación primario no conecta	Montar comunicación en enlace de respaldo	Por definir
Corte de energía eléctrica	• Entrada en funciones de equipo de respaldo de energía • Arranque de generador de energía eléctrica	Por definir
Existe enlace, documentos no pasan	Montar comunicación en enlace de respaldo	Por definir

A continuación se describe las clases de incidentes que podrían presentarse el día de la jornada electoral

5.1 – Incidentes contemplados

5.1 - Funcionamiento de dispositivos eléctricos

- Se deberá probar con anterioridad a los simulacros y al día de la jornada que los equipos arranquen adecuadamente
- Los CATD deberán contar con un respaldo 1 a 1 de los equipos instalados

- Así mismo los espacios físicos en los CATD deberán contar con instalaciones eléctricas adecuadas con tierra física instalada

5.2 - Funcionamiento de dispositivos de red

- Antes, durante y después de los simulacros y antes del día de la jornada se deberá de revisar el correcto funcionamiento de cada uno de los nodos de la red.
- Contar con cables de red de repuesto.
- Contar con una conexión a internet de Telmex en los CATD
- Conexión a internet de respaldo que permita enviar las AEC digitalizadas al Recinto Central
- La red en ese momento deberá estar correctamente aislada a través de VPN´s
- Físicamente no deberá permitir ninguna conexión alambrica o inalámbrica no contemplada dentro del esquema inicial

5.3 - Funcionamiento de terminales de digitalización

- Antes durante y después de los simulacros se deberá de supervisar el correcto funcionamiento y configuración de estas terminales para corregir cualquier eventualidad que se pudiera observar.
- El día de la jornada antes de entrar en producción los equipos deberán de probarse y en caso de observar algún mal funcionamiento deberán ser sustituidos por los equipos de respaldo
- En los CATD se deberá de contar con un respaldo de al menos 1 a 1 de las terminales y equipos de digitalización requeridos

5.4 - Funcionamiento de terminales de captura

- Antes durante y después de los simulacros se deberá de supervisar el correcto funcionamiento y configuración de estas terminales para corregir cualquier eventualidad que se pudiera observar.
- El día de la jornada antes de entrar en producción los equipos deberán de probarse y en caso de observar algún mal funcionamiento deberán ser sustituidos por los equipos de respaldo
- En el recinto central se deberá contar con al menos 1 a 1 de las terminales y equipos de captura requeridos

5.5 - Falla de suministro eléctrico y enlaces de comunicaciones

- En caso de falla del suministro eléctrico todas las terminales y equipos deberán de contar con equipos de respaldo de energía de alta capacidad así como de plantas generadoras de corriente eléctrica con capacidad de sostener el funcionamiento de las terminales, equipos y enlaces de comunicación por al menos el tiempo necesario para que las AEC sean digitalizadas y enviadas al recinto central
- Los enlaces de comunicación deberán contar con alguna vía alterna de comunicación que en caso de falla de la primera permita enviar las AEC digitalizadas al recinto central o a los servidores de los difusores oficiales

5.6 - Carga y funcionamiento del sistema

- Durante los simulacros se deberán de realizar pruebas de bombardeo y captura de datos para verificar la disponibilidad y capacidad del sistema realizando las correcciones pertinentes en caso de falla.

5.7 - Configuración de equipos de comunicaciones, servidores de procesamiento y redes de almacenamiento de información.-

- Antes de los simulacros y del día de la jornada se deberá supervisar que los equipos de comunicación estén debidamente configurados configurados bajo la supervisión del área administrativa de sistemas y tecnologías de computo a fin de garantizar la calidad de la comunicación y corregir en caso de ser necesario para garantizar que el día de la jornada el riesgo de la perdida de datos sea mínima.
- Antes de los simulacros y del día de la jornada se deberá supervisar que los servidores estén debidamente configurados bajo la supervisión del área administrativa de sistemas y tecnologías de computo a fin de garantizar su funcionamiento y corregir en caso de ser necesario, cada servidor deberá tener la capacidad de replicarse o espejearse en otro servidor para que en caso de mal funcionamiento pueda ser switcheado y no perder la continuidad en la recepción de las AEC, su captura , el procesamiento y el envió de información a los Difusores Oficiales
- Antes de los simulacros y del día de la jornada se deberá supervisar que las redes y equipos de almacenamiento de información estén debidamente configurados bajo la supervisión del área administrativa de sistemas y tecnologías de computo a fin de garantizar su funcionamiento y corregir en caso de ser necesario, así como también verificar que las bases de datos estén en ceros antes de cada simulacro y el día de la jornada electoral

5.8 - funcionamiento de sistemas de soporte (aire acondicionado, equipos de energía ininterrumpida, control de acceso, extinción de incendios, etc.)

- Antes de los simulacros y el día de la jornada en los lugares que así lo ameriten se deberá de supervisar el correcto funcionamiento de los equipos de aire acondicionado para garantizar las condiciones óptimas de temperatura y humedad para un correcto funcionamiento de las terminales y equipos de no ser así, deberá de corregirse inmediatamente por lo que se recomienda tener un soporte técnico para ese aspecto.
- Los equipos de energía ininterrumpida deberán de ser probados frecuentemente durante los simulacros para garantizar su confiabilidad y tener en todo momento un respaldo para que puedan ser sustituidos en caso de falla
- El control de acceso a las áreas restringidas deberá de ser completamente prohibido a todo público teniendo acceso exclusivamente el personal que haya sido registrado y autorizado con anterioridad al los simulacros y al día de la jornada ante el Área Administrativa De Sistemas Y Tecnologías
- Todas las áreas deberán ser dotadas con equipos de seguridad contra incendios adecuados para el tipo de eventualidades que puedan presentarse en los simulacros y el día de la jornada

5.9 - Operación de enlaces y redes a nivel estatal

- Durante todos los simulacros y el día de la jornada en todo momento y una vez instalados los enlaces de comunicación, se llevara a cabo verificaciones de trafico autorizado para detectar intrusiones para poder bloquearlas

5.10 - Contingencia en caso de inhabilitación del recinto Central y falla de equipos.

- En caso de inhabilitación del recinto central, se deberá de contar con un recinto alterno donde pudieran ser trasladados las terminales, los equipos y el personal para poder llevar a cabo la jornada
- Si algún equipo presentara falla, se deberá ser capaces de sustituirlo de manera inmediata por otro de iguales características y configurado de antemano para continuar el proceso para el cual fue designado

5.11 - Capacidad y desempeño de cada componente en los centros de cómputo

- Se establecerán umbrales de desempeño y capacidad de los diferentes componentes del sistema los cuales deberán ser probados intensamente durante los simulacros y en caso de ser necesario corregidos para que lleguen en condiciones optimas al día de la jornada

6.- Conclusiones

6.1 - Conclusiones

Un plan de continuidad puede representar una diferencia muy grande entre un proyecto o negocio exitoso a un rotundo fracaso, por lo tanto es de suma importancia implementar un plan de continuidad adecuado a las necesidades que este instituto requiere para la continuidad del PREP el dia de la Jornada Electoral el 7 de junio del presente año