H. Congreso del Estado de Yucatán
LXII Legislatura

Plan de Recuperación de Desastres del Área de TI

Autor: Adán Bates Crespo

Mérida, Yucatán, México

Introducción

El Poder Legislativo del Estado de Yucatán es una entidad gubernamental de suma importancia ya que se encarga de legislar y fiscalizar al Poder Ejecutivo.

El poder legislativo se presenta como un poder que constituye al Sistema Político Mexicano, dedicado a elaborar y modificar las leyes existentes de acuerdo a la opinión de los ciudadanos. Apegándose del mismo modo esta concepción, a la teoría del constitucionalismo moderno, en donde el poder legislativo, consiste en redactar, reformar y derogar las leyes.

Es por esa importancia que es imperativo el correcto resguardo de la información que se genera en el recinto ante cualquier imprevisto ya sea humano o climático.

Este manual servirá de guía para poder llevar a cabo la tarea de recuperación de ese tipo de imprevistos.

Conceptos generales

DESASTRE

Tradicionalmente se ha entendido por desastre a un incendio o inundación, porque este tipo de eventualidades destruía recursos físicos de la organización como archivos, equipos o los registros vitales. En la actualidad, eliminados en gran medida estos riesgos, los altos directivos se enfrentan a una nueva forma de desastre, que afecta directamente a su activo principal, que es la información.

En cualquier momento, la informática de una empresa se puede quebrar total o parcialmente como consecuencia de un siniestro fortuito. Si, las operaciones más importantes de la empresa se suspenden repentinamente, será incalculable el daño causado al negocio y más aún a la reputación de esta. Entre las principales causas de desastres informáticos se tiene los siguientes.

- Fallo en el suministro y red eléctrica.
- Fallos en el hardware y los sistemas de almacenamiento.
- Fallos humanos.
- Fallos de software.
- Ataques maliciosos y virus informáticos
- Desastres naturales.

AMENAZA

Una causa potencial de un incidente no-deseado, el cual puede resultar en daño a un sistema u organización. NIST de los Estados Unidos de América 2008 lo define como: "Cualquier circunstancia o hecho que pueda afectar negativamente a las operaciones de la organización, sus activos de información o individuos a través del acceso no autorizado, destrucción, acceso, modificación de la información, y/o negación de servicio. Además, la posibilidad de una amenaza de fuente de explotar con éxito una vulnerabilidad de la información del sistema en particular. En otra acepción, son todas las actividades, eventos o circunstancias que pueden afectar el buen uso de un activo de información dañando el soporte a un proceso, perjudicando el logro de los objetivos de negocio".

VULNERABILIDAD

Es la debilidad de un activo o grupo de activos que puede ser explotada y perjudicada por una o más amenazas. Son debilidades que pueden ser exploradas para convertir una amenaza en un riesgo real que pueden causar daños graves en una organización. Las vulnerabilidades son una o más condiciones que pueden permitir a una amenaza afectar a un activo. Según el BCI 2010: "Las vulnerabilidades en el negocio y en el modelo de operación de una organización pueden considerarse en siete áreas: reputación, cadena de suministro, información y comunicaciones, sedes e instalaciones, personas, finanzas y clientes". Se puede definir a la ausencia de controles o a su deficiente establecimiento como las principales causas de vulnerabilidad sobre los activos de una organización.

RIESGO

Potencial de que una amenaza – externa o interna – explote una vulnerabilidad de uno o varios activos ocasionando daño a la organización. Su naturaleza puede depender de aspectos operativos, financieros, regulatorios y administrativos (ISO 27005, 2008).

Según COSO en su "Marco de Gestión Integral de Riesgo" (2008): "Los riesgos son futuros eventos inciertos, los cuales pueden influir el cumplimiento de los objetivos estratégicos, operacionales, financieros y de cumplimiento".

Causas de los Riesgos:

- Personal: Fallas cometidas por el personal. Ejemplo: Por falta de conocimiento.

- Procesos: Fallas causadas por debilidades en el diseño y/o ejecución de procesos de la organización como por ejemplo controles inadecuados.

- Sistemas: Fallas causadas por vulnerabilidades en los sistemas, como fallas de red o caídas de sistemas.

- Eventos externos: Fallas que resultan por cambios adversos en el entorno de la organización, por situaciones causadas por terceros o por desastres naturales.

IMPACTO

El Business Continuity Institute (2012) lo define como un "Evento que tiene la capacidad de provocar la pérdida de o la interrupción de las operaciones, servicios o funciones de la organización, el cual, si no se administra, puede escalar y convertirse en una emergencia, crisis o desastre". Su identificación y cuantificación es relevante en el proceso de la Gestión de Riesgos, que es el conjunto de actividades que permite analizar, tratar y evaluar los riesgos en las organizaciones.

Cabe mencionar que la valoración del impacto puede ser expresado de forma cuantitativa, es decir estimando las pérdidas económicas, o de forma cualitativa, asignando un valor dentro de una escala (alto, bajo, medio), también se recurre al análisis de grado de pérdida o daño que causaría una interrupción en un activo de información mediante el manejo de probabilidades de ocurrencia, ya que se utiliza para determinar si se invertirá en medidas para evitar dicha interrupción.

La interrupción se puede evitar teniendo un procedimiento que, o bien proporciona alguna forma alternativa de la continuidad del negocio o corrige el problema dentro de un tiempo aceptable. El impacto no siempre se produce inmediatamente después de una interrupción y la mayoría de las empresas pueden sobrevivir durante algún tiempo antes de que las pérdidas comiencen. Este período es vital para el negocio y varía entre empresas y líneas de negocio.

Si se realiza un análisis de riesgos basado de tipo cuantitativo de impacto y las probabilidades, las escalas cualitativas del impacto son: catastrófico o extremo, grave, medio, moderado o bajo e insignificante probable.

A continuación se mostrará la matriz que se ajustará según las políticas que emplea la entidad referenciada en la presente tesis. Es decir, va a depender del tipo de organización y de los activos de información que se tengan para clasificar los riesgos y calcular los impactos.

CONTROLES

Son las políticas, medidas de seguridad, procedimientos y prácticas para reducir riesgos y que proveen cierto grado de certeza de que se lograrán los objetivos del negocio. Estos permiten que se realicen las correcciones necesarias en caso se detecten eventos que escapan de su alcance.

Los objetivos relevantes de los controles son:

- Garantizar que mediante los mecanismos de control establecidos se logren las metas de la organización.

- Salvaguardar los activos de la organización para mantener la integridad de la información.

Plan de Evacuación.

- Gestión del Incidente: La gestión de Respuesta al incidente como por ejemplo un

Plan de Continuidad en Crisis.

- Continuidad: La repuesta inicial del negocio para asegurar que las actividades esenciales pueden continuar operando a un nivel mínimo aceptable.

- Recuperación: Un plan para recuperar actividades a un nivel sostenible.

- Reanudación: Un plan para reanudar las operaciones de la organización.

Un Plan de Continuidad de Negocio (BCP) está formado por los siguientes planes:

Plan de Emergencia, Plan de Comunicación de Crisis, Plan de Gestión de Crisis y Plan de

Recuperación de Desastres.

Es un proceso documentado o conjunto de procedimientos o acciones para recuperar y proteger la infraestructura de TI de una organización en caso de un desastre. Refiriéndose con desastre a todo evento súbito, imprevisto catastrófico que interrumpe los procesos de negocio lo suficiente como para poner en peligro la viabilidad de la organización .Un desastre podría ser el resultado de un daño importante a una parte de las operaciones, la pérdida total de una instalación, o la incapacidad de los empleados para acceder a esa instalación. El DRP es una declaración exhaustiva de acciones coherentes que deben tomarse antes, durante y después de un desastre".

El Plan de Recuperación de Desastres tiene como objetivo proporcionar un marco para la reconstrucción de las operaciones vitales de la organización, para garantizar la seguridad de los empleados y la reanudación de las operaciones sensibles a tiempo y los servicios en caso de una emergencia.

El DRP incluye la planeación de pasos para evitar riesgos y mitigarlos, DRP es aplicable en todos los aspectos de un negocio, sin embargo se utiliza normalmente en el contexto de operaciones para el procesamiento de datos.

Beneficios de un Plan de Recuperación ante un desastre:

- Permite a la organización evitar riesgos de retrasos o mitigar el impacto de estos al: minimizar potenciales perdidas económicas y; decrementar la exposición a escenarios de desastre.

- Reducir la probabilidad de que ocurran al mejorar la capacidad de recuperar las operaciones normales del negocio.

- Reducir las interrupciones de la operación.

- Provee un procedimiento pre- planificado minimizando el tiempo de toma de decisiones en caso de desastre.

- Elimina la confusión y reduce la probabilidad de error humano debido al estrés que produce una crisis.

- Protege los activos de la organización incluyendo al recurso humano.

Los planes de recuperación de desastres TI facilitan procedimientos detallados a seguir, paso a paso, para recuperar los sistemas y redes que han tenido interrupciones y ayudar a simplificar la normalidad en las operaciones. El objetivo de estos procesos es reducir cualquier impacto negativo en las operaciones de la organización. El proceso de recuperación de desastres identifica los sistemas y redes críticos de TI; fija las prioridades para su recuperación y dibuja los pasos necesarios para reiniciar, reconfigurar y recuperar dichos sistemas y redes. Todo plan integral de recuperación de desastres debe incluir a todos los proveedores más relevantes, las fuentes de experiencia para recuperar los sistemas afectados y una secuencia lógica de los pasos a seguir hasta alcanzar una recuperación óptima.

La ampliación de cada paso del Plan de Recuperación de Desastres de TI son los siguientes.

- El equipo de implementación del plan debería reunirse con el equipo interno de TI, el equipo de aplicación y los administradores de redes, y establecer el alcance de la acción, como por ejemplo, elementos internos, activos externos, recursos de terceros y enlaces a oficinas/clientes/proveedores; debemos asegurarnos de informar a la dirección del departamento de TI sobre dichas reuniones para que estén bien informados.

- Recopilar todos los documentos relevantes de la infraestructura de redes, como los diagramas de las redes, la configuración de los equipos y bases de datos.

- Obtener copias de los planes de recuperación de redes y de TI existentes; si no los hay, proceder con los siguientes pasos.

- Identificar las amenazas contra la infraestructura de TI que la dirección considere más preocupantes: por ejemplo, incendios, errores humanos, apagones de energía, fallo de los sistemas.

- Identificar aquello que la dirección considera que son las principales vulnerabilidades de la infraestructura: por ejemplo, inexistencia de sistemas de respaldo en caso de apagón eléctrico, copias de bases de datos obsoletas.

- Examinar el historial previo de apagones y disrupciones, y cómo fueron gestionados por la empresa.

- Identificar los activos TI que la dirección considera de importancia crítica. Por ejemplo: centro de llamadas, granjas de servidores, acceso a internet.

- Determinar el tiempo máximo de apagón eléctrico que está dispuesta a aceptar la dirección en caso de indisponibilidad de los equipos TI.

- Identificar los procedimientos operativos que se utilizan actualmente para responder a los apagones críticos.

- Determinar cuándo se probaron estos procedimientos para validar si siguen siendo adecuados o no.

- Identificar el/los equipo/s de respuesta de emergencia para todas las disrupciones de la infraestructura crítica de TI; determinar su nivel de conocimientos y preparación para manejar los sistemas críticos, especialmente en casos de emergencia.

- Identificar las capacidades de respuesta de los proveedores en casos de emergencia; si se han utilizado alguna vez; si funcionaron correctamente; cuánto paga la compañía por estos servicios; el estado del contrato de servicio; la existencia del acuerdo de nivel de servicio (SLA) y si se usa alguna vez.

- Recopilar los resultados de todas las evaluaciones en un reporte de análisis de carencias que identifique lo que se está haciendo frente a lo que debería hacerse, con recomendaciones sobre cómo lograr el nivel requerido de preparación y las inversiones necesarias para ello.

- Lograr que la dirección lea el reporte y acuerde tomar las acciones recomendadas.

- Preparar un plan de recuperación de desastres IT que cubra los sistemas y las redes esenciales de TI.

- Realizar pruebas de los planes y activos de recuperación de sistemas para validar su operatividad.

- Actualizar la documentación del plan de RD para que recoja los cambios efectuados.

- Programar la próxima revisión/auditoría de capacidades de recuperación de desastres

DEFINICION DEL PROBLEMA

3.1 Alcance de DRP

Al contar la institución educativa con la identificación de sus funciones y recursos críticos, es posible cumplir con su misión en caso de presentarse una contingencia que afecte el recinto del Congreso del Estado ubicado en la ciudad de Mérida, Yucatán, y conocer cómo va a impactar estas interrupciones a sus funciones o procesos críticos.

El plan proporcionará una descripción de las responsabilidades individuales y los procedimientos necesarios para restaurar los servidores y las telecomunicaciones en el menor tiempo posible.

En muchos casos, la importancia de contar con un DRP eficaz, consistente y actualizado que permita minimizar el tiempo de interrupción de los servicios informáticos en una compañía, se hace evidente cuando se producen situaciones de desastres que ponen en riesgo los activos informáticos, generando consecuencias desfavorables para la organización.

Por ello, antes de que ocurra un desastre informático, es fundamental que la empresa evalué el costo económico de perder sus datos, poner en riesgo su imagen, perder clientes actuales y futuros y, por supuesto, las implicancias de detener las operaciones propias de la compañía, para así darse cuenta de lo indispensable que resulta contar con un sistema DRP.

3.2 Análisis de riesgos de continuidad de DRP

Se realizó el análisis de riesgos correspondiente a la organización, de los cuales, se identificaron seis escenarios de riesgos, se expresa la posibilidad de currencia, se listan las causas de cada escenario, así como el efecto que causaría en la institución.

Tabla 2

Cód.	Escenario	Riesgo (Existe la posibilidad de:)	Causas (Dado que)	Efectos
R1	Indisponibilidad de acceso al centro de cómputo principal.	No se puede ingresar a la sede principal, donde se encuentra el centro de cómputo, y que todos los activos se encuentren intactos (sin ningún daño físico).	1. Ocurra una huelga en contra de UPC por personas externas. 2. Ocurra una huelga por parte de trabajadores de UPC. 3. Accidente de tránsito con heridos graves y/o fallecidos. 4. Amenazas de Bomba, materiales peligrosos (gas tóxico, etc.). 5. Protestas de alumnos en contra de UPC.	Interrupción en la operación de los procesos críticos que son soportados por los sistemas de información
R2	Pérdida total del data center principal.	No se puede ingresar a la sede principal, donde se encuentra el centro de cómputo, y todos los activos se encuentran destruidos.	1. Incendio no controlado 2. Inundación de sitio principal.	Interrupción en la operación de los procesos críticos que son soportados por los sistemas de información
R3	Indisponibilidad de la Información.	No se cuente con la información o los sistemas por algún problema tecnológico	1. Falla de los Aplicativos o Sistemas Críticos. 2. Falta de Energía en el Centro de Cómputo. 3. Falla de seguridad lógica. 4. Lentitud en los sistemas críticos. 5. Ataque Cibernético DoS.	Interrupción en la operación de los procesos críticos que son soportados por los sistemas de información
R4	Indisponibilidad de especialistas de TI (Recurso Humano).	No se cuente con el personal suficiente para realizar los subprocesos críticos de UPC.	1. Epidemias o Pandemias: Puede dar lugar a bajas del personal clave por periodos prolongados de tiempo. 2. Pérdida o fallecimiento de personal clave (por accidente, intoxicación, enfermedades graves, etc.) 3. Rotación de personal.	Interrupción en la operación de los procesos críticos que son soportados por los sistemas de información
R5	Indisponibilidad de	No se cuente con los servicios brindados	1. Interrupción del servicio por problemas externos a la institución. 2. Falta o falla de proveedor de Internet o fluido eléctrico.	Interrupción en la operación de los procesos críticos que
	Proveedores Críticos.	por el proveedor de sistemas u otros.		son soportados por los sistemas de información

Luego de haber identificado los posibles escenarios de amenazas, procedemos a estable la valoración en base a la probabilidad de ocurrencia y el impacto.

Leyenda de Probabilidad, se establece los niveles de probabilidad de acuerdo a los casos presentados en año, para cada escenario, siendo de nivel muy alto, aquellos que tienen más de 11 casos al año o más de un caso al mes.

Tabla 3

Leyenda de probabilidad

Probabilidad	Detalle	Nivel
P1	Se podría presentar hasta 1 caso al año	1.1 Muy bajo
P2	Se podría presentar de 2 a 4 casos al año	1.2 Bajo
P3	Se podría presentar de 5 a 7 casos al año	1.3 Medio
P4	Se podría presentar de 8 a 11 casos al año	1.4 Alto
P5	Más de 11 casos al año o más de 1 caso al mes	1.5 Muy Alto

Leyenda de Impacto, se establece los niveles de impacto de acuerdo a las pérdidas financieras, siendo de nivel muy alto, aquello que tiene pérdidas mayores a $240,000 al año.

Tabla 4

Leyenda de impacto

Impacto	Detalle	Nivel
I1	Pérdida menor o igual a US$ 36,000 al año	1.1 Muy bajo
I2	Pérdida mayor a US$ 36,000 y menor o igual a US$ 60,000 al año	1.2 Bajo
I3	Pérdida mayor a US$ 60,000 y menor o igual a US$120,000 al año	1.3 Medio
I4	Pérdida mayor a US$ 120,000 y menor o igual a US$ 240,000 al año	1.4 Alto
I5	Pérdida mayor a US$ 240,000 al año	1.5 Muy Alto

La clasificación y valoración de los riesgos identificados de acuerdo a los niveles de probabilidad e impacto son los siguientes.

Tabla 5

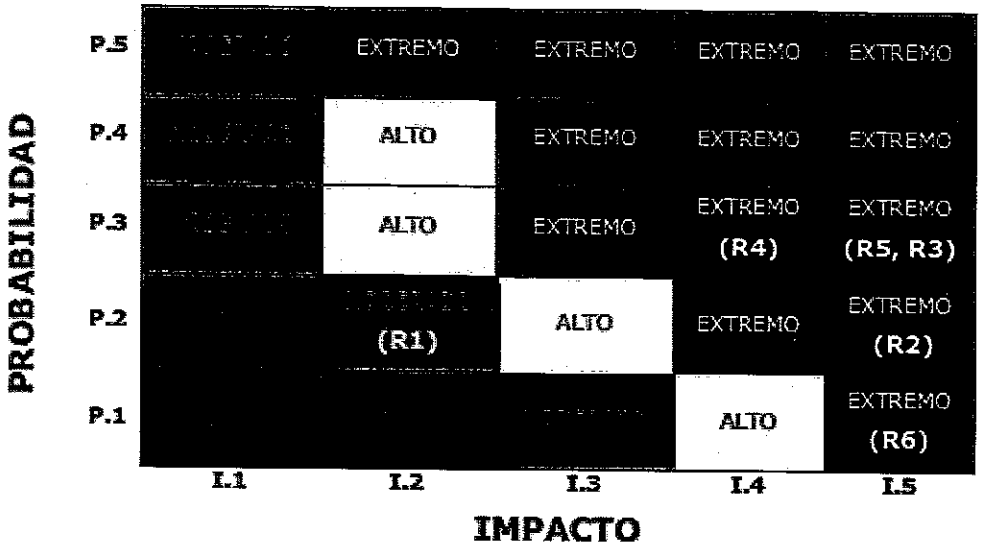
Clasificación y valoración de los riesgos

Cod.	Clasificación		Valoración del riesgo				
	Factor de Riesgo	Tipo de Evento	Detalle Probabilidad	Nivel de Probabilidad	Detalle del Impacto	Nivel de Impacto	Nivel de Riesgo
R1	4.Eventos Externos	5.Daños a activos materiales	1.2.Bajo	P1	1.2 Bajo	I2	
R2	4.Eventos Externos	5.Daños a activos materiales	1.1.Muy Bajo	P2	1.5 Muy Alto	I5	Extremo
R3	3.Tecnología	6.Interrupción del Negocio / fallo en el sistema	1.3.Medio	P3	1.4 Alto	I4	Extremo
R4	2.Personas	7.Ejecución entrega y gestión de procesos	1.3.Medio	P3	1.5 Muy Alto	I5	Extremo
R5	4.Eventos Externos	6.Interrupción del Negocio / fallo en el sistema	1.3.Medio	P3	1.5 Muy Alto	I5	Extremo
R6	4.Eventos Externos	6.Interrupción del Negocio / fallo en el sistema	1.1.Muy Bajo	P1	1.5 Muy Alto	I5	Extremo

Los riesgos identificados se ubican en el Mapa de Riesgos de la siguiente manera.

Tabla 6

Mapa de Riesgos



Identificado los escenarios de riesgos junto con su valoración de probabilidad por impacto se debe iniciar con el análisis de impacto de negocio que se describe a continuación.

3.3 Diseño del análisis de impacto de negocio

El factor tiempo se muestra como un factor crucial en cualquier escenario de recuperación ante interrupciones y debe ser determinado de forma particular para cada organización y actividad dentro de la misma. Mientras en algunos escenarios y/o actividades podríamos soportar tiempos de más de un día de interrupción, en el sector bancario, por ejemplo esto podría suponer el cierre definitivo de operaciones. El análisis del impacto en el negocio debe ser desarrollado mediante entrevistas con cada responsable de las principales actividades de riesgo en la empresa, complementada con talleres de formación y sensibilización sobre las actividades de la continuidad del negocio, procurando mostrar de forma práctica como realizar el análisis BIA. El siguiente paso es determinar las actividades críticas y realizar el análisis de impacto de incidencias poniéndonos en el peor de los casos posibles que tenga en cuenta toda la infraestructura necesaria para el desarrollo de la actividad.

Para organizar una correcta recolección de información deberemos construir un sistema de evaluación sistemático con escalas de tiempo y evaluación cualitativa y cuantitativa del impacto que nos permitan posteriormente establecer los criterios adecuados.

En este sentido, se debe tener en cuenta toda la infraestructura y servicios necesarios versus su impacto en los usuarios tanto internos como externos.

DISEÑO DE LA SOLUCION

4.1 Declaración de política de continuidad de negocio

La política global de continuidad de negocio que se implantará, publicará y difundirá en la organización contemplando los siguientes acuerdos.

ALCANCE: Esta política aplica para todo el personal que labore en la entidad educativa superior del sector privado con el fin de garantizar la continuidad de negocio, en caso de un evento que afecte la operación normal.

INTRODUCCION: La política de continuidad de negocio tiene como objetivo proteger los procesos críticos del negocio, contra desastres o fallas mayores, junto con las posibles consecuencias que se puedan tener, como pérdidas de tipo financiero, credibilidad, productividad, etc. debido a la no disponibilidad de los recursos de la organización. El Plan de Recuperación de Desastres, busca mitigar el riesgo a dichas fallas o desastres, mediante un plan que permita la pronta recuperación de la operación, en caso de presentarse algún evento que afecte el flujo normal de las actividades de la universidad.

OBJETIVO: Evitar interrupciones a los procesos críticos del negocio como consecuencia de fallas o desastres.

ENUNCIADO DE LA POLÍTICA GENERAL: Debido a que cualquier interrupción en los procesos de negocio afecta a la operación, es responsabilidad de las directivas de la organización aprobar un Plan de Recuperación de Desastres, que cubra las actividades esenciales y críticas de la entidad educativa superior del sector privado, así como garantizar la operación de todos los procesos vitales para la organización que son soportados por el área tecnológica.

POLITICAS RELACIONADAS: Políticas de respaldo y restauración, Política de Seguridad Física de Data Center.

ROLES Y RESPONSABILIDADES: Esta política debe ser aprobada por las directivas de la organización, luego del estudio previo y detallado de sus posibles consecuencias, con el fin de garantizar la continuidad de negocio en caso de un evento que afecte la operación normal de los procesos críticos que son soportados por el área tecnológica.

SANCIONES: En este caso especial, si las directivas de la organización se comprometen a desarrollar el plan, será responsabilidad de ellos, no faltar a este compromiso y tener en cuenta que al no realizar dicho plan, la compañía pudiera estar expuesta a procesos legales y contractuales, que pudieran poner en riesgo el futuro de la operación de la entidad educativa.

REVISION DE LA POLITICA: Esta política debe ser modificada si existieran cambios en los procesos de negocio de la organización o en su infraestructura tecnológica, de no haber cambios, se debe realizar su revisión anualmente.

ESTRUCTURA ORGANIZACIONAL

Define los equipos de trabajo involucrados en el esfuerzo de la recuperación de los servicios brindados por la Sala de Servidores en caso de contingencia y sus responsabilidades asociadas. Las responsabilidades se desglosan en categorías de antes, durante y después de la contingencia.

Se muestra un listado con los integrantes de los equipos y sus números telefónicos en las oficinas, de su casa y cualquier otro teléfono alterno para su localización. La organización para la recuperación es la siguiente.

- Equipo Gerencial de la Contingencia
    - Equipo Coordinador de la Contingencia
        - Equipo de Sistemas
        - Equipo de Apoyo Administrativo
        - Equipo de Usuarios

A continuación, se muestra la interacción de los equipos y sus integrantes, es importante recalcar que la organización también debe formar parte del plan general de BCP.

- Equipo Gerencial de la Contingencia:
  - Director de Administración y Finanzas
  - Jefe del Departamento de Informática
- Equipo Coordinador de la Contingencia
  - Líder de la Secretaría General
  - Jefe de RH
  - Líder de Área de Finanzas
- Equipo de Usuarios
  - Líder de Unidad Técnicos Legislativos
  - Líder de Unidad de Servicios Parlamentarios
  - Líder de Diario de los Debates
  - Líder de Área Contable
- Equipo de Apoyo Adminsitrativo
  - Jefe de Compras y Servicios Generales
  - Jefe de Mantenimiento

EJECUCION DEL PLAN DE RECUPERACION

Se muestra a continuación el plan de recuperación por riesgo

Sitio	Riesgo	Acción Preventiva	Acción Correctiva
Site Principal	Incendio	Instalación de Alarma de incendios	Recuperación de equipos Respaldo de información fuera del site principal
	Huracán	Revisión de ductos de ventilación	Respaldo de información fuera del site principal
	Descarga Eléctrica	Instalación de UPS y No break Revisión de instalaciones eléctricas	Recuperación de equipos Respaldo de información fuera del site principal

	Intrusión externa ó ataque informático	Contratación de servicio WAF Instalación de Firewall Uso de contraseñas de alto nivel	Respaldo de información fuera del site principal Servidores en modo offline
Site piso 7	Incendio	Instalación de Alarma de incendios	Recuperación de equipos Respaldo de información fuera del site principal
	Huracán	Revisión de ductos de ventilación	Respaldo de información fuera del site principal
	Descarga Eléctrica	Instalación de UPS y No break Revisión de instalaciones eléctricas	Recuperación de equipos Respaldo de información fuera del site principal
Site Edificio Norte	Incendio	Instalación de Alarma de incendios	Recuperación de equipos Respaldo de información fuera del site principal
	Huracán	Revisión de ductos de ventilación	Respaldo de información fuera del site principal
	Descarga Eléctrica	Instalación de UPS y No break Revisión de instalaciones eléctricas	Recuperación de equipos Respaldo de información fuera del site principal

CONCLUSIONES

La planificación es crítica a la hora de evitar y enfrentar los desastres informáticos. Para ello, es necesario que la organización tenga en cuenta en el día a día los diferentes procesos para la continuidad de las operaciones, como almacenamiento, protección de datos, recuperación efectiva de información, entre otros, que sean fuertes, pero a la vez fáciles de incorporar e implementar, asegurando así la permanencia, integridad y disponibilidad de la información.