**CASO PRÁCTICO**

De acuerdo al caso planteado, podemos concluir que la escuela politécnica Innovativa requiere la implementación de un plan de contingencia, pero específicamente nos enfocaremos en plantear un plan de respaldo, por lo que seguiremos la siguiente estructura:

1. ***Propósito y alcance:***

Lo que deseamos alcanzar en el presente plan es implementar las acciones y procesos necesarios para asegurar la disponibilidad, la integridad y la recuperación de los datos esenciales de Innovativa. El plan se centra en abordar las carencias actuales en el ámbito de TI de Innovativa, especialmente en lo referente a la ausencia de un plan de contingencia y la falta de un sistema de respaldo apropiado.

El plan tiene un alcance amplio que involucra a todas las áreas de la empresa Innovativa que dependen de los recursos de TI, abarcando tanto los sistemas de hardware y software como los datos almacenados en ellos. Esto implica a todos los departamentos y empleados que utilizan la plataforma tecnológica de Innovativa en sus tareas diarias.

1. ***Política de respaldo:***

***Aplicación de la norma ISO 27001***

La norma ISO/IEC 27001 es un estándar internacionalmente reconocido para la gestión de la seguridad de la información.

Dado que Innovativa es una institución que maneja información sensible y crítica, la implementación de la norma ISO 27001 permitirá proporcionar beneficios significativos en términos de la protección de la información, la gestión de riesgos y el establecimiento de controles de seguridad adecuados.

Al aplicar la norma 27001, la institución podría:

1. Establecer un marco de gestión de la seguridad de la información: La norma proporciona un marco estructurado para establecer, implementar, operar, monitorear, revisar, mantener y mejorar continuamente el sistema de gestión de la seguridad de la información (SGSI).
2. Identificar y evaluar riesgos: ISO 27001 requiere la identificación y evaluación de los riesgos de seguridad de la información. Esto permitiría a “Innovativa” comprender las amenazas y vulnerabilidades existentes en su entorno de TI y tomar medidas para mitigarlos.
3. Implementar controles de seguridad: Esta norma proporciona una lista de controles de seguridad que pueden ser aplicados en función de los riesgos identificados. Estos controles incluyen aspectos relacionados con el respaldo de datos, la seguridad física, la gestión de incidentes y la continuidad del negocio, entre otros.
4. Establecer un ciclo de mejora continua: La norma ISO 27001 se basa en el enfoque de mejora continua del SGSI. Esto implica la revisión y mejora regular de los controles de seguridad, así como la aplicación de medidas correctivas y preventivas.

***Ley 28551***

Ley que establece la obligación de elaborar y presentar Planes de Contingencia, Gestop, Asesorías y Consultorías de Sistemas de Gestión.

Tiene como objetivo la reducción de riesgos y la gestión de desastres en el país. Aborda aspectos relacionados con la seguridad y la protección de la población y los activos en caso de desastres.

En el caso de Innovativa, podría aplicarse en términos generales para fortalecer la gestión de riesgos y la preparación ante posibles desastres, ya que como nos lo detalla, la institución no cuenta con un plan de contingencia que permita resolver los problemas que se susciten.

1. ***Copias de seguridad de datos que se realizan:***

De acuerdo al caso, podemos concluir que la institución no cuenta con un plan de contingencia, por lo que, de suceder cualquier tipo de incidente, ya sea robo, daño en los equipos o cualquier otro incidente, la información se perdería. Por lo tanto, proponemos priorizar el resguardo de la información sensible, de manera que se sugiere:

* ***Identificación de los datos críticos:*** Realizar un inventario de los datos críticos de Innovativa que deben ser respaldados. Esto puede incluir información institucional, proyectos en curso, documentos importantes, bases de datos, correos electrónicos, entre otros.
* ***Definición de la frecuencia de respaldo:*** Determinar la frecuencia con la que se realizarán las copias de seguridad. Esto dependerá de la criticidad de los datos y la frecuencia con la que se actualizan. Por ejemplo, los datos que cambian con mayor frecuencia pueden requerir copias de seguridad diarias, mientras que otros datos menos volátiles pueden necesitar copias de seguridad semanales o mensuales.
* ***Selección de tipos de respaldo:*** Esto puede incluir la utilización de sistemas de respaldo en la nube, dispositivos de almacenamiento externo, servidores de respaldo internos, entre otros. Es importante considerar la escalabilidad, la seguridad y la confiabilidad de los métodos seleccionados.
* ***Política de retención de datos:*** Establecer una política clara de retención de datos para determinar durante cuánto tiempo se conservarán las copias de seguridad. Esto debe basarse en las necesidades operativas y legales de la institución. Por ejemplo, es posible que se requiera retener copias de seguridad durante un período específico para cumplir con las regulaciones o requisitos de auditoría.
* ***Almacenamiento seguro de copias de seguridad:*** Garantizar que las copias de seguridad se almacenen en un lugar seguro y protegido. Esto implica implementar medidas de seguridad física, como el acceso restringido a las áreas de almacenamiento, y medidas de seguridad lógica, como la encriptación de datos. Además, se debe considerar la ubicación geográfica de los sitios de respaldo para evitar riesgos compartidos con las instalaciones principales.
* ***Pruebas periódicas de restauración:*** Realizar pruebas periódicas de restauración para verificar la integridad de las copias de seguridad y la capacidad de recuperación de datos. Estas pruebas ayudarán a identificar cualquier problema o falla en las copias de seguridad y permitirán corregirlos antes de que sea necesario restaurar datos en una situación de emergencia.
* ***Capacitación del personal:*** Capacitar al personal sobre los procedimientos de respaldo y restauración de datos. Esto incluye brindarles información sobre cómo realizar copias de seguridad, cómo acceder a las copias de seguridad cuando sea necesario y cómo restaurar los datos de manera adecuada.

1. ***Recuperación de datos:***

Luego de establecer las políticas para las copias de seguridad, pasamos a lo concerniente con la recuperación de datos. En este apartado debemos considerar:

* ***Procedimientos de recuperación:*** Se debe establecer procedimientos claros y detallados para la recuperación de datos en caso de pérdida, corrupción o interrupción del sistema.
* ***Priorización de la recuperación:*** Identificar los datos y sistemas críticos que deben ser recuperados con mayor prioridad. Esto implica evaluar el impacto del tiempo de inactividad en los diferentes sistemas y servicios de la institución y establecer un orden de recuperación basado en la importancia y la urgencia.
* ***Pruebas de recuperación:*** Realizar pruebas periódicas de recuperación para verificar la efectividad de los procedimientos y la integridad de las copias de seguridad. Esto asegurará que las copias de seguridad estén actualizadas y que se puedan restaurar correctamente en caso de una situación real de pérdida de datos.
* ***Infraestructura de recuperación:*** Establecer una infraestructura de recuperación adecuada que incluya servidores de respaldo, sistemas de almacenamiento (físico y en la nube), software de recuperación y otros recursos necesarios para restaurar los datos y sistemas de manera eficiente.
* ***Roles y responsabilidades:*** Definir claramente los roles y responsabilidades del personal involucrado en el proceso de recuperación de datos. Esto incluye identificar a los responsables de iniciar y supervisar el proceso de recuperación, así como a aquellos encargados de la comunicación interna y externa durante la recuperación.
* ***Evaluación y mejora continua:*** Realizar evaluaciones periódicas del proceso de recuperación de datos para identificar áreas de mejora y realizar ajustes según sea necesario. Esto asegurará que el proceso de recuperación se mantenga actualizado y sea eficaz en caso de una situación de pérdida de datos.

1. ***Revisión y mantenimiento del plan:***

La revisión constante del plan de respaldo en la institución garantiza su adaptabilidad a las necesidades cambiantes, protegiendo la información y asegurando la continuidad del negocio frente a amenazas y avances tecnológicos. Se propone:

* ***Programa de revisión periódica:*** Establecer un programa regular de revisión del plan de respaldo y contingencia. Esto puede incluir revisiones trimestrales, semestrales o anuales, dependiendo de las necesidades y la evolución de la infraestructura tecnológica de Innovativa.
* ***Evaluación de riesgos:*** Realizar evaluaciones periódicas de riesgos para identificar posibles amenazas y vulnerabilidades que puedan afectar la efectividad del plan de respaldo. Esto puede incluir cambios en el entorno tecnológico, nuevas amenazas de seguridad, actualizaciones regulatorias, entre otros factores.
* ***Actualización de contactos y responsabilidades:*** Revisar y actualizar regularmente la lista de contactos de emergencia, así como los roles y responsabilidades del personal involucrado en la ejecución del plan de respaldo. Esto asegurará que la información de contacto sea precisa y que todas las partes involucradas estén al tanto de sus responsabilidades durante una situación de emergencia.
* ***Actualización de procedimientos y documentación:*** Revisar y actualizar los procedimientos y la documentación relacionada con el plan de respaldo y contingencia. Esto puede incluir cambios en los sistemas tecnológicos, actualización de instrucciones de respaldo y recuperación, actualización de políticas y procedimientos, entre otros aspectos relevantes.
* ***Capacitación y concientización:*** Realizar capacitaciones periódicas para el personal sobre el plan de respaldo. Esto ayudará a garantizar que todos los trabajadores estén familiarizados con los procedimientos, sepan cómo actuar en caso de una situación de emergencia y comprendan la importancia de la protección de la información.
* ***Evaluación de proveedores y servicios:*** Evaluar regularmente los proveedores de servicios relacionados con el plan de respaldo, como proveedores de almacenamiento en la nube, servicios de copia de seguridad, entre otros. Esto asegurará que los proveedores sigan cumpliendo con los requisitos de la institución en términos de seguridad, confiabilidad y cumplimiento normativo.
* ***Mejora continua:*** Fomentar una cultura de mejora continua en relación con el plan de respaldo y contingencia. Esto implica recopilar comentarios y sugerencias del personal, analizar las lecciones aprendidas de situaciones de emergencia anteriores y realizar ajustes en el plan y los procedimientos en base a estas lecciones aprendidas.