PLAN DE CONTINUIDAD DE NEGOCIO TI

Tecnología e Información

Fecha de elaboración: Cali, noviembre,2023

Introducción

INTENALCO es una Institución Educativa de carácter oficial nacional, Técnica Profesional soluciones adaptadas a las cambiantes dinámicas en las empresas. Esta adaptación se basa en la excelencia y la gestión de riesgos, que son pilares clave para la sostenibilidad de la organización. La entidad cuenta con un equipo interdisciplinario que se centra en la innovación, el enfoque ágil y la tecnología para lograr sus objetivos. El departamento de TIC es fundamental para el funcionamiento y éxito de la entidad. Esto subraya la importancia de garantizar la continuidad de los sistemas de TIC, la seguridad de la información y la gestión de riesgos cibernéticos, especialmente dado el enfoque en la eficiencia y la innovación.

Objetivo

- ✓ Garantizar la continuidad de las operaciones críticas de TIC en la entidad de educación superior, minimizando los impactos de posibles interrupciones y asegurando la disponibilidad de servicios tecnológicos esenciales.

- ✓ Implementar estrategias y medidas preventivas para minimizar los impactos de posibles interrupciones y garantizar la disponibilidad de los servicios tecnológicos esenciales.

- ✓ Asegurar que, incluso en situaciones adversas, la institución educativa pueda seguir operando sus servicios de TI de manera efectiva, protegiendo la integridad, confidencialidad y disponibilidad de la información crítica y manteniendo la eficiencia de sus operaciones.

Alcance del Plan

Para INTENALCO es importante garantizar que siempre este en disponibilidad los:

1. **Sistema de Gestión de Seguridad de la Información (SGSI):** Dado que INTENALACO trabaja con información sensible, el SGSI es esencial para garantizar la protección de los datos y el cumplimiento de las normativas de seguridad.
    a. **Sistema de Registro Académico SIGA**
    b. **Sistema de Permanencia Estudiantil ADVISER**
    c. **Sistema Financiero CG-UNO**
    d. **Sistema de Registro Bibliotecario KOHA**

e. **Sistema de Respaldos**
f. **Sistema de Directorio Activo**

2. **Sistema de Gestión de Personal:** Incluyendo información de empleados, afiliaciones y asignaciones.

3. **Sistema de Comunicaciones:** Los servicios de comunicación, como correo electrónico, telefonía y sistemas de comunicación interna, son cruciales para la coordinación y la respuesta a emergencias.

4. **Sistemas de Almacenamiento y Respaldo de Datos:** Para garantizar la integridad y disponibilidad de los datos críticos en todo momento.

5. **Sistemas de Información de Clientes:** Para acceder a la información de los clientes y brindar un servicio eficiente.

6. **Sistema de Video Vigilancia:** La capacidad de monitorear y grabar video en tiempo real es esencial para la supervisión y seguridad de las operaciones.

Evaluación de Riesgos

Identificación de las amenazas y riesgos a los que se enfrenta el área de TIC en INTENALCO:

1. **Brechas de seguridad:** Esto incluye ataques de hackers, malware, ransomware y otras amenazas cibernéticas que podrían comprometer la seguridad de los sistemas y datos de TIC.

2. **Interrupción del Suministro Eléctrico**: Cortes de energía inesperados que pueden dejar los sistemas de TIC inoperables.

3. **Fallas de Hardware:** El mal funcionamiento de servidores, equipos de red o software crítico podría causar interrupciones.

4. **Fallas de Software:** Posibilidad de fallas Software renovación de licenciamientos y renovación de contratos con los softwares críticos (mantenimientos y soportes).

5. **Deterioro de Rendimiento**: La disminución del desempeño o funcionamiento de sistemas, procesos o actividades relacionadas con la

tecnología, como consecuencia de diversos riesgos. Estos riesgos pueden surgir en el contexto de la implementación, operación y mantenimiento de tecnologías de la información y comunicación, infraestructuras tecnológicas, software, hardware, y otros componentes tecnológicos.

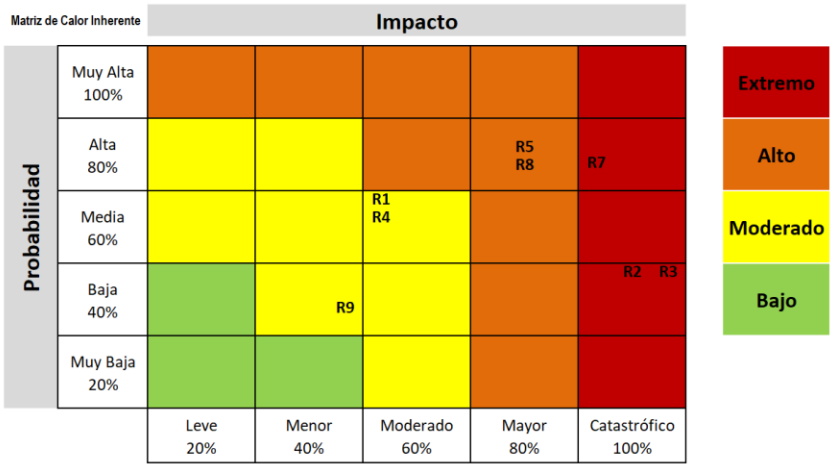
6. **Incumplimiento normativo:** Riesgo de no cumplir con las leyes y regulaciones relacionadas con la privacidad y seguridad de la información o por cambios en las regulaciones gubernamentales que podrían afectar los requisitos de seguridad de la información y la operación de TIC.

7. **Perdida de datos:** Posibilidad de pérdida de información crítica debido a fallos en los sistemas o acciones no autorizadas.

8. **Amenazas Físicas:** Intrusión, robo o vandalismo en las instalaciones de TIC.

9. **Riesgos de Terceros:** Problemas con proveedores de servicios de TIC o subcontratistas que puedan afectar la entrega de servicios.

En la identificación de los riesgos que se evaluaron los eventos anteriores que puede presentar la entidad dio como resultado el siguiente mapa de calor.



Estrategias de Continuidad

Se indispensable desarrollar las siguientes estrategias de continuidad para mitigar los posibles impactos adversos identificados y así garantizar la continuidad del

negocio en el área de Tecnologías de la Información (TI) asegurarse de que las estrategias de continuidad estén alineadas con los objetivos y la capacidad financiera de la institución. Considerar la implementación de pruebas regulares para las estrategias de continuidad, como simulacros de recuperación de desastres.

- ✓ ***Respaldos y recuperación de datos:***

  - Implementar un plan integral de respaldo de datos que incluya copias periódicas de todos los datos críticos. Utilizar soluciones de respaldo automatizadas y almacenamiento en ubicaciones seguras y fuera del sitio.
  - Establecer procedimientos claros y probados para la recuperación rápida de datos en caso de pérdida o corrupción.
  - Definir claramente los intervalos de respaldo y los criterios para determinar qué datos se consideran críticos.
  - Asegurar que los procedimientos de recuperación sean probados periódicamente.

- ✓ ***Infraestructura Redundante:***

  - Implementar sistemas y servicios con redundancia para reducir el riesgo de interrupciones debido a fallos de hardware o software.
  - Utilizar servidores y sistemas de almacenamiento replicados en ubicaciones geográficas distintas para garantizar la disponibilidad continua.
  - Detallar cómo se realizará la supervisión continua de la infraestructura redundante para garantizar su eficacia.
  - Considerar la posibilidad de mantener actualizadas las copias de datos fuera del sitio en tiempo real.

- ✓ ***Planificación de Recuperación ante Desastres (DRP):***

  - Desarrollar un plan de recuperación ante desastres que aborde situaciones como incendios, inundaciones, terremotos, entre otros.
  - Identificar ubicaciones alternativas y equipamiento necesario para restablecer rápidamente las operaciones de TIC en caso de un desastre.
  - Incluir detalles específicos sobre la ubicación y disponibilidad de los recursos necesarios para la recuperación después de un desastre.

✓ ***Contingencia de Personal:***

- Identificar roles y responsabilidades clave en el área de TIC durante situaciones de crisis.
- Establecer protocolos para garantizar la disponibilidad del personal necesario y su capacidad para trabajar de forma remota si es necesario.
- Establecer protocolos claros para la comunicación y coordinación del personal durante situaciones de crisis.
- Considerar la posibilidad de realizar ejercicios de entrenamiento regulares para el personal clave.

✓ ***Seguridad Cibernética:***

- Fortalecer las medidas de seguridad cibernética para prevenir ataques y minimizar los impactos en caso de incidentes.
- Implementar sistemas de detección de intrusiones, firewalls actualizados, y realizar auditorías de seguridad de manera regular.

✓ ***Capacidades de Trabajo Remoto:***

- Facilitar la capacidad de trabajo remoto para el personal de TIC. Esto implica asegurar conexiones seguras a la red, acceso a herramientas esenciales y la posibilidad de colaboración en línea.
- Proporcionar orientación y capacitación a los empleados sobre prácticas seguras de trabajo remoto.
- Asegurarse de que se proporcionen recursos suficientes para facilitar el trabajo remoto, como acceso seguro a la red y herramientas colaborativas.

✓ ***Simulacros y Entrenamiento:***

- Realizar simulacros periódicos para probar la efectividad del plan de continuidad y la capacidad del personal para responder eficientemente a situaciones de crisis.
- Proporcionar entrenamiento regular para el personal, actualizando sus conocimientos sobre procedimientos de continuidad y medidas de seguridad.
- Programar simulacros periódicos y documentar lecciones aprendidas para mejorar continuamente el plan.

✓ ***Colaboración con Proveedores:***

- Establecer acuerdos de nivel de servicio (SLA) con proveedores de servicios críticos, asegurando que tengan sus propios planes de continuidad y que estén alineados con los objetivos de la institución educativa.
- Mantener una lista actualizada de contactos de proveedores clave y establecer protocolos de comunicación en caso de interrupciones.
- Establecer un proceso para revisar y actualizar los SLA con proveedores de servicios críticos de manera regular.

✓ ***Actualización Continua del Plan***:

- Revisar y actualizar el plan de continuidad regularmente para reflejar cambios en la infraestructura, tecnologías emergentes y lecciones aprendidas de eventos pasados.
- Asegurarse de que el personal esté al tanto de las actualizaciones y capacitado en los cambios realizados.
- Asignar responsabilidades claras para la revisión y actualización del plan, y establecer un calendario regular para estas actividades.

✓ ***Comunicación Efectiva:***

- Establecer un plan de comunicación detallado que incluya cómo informar a las partes interesadas en caso de interrupciones.
- Utilizar canales de comunicación alternativos y mantener actualizada la información de contacto de emergencia.
- Detallar los canales de comunicación específicos a utilizar durante una interrupción, y asegurarse de que la información de contacto esté siempre actualizada.

Implementar estas estrategias de continuidad permitirá a la entidad de educación superior enfrentar diversos escenarios de interrupción y asegurar la disponibilidad y funcionalidad continua de sus servicios críticos de TIC.