Gobierno del Estado de Sonora | Instituto Sonorense de Infraestructura Educativa

PLAN DE CONTINUIDAD DEL NEGOCIO Y ANÁLISIS DE IMPACTO AL NEGOCIO

2021

Índice

1. Introducción

Derivado de una observación de la Auditoria Superior de la Federación en la que se analizó el control Interno instrumentado por el Instituto Sonorense de Infraestructura Educativa, referente a que esta Institución no cuenta formalmente con un documento de plan de recuperación de desastres en el cual incluya datos, hardware y software críticos asociados directamente al logro objetivos y metas institucionales. Como parte de las acciones implementadas para atender dicha observación, el ISIE elaboró el Plan de Continuidad al Negocio y Análisis de Impacto al Negocio.

Ya que hoy en día los sistemas de información son el alma de organizaciones, empresas y entidades, el grado de responsabilidad incide en los sistemas, datos e información encaminados al logro de los objetivos internos, estos se pueden mejorar y mantenerse teniendo una adecuada sistematización y documentación.

El tratamiento de la información abarca aspectos que van desde el manejo de documentos en medio físico como el proceso de almacenaje y recuperación conocido también como proceso de gestión documental, hasta los sistemas de información que tenga la organización o sistemas externos a los que esté obligada a reportar información, pasando por aspectos tan importantes como la forma de almacenamiento de los datos digitales, modelos de respaldo de información y planes de contingencia o de continuidad del negocio, si existen, claro está, incluyendo además los sistemas físicos de protección y accesibilidad a sitios o áreas restringidas.

Es por esto que los activos de información han pasado a formar parte de la actividad cotidiana de organizaciones e individuos; los equipos de cómputo almacenan información, la procesan y la transmiten a través de redes y canales de comunicación, abriendo nuevas posibilidades y facilidades a los usuarios, pero se deben considerar nuevos paradigmas en estos modelos tecnológicos y tener muy claro que no existen sistemas cien por ciento seguros, porque el costo de la

seguridad total es muy alto (aunque en la realidad no es alcanzable idealmente), y las organizaciones no están preparadas para hacer este tipo de inversión.

Se tiene la falsa percepción de que la seguridad de la información es una tarea imposible de aplicar, en realidad, con esfuerzo, el conocimiento necesario y el apoyo constante de las directivas se puede alcanzar un nivel de seguridad razonable, capaz de satisfacer las expectativas de seguridad propias.

El Instituto Sonorense de Infraestructura Educativa es una entidad en crecimiento que debe involucrar dentro de sus procesos buenas prácticas encaminadas a la protección de la información; razón por la cual es necesario el desarrollo del análisis de riesgo de la seguridad de la información aplicado a cada uno de los activos de información.

Cabe mencionar que en este documento se desarrollan los componentes fundamentales del Plan de Recuperación de Desastres que son el Plan de Continuidad del Negocio y el Plan de Impacto del Negocio con sus respectivos elementos.

2. Contexto

El Instituto Sonorense de Infraestructura Educativa, no tiene un sistema de seguridad de la información que permita la gestión de vulnerabilidades, riesgos y amenazas a las que normalmente se ve expuesta la información presente en cada uno de los procesos internos; asimismo, no se tienen estandarizados controles que lleven a mitigar delitos informáticos o amenazas a los que están expuestos los datos comprometiendo la integridad, confidencialidad y disponibilidad de la información.

Existen procedimientos creados subjetivamente por iniciativa y experiencia de los miembros del equipo TIC; por ejemplo, no existe una política de uso de claves de usuario, en los servidores se realiza el cambio de claves de acceso a criterio del personal responsable de cada uno de ellos sin una periodicidad y bitácora definida; los administrativos y docentes no hacen uso de claves de acceso, por lo que cualquier persona puede tener acceso a los equipos de cómputo que se les ha asignado, no existe equipo suficiente de respaldo de información (BACK-UP), no se cuenta con protección suficiente en caso de cortes de energías o hasta percances externos climáticos.

Para evitar riesgos mayores es necesario adoptar acciones que permitan integrar dentro de sus sistemas, buenas prácticas y recomendaciones de seguridad informática, resultado del análisis de continuidad del negocio; derivado de estas acciones también se evitaría que el ISIE sea víctima de daños permanentes en su infraestructura informática que obstaculicen su normal funcionamiento como lo pueden ser intrusiones, modificación y/o robo de información, denegación de servicios, robo de equipo de cómputo, entre otros.

3. Justificación

Hoy en día el Instituto Sonorense de Infraestructura Educativa, tiene una infraestructura tecnológica en crecimiento, de la cual dependen muchos de los procesos, dependencias y el funcionamiento administrativo. Gran parte de la información institucional se encuentra en los equipos del personal administrativo y operativo, otra parte en los buzones de correo, también existe información en formato físico y por último la que se encuentra almacenada en sistemas de información.

El Instituto Sonorense de Infraestructura Educativa necesita contar con un Plan para proteger la continuidad de las operaciones, salvaguardar la información que se almacena dentro de su infraestructura tecnológica, por la cual se ha optado por una metodología en la que garantice que sus procesos, políticas y controles aseguren el funcionamiento continuo del flujo de información y se pueda optimizar, garantizar sea confiable, disponible y cuente integridad dicha información.

Este es uno de los retos que debe asumir la institución para estar acorde a los modelos y estándares actuales; para ello es necesario empezar con la ejecución del Plan de Continuidad del Negocio, que permitirá mantener un modelo estable logrando un valor agregado y posicionamiento a nivel regional.

Los beneficios que esto conlleva serían los siguientes:

• Identifica los diversos eventos que pueden impactar sobre la continuidad de las operaciones y su impacto sobre el Instituto.

• Obliga a conocer los tiempos críticos de recuperación, para volver al estado anterior del Instituto.

• Clasifica los activos para priorizar su protección en caso de un incidente.

• Identifica aquellos puntos más débiles de la infraestructura, que son susceptibles de sufrir un incidente y afectar la continuidad del negocio.

• Dispone de un plan logístico de rápida actuación y respuesta, en caso de sufrir un incidente.

• Evaluación técnica de riesgos asociados a la continuidad, evaluación de alternativas y estrategias de minimización de riesgos.

• Mapeo critico de los recursos mínimos requeridos en la continuidad de los procesos del Instituto.

4. Objetivos

4.1. General

Realizar el Plan de Continuidad que permita generar controles para minimizar la probabilidad de ocurrencia e impacto de los riesgos asociados con las vulnerabilidades y amenazas que puedan ocurrir en la infraestructura y seguridad de la información existentes en el Instituto Sonorense de Infraestructura Educativa.

4.2. Específicos

- Identificar y clasificar los activos de información presentes en el Instituto Sonorense de Infraestructura Educativa.

- Sugerir mecanismos de control y gestión que minimicen las vulnerabilidades encontradas en el estudio del análisis de riesgos realizado.

- Elaborar un informe de recomendaciones donde se muestre los hallazgos que permita definir un Sistema de seguridad ajustado a la realidad del Instituto Sonorense de Infraestructura Educativa.

- Generar una matriz de riesgos donde se pueda identificar fácilmente las prioridades en las cuales cubrir cada una de manera prioritaria

- Elaborar un Plan Estratégico para minimizar riesgos e impactos a la Institución.

5. Marco organizacional

Elementos a contemplar para la recopilación de información acerca de la Institución y lo que contiene conforme a Políticas, Metodologías, Infraestructura, Hardware, Software y Documentación que aportara al Desarrollo del Plan de Continuidad y establecer normas reales conforme a sus activos actuales para plasmarlos lo más efectivamente posible.

Diseño Metodológico:

Es el marco estratégico constituido por los métodos, técnicas(procedimientos), e instrumentos que se emplearan en la ejecución del proyecto de investigación para poner a prueba la hipótesis, alcanzar los objetivos de investigación, y así dar una respuesta al problema de la investigación.

Informe Técnico:

Es la exposición por escrito de las circunstancias observadas en el examen de la cuestión que se considera, con explicaciones detalladas que certifiquen lo dicho.

Desarrollo del Plan de Continuidad:

Etapa Final del Marco Organizacional en el que se pretende recopilar con el Diseño Metodológico y el Informe Técnico tener las herramientas suficientes para realizar dicho Plan de Continuidad en ISIE.

5.1. Introducción al BCP

La Continuidad del Negocio o BCM (Business Continuity Management) se define como la capacidad estratégica y táctica que permite a las organizaciones realizar la planeación para responder, recuperar y restaurar organizadamente sus procesos críticos ante incidentes o contingencias que puedan presentarse; tomando en cuenta el tiempo y recursos requeridos para mantener su operación en un tiempo y nivel aceptable; tal y como se muestra en el siguiente diagrama:

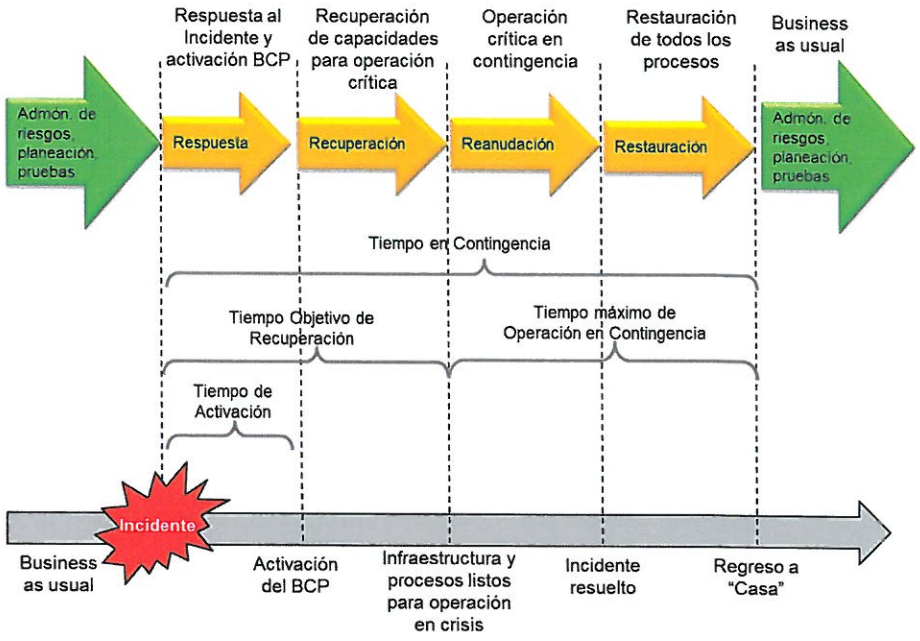


Figura 1. Proceso de Continuidad del Negocio

Derivado de la metodología COBIT (Control Objectives for Information and related Technology) para cubrir los siguientes objetivos de la Continuidad del Negocio:

- Asegurar la sobrevivencia de la organización.
- Proporcionar protección a los activos
- Proporcionar medidas preventivas y mitigar impactos
- Tomar el control en una crisis
- Mantener la imagen pública y la reputación
- Cumplir con regulaciones

5.2. ANALISIS DE RIESGOS

5.2.1. Componentes a Considerar en Análisis de Riesgos (RA)

5.2.1.1. Entrevistado/Área

Persona a la cual se le hará una entrevistado y este a cargo de un área específica o que contenga el Rol más importante dentro del Departamento para así recabar información más concreta.

5.2.1.2. Escenario de Riesgo

- Activo. (Un activo es algo que tiene valor para la institución y por lo tanto tiene que protegerse. Los activos incluyen toda la información y soporte que la organización requiera para conducir el negocio. Por ejemplo: Hardware, Software, Redes)

- Amenaza. (Algo que pueda causar daños a los Sistemas de Información de la institución, Por ejemplo: Robos, errores de operación o virus)

- Vulnerabilidad. (Partes susceptibles a algún ataque o daño ya sea en Software o Hardware).

5.2.1.3 Perdida de CID (Confidencialidad, Integridad y Disponibilidad)

- Confidencialidad. La información de la institución nunca debería ser accesible a los usuarios sin la autorización correspondiente.

- Integridad. Consiste en preservar la información completa y exacta.

- Disponibilidad. La información está disponible a los usuarios autorizados cuando estos la requieran.

Estas se clasificarán dependiendo si es confiable, integra o es disponible:

NINGUNA.

PARCIAL.

COMPLETA.

5.2.1.4 Evaluación de Riesgo

- Probabilidad. Estimación cualitativa de que suceda algún daño dependiendo si es **BAJO**, **MEDIO**, **ALTO**.

- Impacto. Que tanto repercute en la institución el daño que vaya a surgir dependiendo si es, **BAJO**, **MEDIO**, **ALTO**.

5.2.1.5. Nivel de Riesgo Actual.

Ponderación entre la Probabilidad y el Impacto de los riegos a considerar en el Análisis según la más baja evaluación de ellas del respectivo riesgo.

5.3. ANALISIS DE IMPACTO AL NEGOCIO (BIA)

La fase de Análisis de Impacto del Negocio BIA (Bussiness Impact Analysis) Por sus siglas en inglés), permite identificar con claridad los procesos misionales de cada entidad y analizar el nivel de impacto con relación a la gestión del negocio.

Cada entidad debe disponer de un documento que permita identificar todas las áreas críticas del negocio y sea un instrumento para garantizar la medición de la magnitud del impacto operacional y financiero de la entidad, al momento de presentarse una interrupción. En esta etapa, el análisis de impacto del negocio, debe poder clarificar los siguientes requerimientos:

- Identificar las funciones y procesos importantes para la supervivencia de la entidad al momento de la interrupción, esto es tener en cuenta cuales de los procesos son claves para que entren en operación rápidamente asignándoles la mayor prioridad posible, frente a los de menor prioridad; debe quedar claro que para los procesos identificados como no tan prioritarios se deben preparar también planes de recuperación.

- Revisar las consecuencias operacionales, que una interrupción tendrá en los procesos considerados de alta prioridad.

- Estimar los tiempos de recuperación, en razón a las posibles alteraciones de los procesos considerados de alta prioridad para el funcionamiento de las infraestructuras de TI.

5.3.1. REQUERIMIENTOS DE TIEMPO DE RECUPERACIÓN

Como parte del plan de continuidad del negocio de una organización, es importante poder definir y entender los requerimientos de tiempo necesarios para recuperar a las entidades de servicios que han sido interrumpidos por diferentes motivos dentro de la organización; estos requerimientos obedecen a varios componentes que hacen referencia concreta al tiempo disponible en la cual una organización puede recuperarse oportuna y ordenadamente a las interrupciones en los servicios e infraestructuras de TI. Los componentes se describen a continuación:

- **MTD** (Maximun Tolerable Downtime) o Tiempo Máximo de Inactividad Tolerable. Espacio de tiempo durante el cual un proceso puede estar inoperante hasta que la empresa empiece a tener pérdidas y colapse.

- **RTO** (Recovery Time Objective) o Tiempo de Recuperación Objetivo. Es el tiempo transcurrido entre una interrupción y la recuperación del servicio. Indica el tiempo disponible para recuperar sistemas y recursos interrumpidos.

- **RPO** (Recovery Point Objective) o Punto de Recuperación Objetivo. Es el rango de tolerancia que la entidad puede tener sobre la pérdida de datos y el evento de desastre.

- **AREA**. El área de la institución donde se implementará el BIA.

- **RESPONSABLE.** Identificador único del responsable que se encuentra registrado en la Lista de Contactos.

- **PROCESOS**. Proceso del Área de la Institución responsable donde se realizará el BIA.

- **RIESGOS**. Consecuencias aparentes que podrían presentarse daños o errores en los procesos del área.

- **REQUERIMIENTOS MINIMOS**. Solventar con lo mínimo de Herramientas o Personal para resolver la contingencia.

- **REQUERIMIENTOS MINIMOS NECESARIOS**. Lo óptimo de Herramientas que nos ayudaran para resolver la contingencia

- **REGISTROS VITALES**. Backups de Información o Procesos de Información.

- **CRITERIOS (Legales, Contractuales, Marcos Normativos).** Sobre que reglamentos se pueden regir o sobre que leyes.

- **DAÑO**. Donde o de qué forma podría causar problemas en la institución.

6. Diseño Metodológico

6.1. Investigación Aplicada

Cuyo propósito es la solución de problemas específicos para mejorar la calidad de vida de las sociedades, este tipo de investigación está vinculada a la investigación pura, en el caso particular del análisis de riesgos informáticos en el Instituto Sonorense de Infraestructura Educativa, este tipo de investigación permite la búsqueda de una posible solución a los problemas conocidos o que aún se desconocen de acuerdo a los riesgos informáticos que se pueden presentar o que se están presentando en la institución, tratando de dar una solución práctica a una problemática definida a través de respuestas a las necesidades que la investigación sugiere y que puede valerse de algún proceso sistemático para el desarrollo como tal del proyecto. Se podría asociar la siguiente frase para explicar de mejor forma lo que implica la utilización de la investigación aplicada.

La investigación aplicada esta soportada en aportes teóricos y el desarrollo de actividades tendientes a determinar las posibles causas del problema y evidenciar los hallazgos, que más adelante y gracias a los resultados de la investigación, proporcionaran un marco de trabajo en búsqueda de la aplicabilidad de las posibles soluciones.

Como parte del desarrollo de la investigación aplicada, se plantean a nivel general actividades que tratan de dimensionar y atacar el problema mencionado para brindar al final del proyecto las posibilidades que tiene la institución para adoptar un plan de mejora, de acuerdo a los resultados que se obtengan a partir del análisis de riesgos. Algunas de estas actividades se mencionan a continuación.

- Definición de los objetivos del proyecto y delimitación del alcance de acuerdo al problema planteado.

- Análisis de fuentes de datos y recopilación de información: Esta etapa busca recolectar la mayor cantidad de información posible con respecto al estado actual, estudios o proyectos que tengan relación con el análisis de riesgos y en general en materia de seguridad informática en la institución.

- Generación del plan de trabajo y establecimiento de plazos de tiempo: Esta actividad hace referencia a la generación de un cronograma de actividades a nivel general que establezca límites de tiempo y asignación de tareas para lograr el desarrollo del proyecto.

- Recolección de documentos organizacionales: Para realizar el análisis de riesgos es importante conocer el entorno y contexto en el que se basa la Institución objeto de estudio, conocer su estructura organizacional, forma de operación, lineamientos, normatividad y reglamentaciones en las que se ampara, entre otras.

- Reconocimiento del entorno y del ámbito de trabajo: Se requiere realizar una valuación de activos, infraestructura y visita de los lugares físicos donde tendrá aplicación el proceso de análisis de riesgos.

- Desarrollo de análisis de riesgos: Gracias al plan de trabajo y la determinación de los componentes a evaluar, se recogen datos que permitan demostrar posibles deficiencias o fallas que puedan llegar a materializarse.

- Identificación de vulnerabilidades: Se enfoca en el desarrollo de actividades y/o la aplicación de herramientas sobre sistemas de información, aplicaciones web, sistemas de comunicación o servicios de red y los activos de información críticos con el objetivo de determinar su estado actual desde el punto de vista de seguridad de la información.

- Análisis de vulnerabilidades: Luego de obtener las evidencias se realiza un compendio y organización de todos estos datos, con información relevante que permita determinar focos de falla.

- Análisis de los datos, hallazgos de debilidades y generación de recomendaciones: Con la información, datos obtenidos se genera una matriz con la valoración de los riesgos obtenidos, sugerencias y recomendaciones.

- Discusión de resultados y obtención de la conclusión: paralelo a la generación del informe técnico, se realiza un resumen ejecutivo que muestre de una manera general y objetiva los resultados del proyecto.

- Presentación del informe definitivo a las directivas de la Institución: Se prepara la sustentación del proyecto para socializar le trabajo realizado.

7. Informe Técnico

Etapa 1:

La primera etapa fue un reconocimiento de infraestructura física y tecnológica, así como la recolección de documentación e información relevante para el desarrollo del proyecto:

- Información contextual de la institución
- Manuales de configuración por parte de fabricantes o elaborados por personal del área en cuanto a servicios, servidores y dispositivos de red.
- Estudios o contrataciones relacionados con sistemas de información.

Etapa 2:

En esta fase luego de comprender la estructura organizacional y su manera de operación, basada en el modelo de negocio (actividad principal) de la institución, se clasifican activos por criticidad, se definen planes para realizar y obtener datos sobre el estado de seguridad a nivel hardware y software de equipos, servicios, procesos y procedimientos; además de conseguir información con respecto a instalaciones físicas.

- Visitas a los sitios físicos donde se encuentran los equipos de comunicación, seguridad perimetral, almacenamiento y procesamiento de datos para tomar evidencias de las condiciones actuales.

- Clasificación de los activos de información más críticos que pueden detener el normal funcionamiento del SITE en caso de falla.

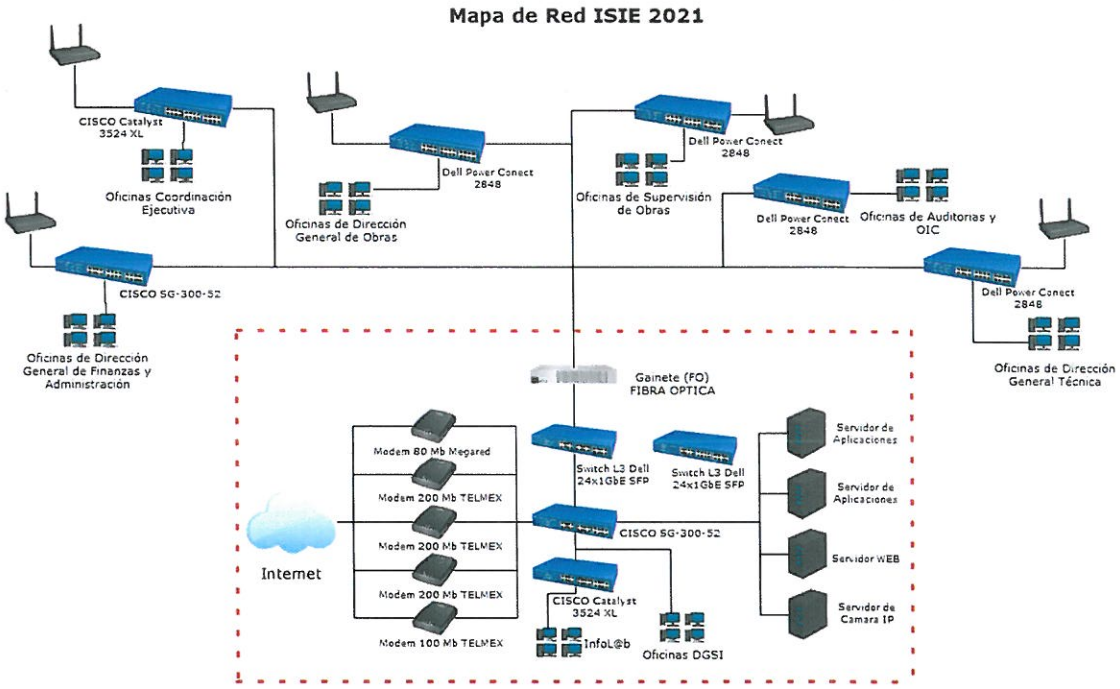
- Solicitud formal de acceso a servidores y equipos de comunicación, tales como firewalls, switchers y routers, con el fin de tomar evidencia del proceso y forma de configuración de cada dispositivo y/o sistema operativo.

- Solicitud de acceso a la documentación de la red, se evidencio el diseño lógico (Definición de segmentos, diseño de direccionamiento, diagramas lógicos, VLANs), privilegios y características de cuentas de usuario, perfiles de cuentas de acceso, políticas definidas en los firewalls.

8. Activos de Información

Topología de Red de la que constituye el Instituto de Infraestructura Educativa actualmente donde se contempla que se encuentra en crecimiento y falta algo de Hardware para fortalecer la Infraestructura Tecnológica.

8.1. Mapa de Red



8.2. Inventario de Activos Informáticos.

[Nombre o Identificador de archivo informático]	[Fecha del alta del archivo informático]	[Número del Inventario asignado al archivo informático]	[Número de serie asignado al archivo informático]	[Puesto del responsable del resguardo del archivo informático]	[Ubicación Física del archivo informático (DIRECCION)]
SERVIDOR POWEREDGE R710	03/07/12	1000-1100-1240-1241-12412-20243	DXMW7V1	DIRECTOR GENERAL DE INNOVACION Y SISTEMAS	DIRECCION GENERAL DE INNOVACION Y SISTEMAS (SITE)
SERVIDOR POWEREDGE R540	06/09/18	80000000408	374VHQ2	DIRECTOR GENERAL DE INNOVACION Y SISTEMAS	DIRECCION GENERAL DE INNOVACION Y SISTEMAS (SITE)
Computadora Brain LX. Pentium IV 3.2 GHz, 1 GB RAM, DD 80 GB.	11/10/05	1000-1100-1240-1241-12413-30192	00509229383	DIRECTOR GENERAL DE INNOVACION Y SISTEMAS	DIRECCION GENERAL DE INNOVACION Y SISTEMAS (SITE)
Computadora Brain LX 3090. Pentium IV 3.2 GHz, 1 GB RAM, DD 80 GB.	11/10/05	1000-1100-1240-1241-12413-30217	00509229376	DIRECTOR GENERAL DE INNOVACION Y SISTEMAS	DIRECCION GENERAL DE INNOVACION Y SISTEMAS (SITE)
Switch Catalyst 3508G XL 8 Puertos	06/07/01	1000-1100-1240-1241-12416-60098	SS004	DIRECTOR GENERAL DE INNOVACION Y SISTEMAS	DIRECCION GENERAL DE INNOVACION Y SISTEMAS (SITE)

Switch Catalyst 3524 XL 24 Puertos	06/07/01	1000-1100-1240-1241-12416-60099	SS005	DIRECTOR GENERAL DE INNOVACION Y SISTEMAS	DIRECCION GENERAL DE INNOVACION Y SISTEMAS (SITE)
Computadora Brain LX 3090. Pentium IV 3.2 GHz, 1 GB RAM, DD 80 GB.	11/10/05	1000-1100-1240-1241-12416-60137	00509229380	DIRECTOR GENERAL DE INNOVACION Y SISTEMAS	DIRECCION GENERAL DE INNOVACION Y SISTEMAS (SITE)
Servidor Xeon 3.6 GHz, segundo procesador Xeon 3.6 GHz, 4Gb, DDR2, 400MHz, 4 Discos Duros de 73 GB Ultra 320 SCSI, 10,000 rpm), tarjeta de red integrada, Fuente de poder redundante unidad 24X CD-ROM, Unidad de Floppy, 3.5 de 1.44 Mb, Panel Plano Digital Dell 15"	19/12/05	1000-1100-1240-1241-12416-60139	DDRGZ81	DIRECTOR GENERAL DE INNOVACION Y SISTEMAS	DIRECCION GENERAL DE INNOVACION Y SISTEMAS (SITE)
Computadora Vostro 230 Slim Tower. E.S.C. 20332000117	27/12/10	1000-1100-1240-1241-12416-60174	9C95BP1	DIRECTOR GENERAL DE INNOVACION Y SISTEMAS	DIRECCION GENERAL DE INNOVACION Y SISTEMAS (SITE)
Switch Catalyst 3524 XL 24 Puertos	06/07/01	1000-1100-1240-1241-12416-60100	SS006	JEFE DE RECURSOS MATERIALES	DIRECCION GENERAL DE FINANZAS Y ADMINISTRACION

Switch Catalyst 3524 XL 24 Puertos	06/07/01	1000-1100-1240-1241-12416-60101	SS007	DIRECTOR GENERAL DE INNOVACION Y SISTEMAS	DIRECCION GENERAL DE INNOVACION Y SISTEMAS (SITE)
Switch Catalyst 3524 XL 24 Puertos	06/07/01	1000-1100-1240-1241-12416-60102	SS008	SUBDIRECTOR DE COSTOS Y PRESUPUESTOS	DIRECCION GENERAL DE OBRAS - COSTOS
Switch Catalyst 3524 XL 24 Puertos	06/07/01	1000-1100-1240-1241-12416-60103	SS009	DIRECTOR GENERAL DE OBRAS	DIRECCION GENERAL DE OBRAS
SWITCH POWER CONNECT 2848 48 1GBE PORTS 4 PORTS WITH SFP	10/04/12	1000-1100-1240-1241-12416-60191	JTD67M1	DIRECTOR GENERAL DE OBRAS	DIRECCION GENERAL DE OBRAS
SWITCH POWER CONNECT 2848 48 1GBE PORTS 4PORTS WITH SFP	10/04/12	1000-1100-1240-1241-12416-60192	FSD67M1	DIRECTOR GENERAL TECNICO	DIRECCION GENERAL TECNICA
Switch Catalyst 3524 XL InLine Power Ethernet	08/08/06	SC-001	SS010	DIRECTOR GENERAL DE INNOVACION Y SISTEMAS	DIRECCION GENERAL DE INNOVACION Y SISTEMAS (SITE)
Switch Catalyst 3524 XL InLine Power Ethernet	08/08/06	SC-002	FAB0520U0SH	COORDINADOR EJECUTIVO	COORDINACION EJECUTIVA
SWITCH POWER CONNECT 2848 48 1GBE PORTS 4PORTS WITH SFP	06/05/14	SC-003	85CXFH1	DIRECTOR GENERAL DE OBRAS	DIRECCION GENERAL DE OBRAS - SUPERVISION

TARJETA DE 16 EXTENSIONES ANALOGICAS	03/07/12	1000-1100-1240-1241-12416-60195	KXTD1745ABKE090421	DIRECTOR GENERAL DE INNOVACION Y SISTEMAS	DIRECCION GENERAL DE INNOVACION Y SISTEMAS (SITE)
CENTRAL TELEFONICA MARCA PANASONIC, MODELO KX-TDA100DBP -MODULO O´ TARJETA DE 16 EXT. -TARJETA PARA 8 EXT. DIGITALES -TARJETA PARA 4 TRONCALES COESNE SA de CV	03/07/12	1000-1100-1240-1241-14216-60211	2BBCA0010001396	DIRECTOR GENERAL DE INNOVACION Y SISTEMAS	DIRECCION GENERAL DE INNOVACION Y SISTEMAS (SITE)
SWITCH CISCO SG300-52	24/12/2015	80000000319	ADI19340CQS	DIRECTOR GENERAL DE INNOVACION Y SISTEMAS	DIRECCION GENERAL DE INNOVACION Y SISTEMAS (SITE)
SWITCH CISCO SG300-52	24/12/2015	80000000320	ADI19340C4D	DIRECTOR GENERAL DE FIANNZAS Y ADMINISTRACION	DIRECCION GENERAL DE FINANZAS Y ADMINISTRACION
SWITCH CISCO SG300-52	24/12/2015	80000000321	DNI19340CTN	COORDINADOR EJECUTIVO	AUDITORIAS
SWITCH L3 MARCA DELL 24x1 GbE SFP	06/11/2018	80000000409	45SJXC2	DIRECTOR GENERAL DE INNOVACION Y SISTEMAS	DIRECCION GENERAL DE INNOVACION Y SISTEMAS (SITE)
SWITCH L3 MARCA DELL 24x1 GbE SFP	06/11/2018	80000000410	77SJXC2		

8.3. INVENTARIO DE APLICACIONES

8.3.1. Aplicaciones Desarrolladas por ISIE de Versiones para Escritorio

Inventario de aplicaciones que ISIE utiliza para su operación habitual recopilando información en su base de datos conectados en red con privilegios de usuarios y lo contienen en repositorios locales en sus Servidores, todas estas compiladas en Versión para Escritorio(Windows).

SERVIDOR (características específicas)	SISTEMA OPERATIVO UTILIZADO (características especificas)	BASE DE DATOS (Esquema - Diagrama, nombre y versión del motor, funciones personalizadas respaldos)	LENGUAJE DE PROGRAMACIÓN (por ejemplo: Versión Java, PHP. Etc.)
SERVIDOR POWEREDGE R540 Xeon Silver 4116 2.1 GHz (2 processors) Ram 128 GB Disk 0 - Raid 1 - 2 discos de 372 GB SSD Disk 1 - Raid 5 - 3 discos de 1.75 TB SSD	WINDOWS SERVER	TOPSPEED DATABASE	CLARION 5.5

APLICACIÓN	PUESTO DEL RESPONSABLE	REPOSITORIO DE CÓDIGO FUENTE
Bitácora de Registros Informáticos	Jefe de Sistemas de Obras y Servidores de Datos	10.10.10.101\D$\ISIE\FUENTES\BITACORA
Gestión de Calidad	Jefe de Sistemas Técnicos, Administrativos y Transparencia	10.10.10.101\D$\ISIE\FUENTES\CALIDAD
Control de Gestión	Director General de Innovación y Sistemas	10.10.10.101\D$\ISIE\FUENTES\CG

Checador del Personal ISIE	Jefe de Sistemas Técnicos, Administrativos y Transparencia	10.10.10.101\D$\ISIE\FUENTES\CHECADOR
Contrarecibos	Jefe de Sistemas Técnicos, Administrativos y Transparencia	10.10.10.101\D$\ISIE\FUENTES\CONTRARECIBOS
Activo Fijo	Jefe de Sistemas de Obras y Servidores de Datos	10.10.10.101\D$\ISIE\FUENTES\INVENTARIO
ISIETrack	Director General de Innovación y Sistemas	10.10.10.101\D$\ISIE\FUENTES\ISIETRACK
Asignación de Memos y Oficios	Jefe de Sistemas Técnicos, Administrativos y Transparencia	10.10.10.101\D$\ISIE\FUENTES\MEMOSYOFICIOS
ISIEAdmin	Jefe de Sistemas Técnicos, Administrativos y Transparencia	10.10.10.101\D$\ISIE\FUENTES\PRESUPUESTO
Prodies	Jefe de Sistemas Técnicos, Administrativos y Transparencia	10.10.10.101\D$\ISIE\FUENTES\PRODIES
Sistema de Control de Obras	Director General de Innovación y Sistemas	10.10.10.101\D$\ISIE\FUENTES\SCO
Estimático	Director General de Innovación y Sistemas	10.10.10.101\D$\ISIE\FUENTES\SCO
Módulo Generador de Contratos de Obra y Equipamiento	Jefe de Sistemas Técnicos, Administrativos y Transparencia	10.10.10.101\D$\ISIE\FUENTES\SCO
Sistema de Control de Obras 2015	Director General de Innovación y Sistemas	10.10.10.101\D$\ISIE\FUENTES\SCO
Archivo Digital	Director General de Innovación y Sistemas	10.10.10.101\D$\ISIE\FUENTES\SCO

Generador de Consultas Globales	Jefe de Sistemas de Obras y Servidores de Datos	10.10.10.101\D$\ISIE\FUENTES\SCO
Reportes de Supervisión	Jefe de Sistemas de Obras y Servidores de Datos	10.10.10.101\D$\ISIE\FUENTES\SCO
Registro de Contratos para ECFlow	Jefe de Sistemas de Obras y Servidores de Datos	10.10.10.101\D$\ISIE\FUENTES\SCO
Generador de archivo para importación de datos a plataforma ECFlow	Jefe de Sistemas de Obras y Servidores de Datos	10.10.10.101\D$\ISIE\FUENTES\SCO
Generador de archivos pdf con estados de cuenta de contrato para ECFlow	Jefe de Sistemas de Obras y Servidores de Datos	10.10.10.101\D$\ISIE\FUENTES\SCO
Generador de archivo xls con finiquito de contrato para ECFlow	Jefe de Sistemas de Obras y Servidores de Datos	10.10.10.101\D$\ISIE\FUENTES\SCO
Módulo Generador de Documentos de Licitación	Jefe de Sistemas Técnicos, Administrativos y Transparencia	10.10.10.101\D$\ISIE\FUENTES\SCO
Pago de Estimaciones	Jefe de Sistemas de Obras y Servidores de Datos	10.10.10.101\D$\ISIE\FUENTES\SCO
Catálogo de Contratistas	Jefe de Sistemas de Obras y Servidores de Datos	10.10.10.101\D$\ISIE\FUENTES\SCO
Registro de Transferencias Contables	Jefe de Sistemas de Obras y Servidores de Datos	10.10.10.101\D$\ISIE\FUENTES\SCO
Supervisión de Obra	Jefe de Sistemas de Obras y Servidores de Datos	10.10.10.101\D$\ISIE\FUENTES\SCO
Viáticos	Jefe de Sistemas Técnicos, Administrativos y Transparencia	10.10.10.101\D$\ISIE\FUENTES\VIATICOS

Auditorias	Director General de Innovación y Sistemas	10.10.10.101\D$\ISIE\FUENTES\SAUDITORIAS

8.3.2. Aplicaciones Desarrolladas por ISIE de Versión WEB

Aplicaciones propietarias de ISIE que utiliza para la publicación y uso remoto o externo ya se a publicar información o comunicarse con operativos de la Institución y se encuentran diseñadas en Versión WEB la del Sistema de Consulta de Tramites en Línea con GoDaddy y otras dos se encuentran hospedadas en sus propios servidores.

SERVIDOR (características específicas)	SISTEMA OPERATIVO UTILIZADO (características especificas)	BASE DE DATOS (Esquema - Diagrama, nombre y versión del motor, funciones personalizadas, respaldos)	LENGUAJE DE PROGRAMACIÓN (por ejemplo: Versión Java, PHP. Etc.)
2 Procesadores Intel Xeon 3.6 GHz, RAM de 4 GB, 4 discos SCSI de 73 GB cada uno	WINDOWS SERVER	MySQL	PHP, HTML5
APLICACIÓN	**PUESTO DEL RESPONSABLE**	**REPOSITORIO DE CÓDIGO FUENTE**	
Sistema de Consulta de Trámites en Línea	Prestador de Servicios	10.10.12.252\C$\WAMP\WWW\BUSCATRAMITES	
SERVIDOR (características específicas)	**SISTEMA OPERATIVO UTILIZADO (características especificas)**	**BASE DE DATOS (Esquema - Diagrama, nombre y versión del motor, funciones personalizadas, respaldos)**	**LENGUAJE DE PROGRAMACIÓN (por ejemplo: Versión Java, PHP. Etc.)**
PROVEEDOR	WINDOWS SERVER	MySQL	PHP, JavaScript, HTML5, JSON, JQuery, Bootstrap
APLICACIÓN	**PUESTO DEL RESPONSABLE**	**REPOSITORIO DE CÓDIGO FUENTE**	
ECFlow	Director General de Innovación y Sistemas	10.10.10.101\D$\ISIE\FUENTES\ECFlow	

8.3.3. Aplicaciones Desarrolladas por Terceros de Versión WEB

Aplicación creada por un tercero hospedad con GoDaddy y la página Web oficial de ISIE proporcionada por la Contraloría del Gobierno del Estado de Sonora

SERVIDOR (características específicas)	SISTEMA OPERATIVO UTILIZADO (características especificas)	BASE DE DATOS (Esquema - Diagrama, nombre y versión del motor, funciones personalizadas, respaldos)	LENGUAJE DE PROGRAMACIÓN (por ejemplo: Versión Java, PHP. Etc.)
PROVEEDOR	WINDOWS SERVER	MySQL	PHP, JavaScript, HTML5,JQuery, BootstraP,AJAX
APLICACIÓN	**PUESTO DEL RESPONSABLE**	**REPOSITORIO DE CÓDIGO FUENTE**	
Página WEB del ISIE	Prestador de Servicios	CONTRALORIA DEL GOBERNO DEL ESTADO DE SONORA	

9. Plan de Continuidad al Negocio

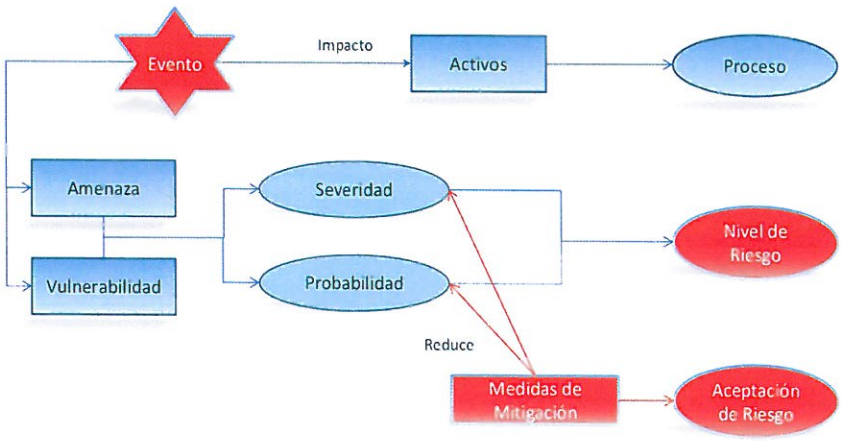
Componentes de un Plan de Continuidad del Negocio que debe contemplar la institución para su correcta aplicación de este:

1. Análisis de Riesgos (RA)

El análisis de riesgos es una herramienta que permite identificar las amenazas y vulnerabilidades a las que se encuentran expuestos los procesos o servicios del ISIE y pueden comprometer la continuidad de las operaciones. Identificar esos riesgos inherentes y entender su nivel de impacto en el negocio es el resultado se este análisis. El análisis de riesgo debe aplicarse sobre las instalaciones, infraestructura de TI y activos relacionados con los procesos que se determinen como críticos.

Los objetivos del análisis de riesgos son:

- Identificar los activos críticos del negocio, sus amenazas y sus vulnerabilidades
- Identificar los riesgos que tienen una mayor probabilidad de ocurrencia y un mayor impacto en la continuidad de negocio
- Identificar los controles actuales y evaluar la efectividad de los mismos
- Definir los controles necesarios para reducir la exposición de la organización a los riesgos y/o reducir el impacto
- Establecer los escenarios de interrupción para los cuales se definirán estrategias de continuidad



1. Análisis de Impacto al Negocio (BIA)

Una vez realizado el análisis de la información proporcionada por el ISIE, se realizaron las entrevistas con el personal responsable de los procesos. Para el levantamiento y documentación de la información obtenida se debe utilizar el "Cuestionario BIA", el cual permitirá identificar:

- Información general del proceso
- Entradas, salidas y periodos críticos del proceso
- Tipos de impactos al proceso. Los impactos aplicables al proyecto deben ser validados y aprobados por el representante de la Dirección del cliente
- Aplicaciones y/o equipo tecnológico que da soporte al proceso
- Requerimientos mínimos y registros vitales
- Proveedores relacionados

2. Estrategias de Continuidad

Durante esta fase se toman como base los escenarios de interrupción planteados en el análisis de riesgos para desarrollar las estrategias de continuidad necesarias para recuperar la operación en caso de una contingencia.

Los principales objetivos de esta fase son:

- Identificación de posibles estrategias de recuperación para los escenarios de interrupción establecidos
- Evaluación de las opciones de estrategia (costo-beneficio)
- Selección de la estrategia de continuidad y aceptación de posibles riesgos no cubiertos
- Definición de requerimientos de recuperación de acuerdo a la estrategia seleccionada
- Definición de interacción con terceros (proveedores, entes normativos y autoridades)

9.1. Análisis de Riesgos (RA)

Mapa de Riesgos que nos da a conocer de qué manera afectarían a la Institución si ocurriera una contingencia y permitiéndonos actuar desde antes para evitar cualquier error o daños evitando a su máxima expresión un Impacto y Probabilidad de que ocurra un desastre en el Instituto.

Escenario de Riesgo			Pérdida de CID				Evaluación de Riesgo		Nivel de Riesgo Actual
Activo	Amenaza	Vulnerabilidad	Confidencialidad	Integridad	Disponibilidad	Ponderación de CID	Impacto	Probabilidad	
1. Energía Eléctrica	Falla Suministro de Energía	Servicios se detienen momentáneamente	N	P	P	P	A	B	B
		Daño de equipos							
	Falla de UPS	Servicios se detienen momentáneamente							
2. Equipo de Computo	Robo	Atraso de labores	P	P	P	P	A	M	M
		Gasto en reposición							
		Pérdida de Información							
	Fraude	No cumple con propósito de adquisición							
	Sabotaje	Pérdida de Información							
		Gasto de reparación							

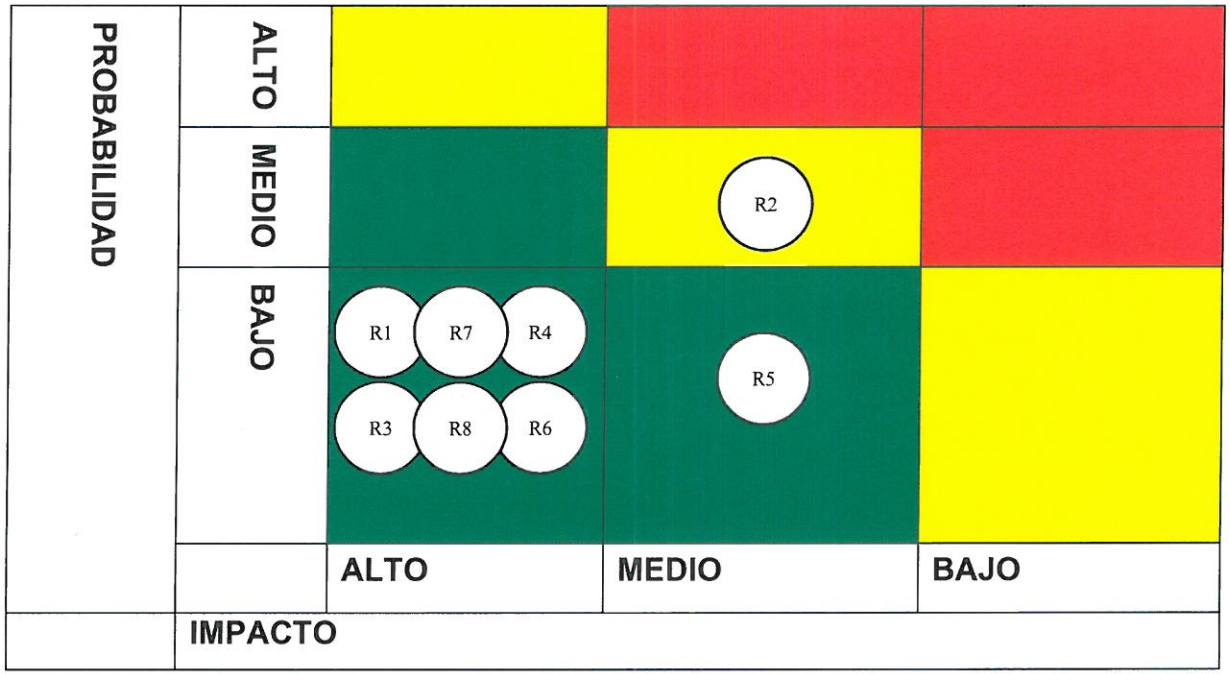
	Destrucción o falla de Equipos	Atraso de labores							
		Gasto en reposición							
		Pérdida de Información							
3. Sistemas Operativos	Perdida de Accesos	Atraso de labores	P	P	P	P	A	B	B
	Falla del S.O.	Atraso de labores							
	Virus o Troyanos	Pérdida de Información							
		Pérdida de acceso al S.O.							
	Privilegios Erróneos	Atraso de labores							
4. Infraestructura o Edificio	Incendio	Paro de labores	P	P	C	P	A	B	B
		Pérdida de información							
		Pérdida de Equipos							
	Inundación	Daño de equipos							
		Pérdida de información							
		Atraso de labores							
	Corto Circuito	Servicios se detienen momentáneamente							
		Daño de equipos							

	Tormenta Eléctrica	Servicios se detienen momentáneamente							
		Daño de equipos							
5. Redes y Telecomunicaciones	Cableado Descompuesto	Fallas en los sistemas	N	N	P	N	M	B	B
		Falla de comunicación							
		Falla de comunicación en NODO							
	Falla de Router o Switcher	Atraso de labores							
		Falla de comunicación							
	Falla de Access Point WIFI	Falla de internet							
	Intrusiones indebidas	Robo de información							
		Daño de información							
6. Servidores	Falla en Discos Duros	Pérdida de información	N	P	P	P	A	B	B
		Gasto en reparación							
	Servidor Descompuesto	Atraso de labores							

	Falla de Periférico (Lan, CD, Salida de Video, etc.)	Gasto en Reposición							
		Atraso de labores							
	Hardware Obsoleto	Falla de comunicación en NODO							
	Falla de Componentes Internos	Gasto en reparación							
7.SITE	Fallas en las condiciones idóneas	Falla de equipos	N	P	P	P	A	B	B
8. Software	Pérdida de código fuente	Pérdida de operación	P	C	C	C	A	B	B
	Fallas en los componentes	Pérdida de operación							
		Pérdida de Información							

9.1.1. Mapa de Riegos

Nos muestra una relación en Forma de Matriz donde nos indica de manera gráfica la detección de los riesgos con más probabilidad e impacto hacia la institución.



En la Etapa de Análisis de Riesgos es primordial contemplar el alto riesgo que nos muestra en las anteriores tablas ya que nos arroja un alto impacto en lo que respecta a perdida de infraestructura y equipo tecnológico que conllevaría a un mucho gasto económico para ISIE así también como interrupción de operaciones y perdida de información significativa.

9.2. Análisis de Impacto al Negocio (BIA)

El siguiente componente se utilizó para estimar la afectación que podría padecer la Institución como resultado de la ocurrencia de algún incidente o un desastre. Este es un proceso más especializado en la identificación de los tipos de impacto, orientado en conocer qué podría verse afectado y las consecuencias sobre los procesos del ISIE.

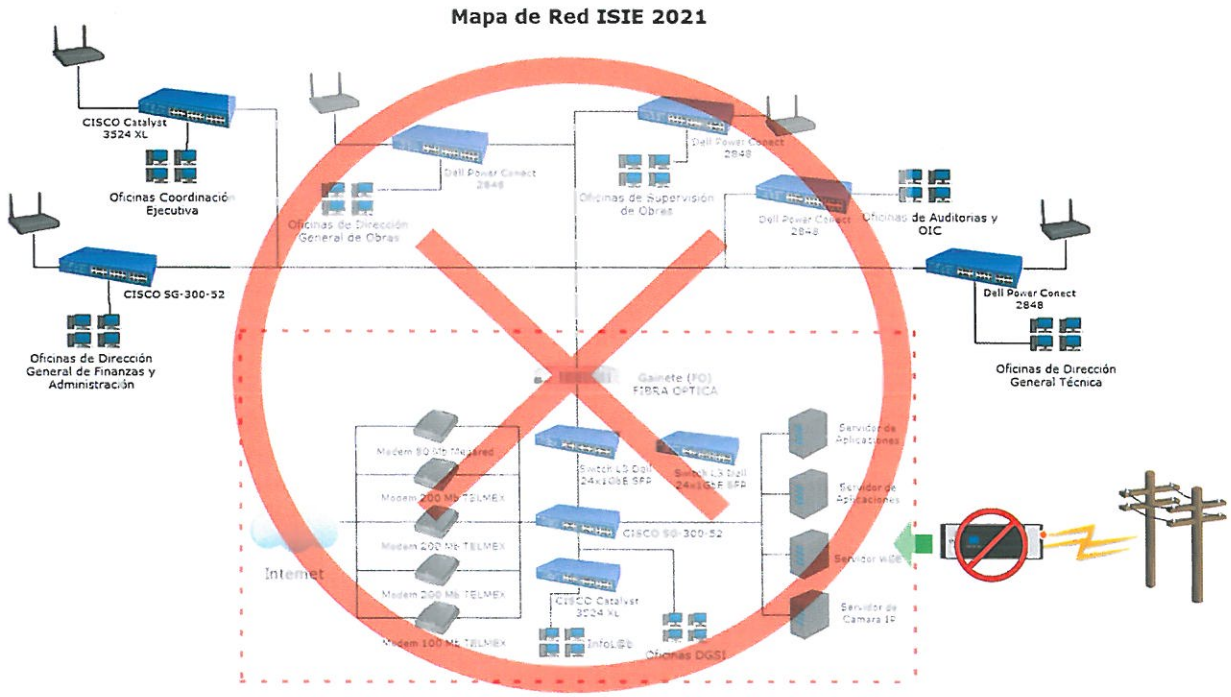
AREA	RESPONSABLE	PROCESOS	RPO	RTO	MTD	RIESGOS	REQUERIMIENTOS MINIMOS	REQUERIMIENTOS MINIMOS NECESARIOS	REGISTROS VITALES	CRITERIOS	DAÑO
DGIS	Carlos Rodriguez	Publicación de información en portal web	1 día	2 días	3 días	Perdida de información	2 personas, acceso a internet	Acceso a internet, 2 personas	Back up	SECOG	Perdida de presencia web del instituto
DGIS	Alberto Beltrán	Configuración de Red	1 día	5 días	6 días	Falta de comunicación con los NODOS	1 persona, herramienta adecuada	4 personas, herramienta adecuada, material (cable)	Servidor	N/A	Económico/ Reemplazo del equipo
DGIS	Toda el área	Reparación menor	1 día	3 días	4 días	Pérdida total del equipo	1 persona, herramienta adecuada	1 persona, herramienta adecuada	Back up, equipo de respaldo	N/A	Económico/ Reemplazo del equipo
DGIS	Carlos Rodriguez	Transmisión de eventos de licitacion	1 día	2 días	3 días	Perdida de información	1 personas, acceso a internet, equipo adecuado	2 personas, acceso a internet, equipo adecuado	equipo de respaldo	SECOG	Incapacidad de transmitir los eventos de licitacion
DGIS	Carlos Rodriguez	Respaldo de Sistema EC-FLOW	1 días	2 días	3 días	Perdida de información	Acceso a internet, 1 personas	Acceso a internet, 2 personas	Servidor		
DGIS	Carlos Rodriguez, Mirna Mendivil, Emmanuel Espencueta	Configuracion de Correo Electronico	1 día	2 días	3 días	Atrazo de labores, perdida de informacion	1 personas, acceso a internet	2 personas, acceso a internet			Perdida de disponibilidad de Correo electronico oficial
DGIS	Toda el área	Falla en S.O.	1 día	1 día	2 días	Pérdida de información	1 persona, software de restauración S.O.	1 persona, software de restauración S.O.	Respaldo de Información	N/A	Atraso de Operaciones
DGIS	Toda el área	Daños en Infraestructura	30 días	7 días	37 días	Información y de Equipo	2 personas, equipo de respaldo	4 personas, equipo de respaldo	Respaldo de Información y de configuraciones	N/A	Económico/ Reemplazo de equipo, Atraso de Operaciones
DGIS	Mirna Mendivil	Falla en Servidores	1 día	1 día	2 días	Pérdida de información	herramienta adecuada	2 personas, herramienta adecuada	Respaldo de información	N/A	Atraso de Operaciones
DGIS	Toda el área	Daño en Sistemas	1 día	1 día	2 días	Pérdida de información	conocimiento del lenguaje de	2 personas con conocimiento del lenguaje de programaciòn	Código Fuente	N/A	Atraso de Operaciones

El BIA que se realizó nos permite priorizar sobre procesos que nos puedan afectar en la Continuidad de Operaciones de la Institución en el cual se puede observar que lo que más dañaría será en la parte de Hardware al no contar con suficiente equipo ya sea de respaldo de energía y Equipo de Back-UP de datos suficientes hay una probabilidad alta de sufrir daños en la parte de Infraestructura Tecnológica.

9.3. Estrategias de Continuidad

9.3.1. Instalación de UPS en SITE

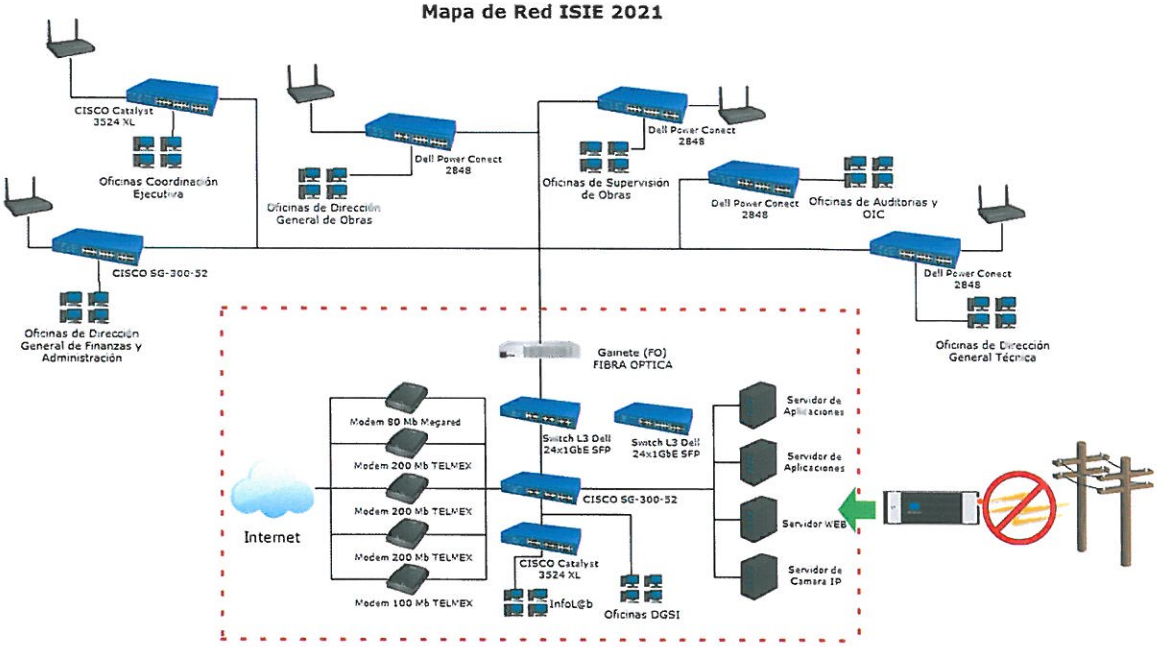
Un corte prolongado de energía interrumpiría totalmente la operación de la institución, al no contar con comunicación tecnológica digital, esto llevaría a cabo perdida de información, de tiempo, y paro de labores.



SITE de ISIE

Así mismo la institución cuanta con un UPS que le ayuda a crear respaldos momentáneos y tener menos probabilidades de perdida de información, pero este es insuficiente para mantener operando el SITE del instituto por un tiempo prolongado. Aumentando la cantidad de dispositivos UPS se mejoraría el tiempo de autonomía ante un corte de energía para de esta manera seguir laborando momentáneamente y así dar más tiempo a un restablecimiento de la corriente eléctrica y continuar labores sin problemas.

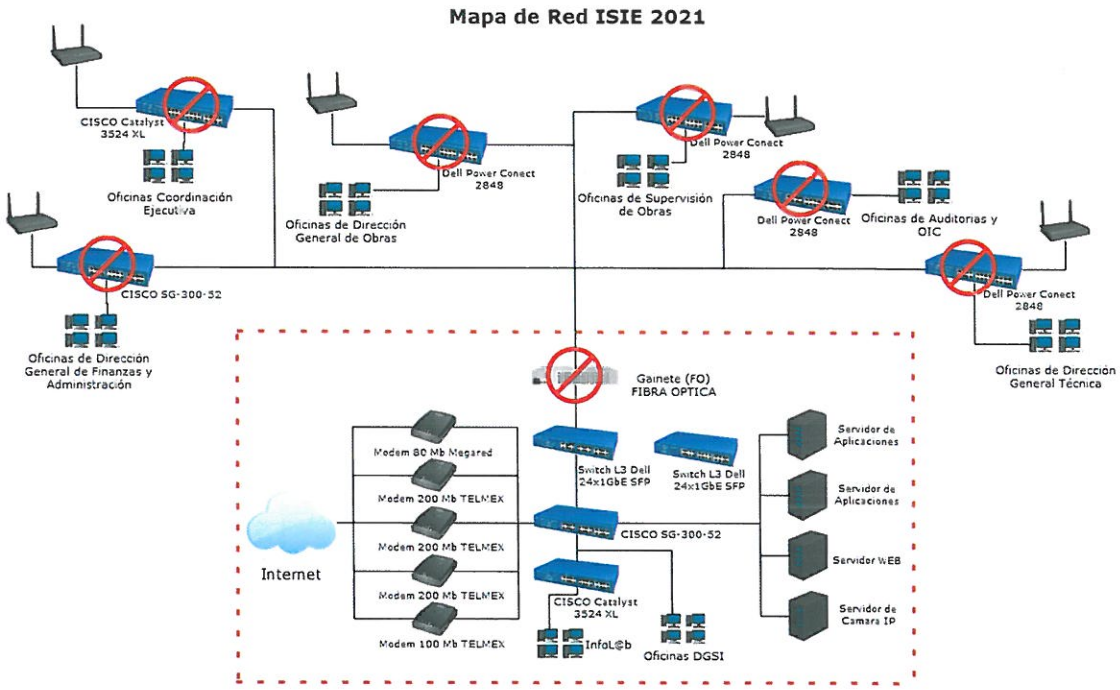
Mapa de Red ISIE 2021



SITE de ISIE

9.3.2. Falla en Gabinete de Fibra Óptica

El no contar con un Gabinete actual en componentes en el mercado conlleva un alto riesgo de paro de labores en nodos importantes de la institución en la cual habría un retardo de labores y se dificultaría la comunicación con los sistemas.



Es recomendable mantener actualizado los equipos y siempre contar una bitácora o registros de activos que no se encuentren descontinuados en el mercado y siempre contar con equipo de respaldo de preferencia de los más importantes en los nodos. Así al momento de una interrupción por el gabinete de fibra óptica podrá reemplazarse de inmediato o de no contar físicamente con uno tener a la mano la comunicación directa con algún proveedor que resuelva dicha contingencia.

9.3.3 Restaurar la Página Web a partir de Akeeba Backup

Mediante la extensión de Akeeba Backup se puede crear respaldos completos tanto de contenido como de las bases de datos de la pagina web de manera periódica. Estos respaldos se generan en archivos comprimidos en zip. Dentro de estos archivos comprimidos se encuentra el sitio web a manera de instalador.

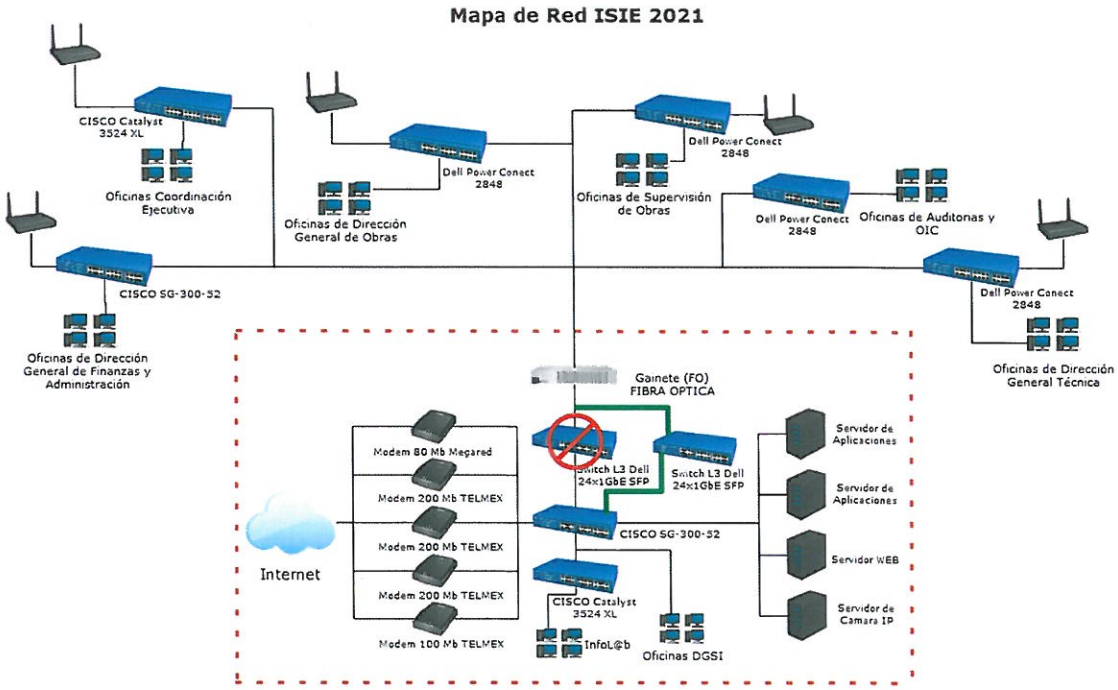
En caso de una contingencia, ya sea perdida de información o incluso perdida total del sitio web, este se puede restaurar de manera total a la fecha del último respaldo creado con Akeeba Bakcup. Simplemente se tiene que subir el archivo zip del respaldo al servidor mediante ftp y descomprimir el contenido dentro de una ruta con permisos de escritura, una vez hecho esto se deberá acceder a la ruta mediante URL y seguir los pasos del instalador del respaldo.

Una vez concluidos los pasos del instalador del respaldo, el sitio se encontrará de nuevo operativo y sin perdidas de información.

9.3.4 Reemplazo de Switch o reparación de nodos de Voz/Datos

En caso de descompostura de uno de los switch de un algún nodo de la institución, se recurrirá hacia la instancia correspondiente, en este caso, la Dirección de Sistemas e Innovación y se reportará el suceso. Esta a su vez corroborará los hechos y ya sea si fue daño menor se dispondrá de la herramienta necesaria en almacén para arreglar el daño, y si de lo contrario ocurre un daño irreparable se Reportará al área de finanzas para solicitar al proveedor de equipos para disponer de uno nuevo.

Si la falla se presenta en el concentrador de fibra óptica, el instituto cuenta con un equipo de respaldo al cual se deberán de interconectar los nodos de fibra óptica para de esta manera reestablecer la conexión con el resto de las áreas.

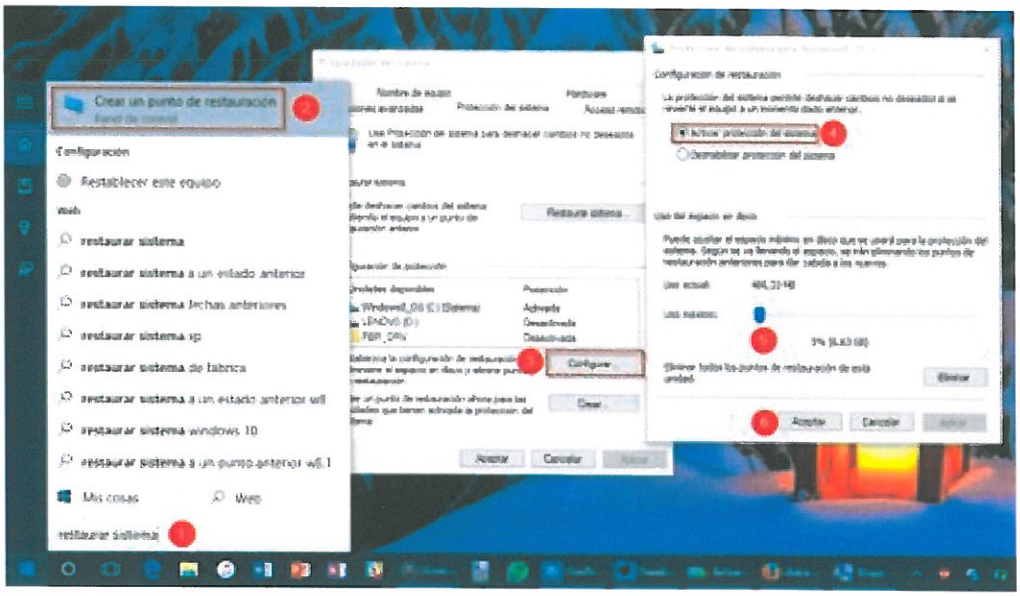


9.3.5 Recuperar funcionamiento de Sistema Operativo con ayuda del Punto de Restauración.

Restaurar Sistema está diseñado para **resolver problemas con instalación de programas, actualizaciones de sistema, o cambios en el registro** que puedan haber generado un error que desestabilice el equipo, y esta restauración puede iniciarse también en modo seguro/a prueba de fallos, lo que lo convierte en la herramienta ideal para resolver errores asociados a trucos de Windows 10 mal aplicados.

Por desgracia, Restaurar Sistema está **desactivado por defecto en Windows 10**, pero es posible volverlo a activar mediante los siguientes pasos:

- Abrir el Menú Inicio o Cortana y escribir "restaurar sistema".
- Hacer clic en el primer resultado que aparecerá: "Crear punto de restauración".
- Aparecerá una ventana de "Propiedades del sistema". Ahí hay que hacer clic en el botón "Configurar".
- En la nueva ventana que aparecerá, debemos marcar "Activar protección de sistema".
- Si queremos que existan muchos puntos de restauración disponibles, debemos aumentar el espacio reservado para Restaurar Sistema (yo lo aumenté de 486 MB a 6,6 GB). Cada punto de restauración gasta espacio, y cuando el espacio reservado se llena Windows empieza a borrar los puntos de restauración más antiguos. Por ende, si el espacio reservado es muy bajo, habrá a lo máximo 1 o 2 puntos de restauración disponibles (los más recientes), y no podremos deshacer cambios más antiguos.
- Finalmente, presionamos "Aceptar" para guardar la configuración.



9.3.6. Recuperación de Código Fuente.

Se realizará un respaldo diario de los Códigos Fuente de las aplicaciones por parte del personal de sistemas encargado. Estos respaldos se resguardarán en un servidor de respaldos y se llevara una bitácora de versiones para su completa disponibilidad en caso de presentarse un fallo con alguna de las aplicaciones del instituto.

9.4. Estrategias y Tiempos de Recuperación

		Tecnología / Servicios Tiempo de recuperación						
Riesgo	Estrategia de Recuperación	< 4 horas	1 días	3 días	1 semana	2 semanas	> 2 semanas	comentarios
6.2	Restaurar la página Web a partir de Akeeba Backup		X					
5.1	Reemplazo de Switch o reparación de nodos de Voz/Datos			X				
2.1	Contar con la herramienta necesaria para reparaciones en caso de Equipo de Computo Dañado por usuarios o uso constante	X						
5.2	Instalar cámara de respaldo para transmitir eventos de licitación y configurar software necesario.		X					
8.1	Descargar plataforma ECFLOW mediante FTP			X				
6.1	Contactar proveedor de correo electrónico para reestablecer cuentas		X					
8.2	Diagnostico e instalación de programas		X					

4.1	Restaurar Labores a partir de un Edificio o Infraestructura Alterna.			X				
3.1	Recuperar funcionamiento de Sistema Operativo con ayuda del Punto de Restauración	X						
7.1	Recuperar Sistemas mediante Respaldo de Aplicaciones para restauración de Servidor de Aplicación	X						
2.1	Recopilar formatos del respaldo y volver a publicar			X				
1.1	Respaldar Fallo de Energía por Medio de un UPS	X						
8.3	Recuperación de Código Fuente		X					

En esta etapa muestra las estrategias a realizar para el Plan de Continuidad de acuerdo a tiempos de atención y de respuesta de acuerdo al Mapa de Riesgos teniendo en cuenta la Priorización de la Matriz de Riesgos resultantes de la ponderación de los mismo.

Se muestra el número de riesgo correspondiente al mapa de riesgos, la descripción de la estrategia y el tiempo que este requiere para la recuperación del desastre.

9.5. ROLES Y RESPONSABILIDADES

9.5.1 Estructura de Gobierno de Continuidad del Negocio

La Estructura de Gobierno de Continuidad de Negocio es la estructura responsable de realizar las actividades necesarias para responder cuando se presente alguna interrupción en el negocio; desde el momento en que se declare el estado de contingencia hasta que los procesos operativos regresen a la normalidad.

Las eficacias de las fases de respuesta, recuperación y reanudación de procesos dependen directamente de la eficacia con que realicen las actividades el personal que forma parte de la estructura de gobierno de continuidad cuando se presente la contingencia. Este personal es el que se identificó como crítico para la operación en el BIA.

La Estructura de Gobierno Continuidad de Negocio es responsable de mantener la continuidad de negocio mediante la ejecución de actividades de emergencia y el manejo de las operaciones de recuperación.

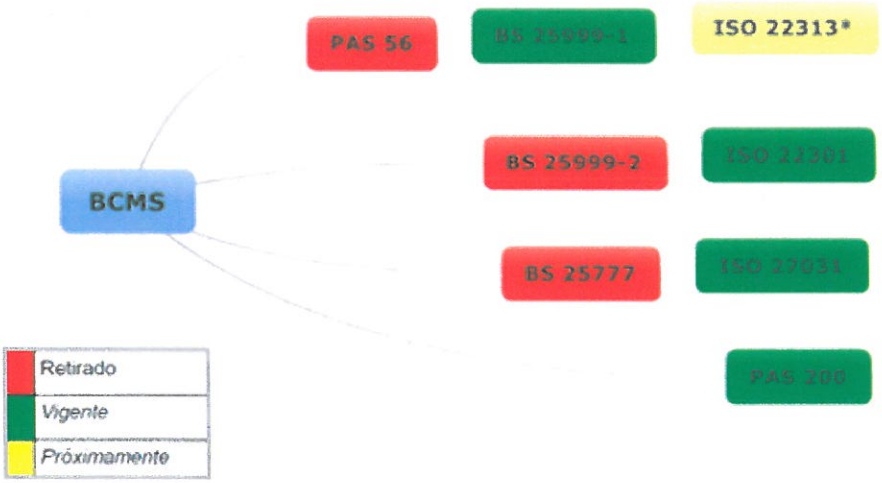
Roles y responsabilidades del ISIE

Rol	Responsabilidades	
Grupo de Directores	Director de Innovación y de Sistemas	
Grupo de Manejo de Crisis	Responsables de coordinar la recuperación, planear y revisar las actividades de los planes de continuidad de negocio	Jefe de Sistemas de Obras y Servicios de Datos
Grupos de trabajo	<u>Primera respuesta</u> Evaluar la situación y atender inicialmente el incidente	Analistas Técnicos
	<u>Recuperación de desastres</u> Habilitar aplicaciones, voz, datos e infraestructura	Jefe de Redes y Telecomunicaciones
	<u>Comunicación en crisis</u> Manejar la comunicación externa/ interna	Jefe de Sistemas Técnicos, Administrativos y Transparencia
	<u>Recuperación de instalaciones</u> Proveer de insumos materiales e instalaciones	Jefe de Gestión de Calidad y Normatividad
Recuperación de operaciones	Personal operativo responsable de operar durante una contingencia	Todo el Área de Innovación y de Sistemas

10. Mejores prácticas

- Lo más importante dentro de la gestión de la continuidad del negocio es que **los planes de continuidad sean probados**. De nada sirve tener todo documentado, definidos los responsables, contar con la tecnología de respaldo si no se hacen pruebas para determinar que las actividades definidas para responder ante una emergencia son las adecuadas para la organización. Si bien el estándar es único, **la forma en que se desarrolla y se aplica es único** y debe estar en concordancia con los procesos más críticos del negocio.
- Como parte de los requerimientos que se deben tener en cuenta dentro de la implementación de este estándar es la **definición de las necesidades de la organización**, lo cual se logra estableciendo un alcance determinado. Debe quedar muy claro **cuáles son los procesos que quedan cubiertos por los planes de continuidad**.
- La selección de los procesos incluidos en el alcance del sistema, debe estar basado en la definición del **apetito al riesgo**, el cual debe ser aprobado por la dirección de la organización, para garantizar que **esté conforme con la definición estratégica de la organización**.
- Mantenerse sobre un estándar de Plan de Continuidad en el cual se encuentre fuertemente **afianzado en metodologías y herramientas si se desee mejorar, que basado en el ciclo de mejora continua**, plantea los pasos para **planear**, **implementar**, **operar**, **revisar** y **mejorar la gestión de la continuidad del negocio**.
- Mantener capacitado a todo el personal de acuerdo a sus roles, así como las herramientas que existen para combatir la contingencia y las políticas que se generen.

Normas de Buenas Prácticas:



Estándar o Norma	Descripción
PAS 56:2003	Publicly Available Specification BCM
BS 25999-1:2006	Business Continuity Management---Code of Practice
BS 25999-2:2007	Business Continuity Management---Specification
ISO 22313:2012	Business continuity management systems – Guidance
ISO 22301:2012	Business continuity management systems --- Requirements
BS 25777:2008	Information and communications technology for BCM--Code of practice
ISO 27031:2011	Information and communication technology readiness for BC (IRBC)
PAS 200:2011	Crisis management. Guidance and good practice
Disaster Recovery Institute (DRI)	Prácticas profesionales para planificadores de continuidad de negocio

11. Conclusión

El plan se desarrolló para cubrir hasta el peor escenario que pueda surgir en la Institución de manera que hasta el más mínimo escenario de contingencia pueda ser cubiertos también.

Esto a su vez servirá de base al momento de determinar las alternativas viables para la recuperación ya que la diferencia entre tener y no tener un plan de continuidad implica que se puedan mitigar muchos errores que impedirán las operaciones normales en el ISIE y el contar con un plan de continuidad bien documentado y desarrollado nos llevara al éxito sin perdidas de información y más seguridad en la Institución que son tan valiosos para los ciudadanos a los cuales tendremos que responderles con datos confiables, íntegros y disponibles para ellos.

En un Plan de Continuidad es recomendable mantener una retroalimentación y actualización de sus procesos en base a las mejoras que ocurran en la institución estas propuestas pueden ser las siguientes:

- Reducir el ambiente de riesgo vigente.
- Disponer de las medidas de control interno necesarias.
- Disminuir el grado de exposición de los sistemas que se procesan.
- Incrementar la confiabilidad, integridad y disponibilidad de la información.
- Optimizar los procesos orientados al cumplimiento de los objetivos de la Institución.
- Conseguir disminuir el riesgo actual a su nivel mínimo.

Elaboró
Ing. Carlos Alberto Rodriguez Robles

Autorizó
Lic. Ismael Acevedo Esmerio