Marzo 13 de 2023

Plan de Continuidad (Contingencia) de las TICS para el INVISBU

Base Normativa

ISO 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información.

Introducción

La continuidad de operaciones apoyadas por la infraestructura tecnológica en el INVISBU es de gran importancia, en razón al manejo de información que se guarda en las bases de datos de los sistemas de información y que estable su flujo a través de la red de los diferentes medios de transmisión.
Por este motivo se vinculan todos los elementos de la infraestructura tecnológica como lo son los servidores, la red datos, los switches. los routers, los sistemas de información, el servicio de internet, el servicio del fluido eléctrico, el sistema de potencia, el servicio de hosting, el firewall, los equipos de computador, etc.

Por cualquier evento o incidente que altere la disponibilidad de la información en la entidad se debe activar los protocolos de contingencia establecidos y así poder minimizar los riesgos y garantizar la correcta prestación de los servicios y operaciones soportadas por la tecnología dispuesta en la organización

Justificación

El plan de continuidad de las TICS está basado en la disposición efectiva de la entidad frente a contingencias, apoyado en protocolos que permitan reiniciar los procesos importantes en la prestación del servicio al usuario, el manejo de la información y la buena imagen de la organización.
Es necesario diseñar plan de continuidad de las TICS, apoyado en el modelo PHVA que permita proteger la entidad de cualquier amenaza, que garantice la continuidad de la prestación del servicio y del normal funcionamiento de los sistemas de información.
Como visión objetiva de la seguridad la información, deberá estar en posibilidad de disminuir los riesgos asociados a la información (Disponibilidad, Integridad y confidencialidad); previniendo contingencias que garanticen una segura y mejor prestación del servicio.

Objetivo General

Asegurar que el INVISBU responda en forma efectiva en cualquier situación que afecte el normal funcionamiento de las operaciones que están apoyadas por las TICS, permitiendo de esta manera dar continuidad de la totalidad de los servicios que presta tanto a los usuarios internos como a los externos en el menor tiempo posible.

Objetivos Específicos

- Continuar con las operaciones de la Institución y el servicio a los clientes.
- Reducir las pérdidas de productividad dada la ocurrencia de un incidente que genere una interrupción

- Minimizar pérdidas de información.
- Mantener la Reputación e Imagen de la Institución.
- Prevenir o minimizar la pérdida o la corrupción de archivos de datos críticos para la continuidad de las operaciones del INVISBU.
- Indicar los lineamientos para la recuperación de los servicios informáticos ante un desastre o falla.
- Prevenir o minimizar el daño permanente a los recursos informáticos.
- Establecer procedimientos específicos que respondan a interrupciones del servicio, con el fin de proteger y recuperar las funciones criticas del negocio que se puedan ver comprometidas por eventos naturales, o sean ocasionados por el hombre.
- Identificar las aplicaciones y las plataformas consideradas críticas para la operación del negocio.
- Identificar al personal clave interno y externo requerido para la operación de las actividades críticas del negocio.
- Establecer los tiempos mínimos de recuperación requeridos en los que no se vea afectado el negocio.
- Definir la funcionalidad mínima que requiere el negocio en caso de contingencia.
- Identificar los riesgos presentes para la continuidad.
- Establecer los elementos esenciales requeridos en el plan de recuperación de desastres.
- Desarrollar procedimientos específicos y guías de operación en caso de desastre para cada uno de los servicios críticos vitales especificados en el alcance del plan.
- Desarrollar e impartir la capacitación inicial para el correcto funcionamiento del plan.
- Establecer un plan de prueba, gestión y mantenimiento necesarios para garantizar los objetivos del Plan.

Alcance

Seguros de que la información es el principal activo de cualquier organización, se hace necesario desarrollar procedimientos, normas y demás documentos que conlleven a la protección de todos los activos.

En este mundo globalizado donde los procesos administrativos y de servicios son gestionados a través de la prestación de servicios eficientes, donde la tecnología juega un papel importante. Surge la necesidad y responsabilidad de la protección de la información, medios tecnológicos y ambiente de operación.

La entidad cuenta con una plataforma tecnológica que le permite agilizar los procesos y el manejo eficiente de la información; la cual se convierte en la materia prima para la toma de decisiones y el cumplimiento de los objetivos misionales y estratégicos de la organización. Toda esta información almacenada en los activos de información se considera como uno de los elementos más importantes para el funcionamiento del INVISBU y su integridad está relacionada con la posibilidad de su pérdida, destrucción intencional o no intencional. En este sentido todos los funcionarios que trabajan para la organización tienen la responsabilidad directa o indirecta de ayudar a su buen uso y operación.
Por esto el INVISBU hace gestiones para la apropiación y adopción de medidas de seguridad con el fin de proteger dicha información, la continuidad de todas sus operaciones y la prestación de sus servicios.

Definiciones

Acceso: es la recuperación o grabación de datos que han sido almacenados en un sistema de computación.

Amenaza: cualquier cosa que pueda interferir con el funcionamiento adecuado de un computador o causar la difusión no autorizada de información confiada en un servidor. Ejemplo: Fallas de suministro eléctrico, virus, saboteadores o usuarios descuidados.

Análisis de Impacto en el Negocio o Business Impact Analysis (BIA por sus siglas en inglés): proceso de análisis de las actividades de negocio y las consecuencias que una interrupción sobre las mismas puede provocar en la organización.

Análisis de Riesgos: proceso de identificación, análisis y evaluación de riesgos.

Ataque: término general usado para cualquier acción o evento que intente interferir con el funcionamiento adecuado de un sistema informático, o intento de obtener de modo no autorizado la información confiada a un computador.

BCP: sigla en inglés (Business Continuity Plan) que hace referencia al Plan de Continuidad de Negocio, el cual integra el DRP, planes de contingencia y recuperación de procesos de la entidad, planes de emergencia, y plan de comunicación y administración de crisis.

Datos: los datos son hechos y cifras que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilizan como sinónimos. En su forma más amplia los datos pueden ser cualquier forma de información: campos de datos, registros, archivos y bases de datos, texto, hojas de cálculo, imágenes, vídeo, etc.

Equipos de cómputo: elementos o dispositivos de hardware, software, redes y telecomunicaciones interconectados que son utilizados para llevar a cabo las actividades operativas sistematizadas de la Institución.

Impacto: consecuencia evaluada de una interrupción.

Incidente: cuando se produce un ataque o se materializa una amenaza, como por ejemplo las fallas de suministro eléctrico o un intento de borrado de un archivo protegido.

Integridad: se refiere a que los valores de los datos se mantengan tal como fueron puestos intencionalmente en un sistema. Las técnicas de integridad sirven para prevenir que existan valores errados en los datos provocados por el software de la base de datos, por fallas de programas, del sistema, hardware o errores humanos.

ISO/IEC 27002: 2005 – código de buenas prácticas para la Gestión de la Seguridad de la Información. Es la antigua ISO 17799 y comprende un apartado dedicado especialmente a la continuidad de negocio.

Plan de contingencia: estrategia planificada con una serie de procedimientos que faciliten u orienten a tener una solución alternativa que permita restituir rápidamente los servicios de la Institución ante la eventualidad de todo lo que la pueda paralizar, ya sea de forma parcial o total.

Punto de Recuperación Objetivo – RPO (Recovery Point Objective por sus siglas en inglés): cantidad de información que la organización puede llegar a perder como consecuencia de un desastre. Marca desde un punto de vista tecnológico la estrategia de realización de copias de seguridad de la información.

Riesgo: probabilidad de que una amenaza aproveche y explote una debilidad asociada a un proceso/activo/recurso provocando daño sobre el mismo.

Sistema de Información: Organización sistemática para almacenar los datos de una organización y ponerlos a disposición de su personal.

Tiempo de Recuperación Objetivo - RTO (Recovery Time Objective por sus siglas en inglés): variable temporal dentro de la cual una actividad de negocio debe ser recuperada después de un desastre.

Plan de Continuidad de Negocio: Es un plan integral para la práctica de cómo una organización debe recuperar y restaurar sus funciones críticas parcial o totalmente interrumpidas dentro de un tiempo predeterminado después de una interrupción no deseada o desastre.

Procedimientos documentados que orientan a las organizaciones para responder, recuperar, reanudar y restaurar la operación a un nivel pre-definido de operación debido una vez presentada / tras la interrupción.

Plan de continuidad de las TICS: Es un documento que se diseña con la finalidad de saber cómo actuar frente a cualquier problema relacionado con el sistema informático de la organización, garantizando de esta forma la protección de los datos y su pronta recuperación en caso de pérdida.

Identificación Infraestructura Informática actual

En la actualidad el INVISBU posee una infraestructura tecnológica que garantiza la comunicación y funcionamiento de sus aplicativos; los cuales le permiten prestar servicio a sus clientes internos y externos.

Estos sistemas de información para su correcta operatividad se apoyan en:

- **La Red LAN:** de 96 puntos, con cableado UTP cat 6, 6 switches los cuales están disponibles en piso 3 y 4 del Edificio.
- **Red Wifi:** 2 access point marca Aruba, uno en cada piso con firewall incluido.
- **Rack de Comunicaciones:** con 2 Switches de 48 puertos, 6 switches adicionales en el 3er piso y 6 switches adicionales en el 4to piso.
- **Firewall(UTP) :** Un Fortinet para protección de la red de datos.
- **Equipos de Computador:** 50 Equipos de Escritorio y 6 Portátiles.
- **Servidores:** Un servidor HP “SERVER” en donde opera el SGC y un servidor HP en Linux en donde se encuentra operando el sistema SIGAPI.
- **UPS:** Una UPS de 2 KVA, 3 UPS de 700 Watt (Presupuesto, Contabilidad y Tesorería).
- **Impresoras:** 13 impresoras.

- **Escáner:** 8 Escáner.
- **Sistemas Operativos:** Sistema Operativo Windows Server R12, Windows 10, Windows 7.
- **Aplicativos:** Eco Financiero, Gd Histórico, Se paga admón. Anual, SGC y PQRS cedido por la alcaldía, SIGAPI sistemas de certificación de PH propio del INVISBU.
- **Servicio de Internet:** una línea con disponibilidad de 100 Mb y 3 IP públicas.
- **Servicio de Hosting:** 150 Gb, el cual soporte el Sitio WEB, FTP, algunos aplicativos y las cuentas de correo.
- **Antivirus:** 55 licencias Karpersky por un año.
- **PETI:** este es el plan estratégico de Sistemas en donde se proyecta y se direcciona la actividad anual a llevar a cabo por las TICS en el INVISBU.
- **Plan de Copias de Seguridad:** se hacen copias periódicas al sistema financiero, al sistema de correspondencia, propiedad horizontal, nómina y página WEB. Una copia al año a los computadores de escritorio de la entidad. Además, se hacen copias esporádicas a las cuentas de correos de la Dirección, Subdirector Financiero, Subdirector Técnico y Jefe de Oficina Jurídica.
- **Plan de Mantenimiento Preventivo:** se hace un mantenimiento preventivo a los computadores activos e impresoras que se tienen en la Entidad.
- **Plan de Seguridad y Privacidad de la Información**: plan anual en donde se plantean actividades relacionadas con MIPG y que tienen que ver con la seguridad de la información; las cuales se realizan en el año.
- **Plan de tratamiento de Riesgos de SPI:** en este documento se escribe todo lo relacionado con el manejo de los riesgos de la información.
- **Política de Protección de la Información de las Bases de datos Personales**: esta política fue adoptada desde el año 2019.
- **Página y Sitio WEB:** este es el sitio en el cual se encuentran publicados todos los documentos relacionados con la ley de transparencia y del derecho de acceso a la información (Ley 1712 de 2014).
- **Otros Elementos:** índice de información clasificada y reservada, relación de activos de información, plan de comunicaciones, etc.

Aspectos y criterios tenidos en cuenta en el Análisis de los Riesgos:

Tabla criterios para calificar el impacto (consecuencias) – Riesgo de gestión

NIVEL	IMPACTO (CONSECUENCIAS) CUANTITATIVO	IMPACTO (CONSECUENCIAS) CUALITATIVO
CATASTROFICO	• Impacto que afecta la ejecución presupuestal en un valor ≥ 50% • Perdida de cobertura en la prestación de los servicios de la entidad ≥ 50% • Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥ 50% • Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥ 50% del presupuesto general de la entidad	• Interrupción de las operaciones de la entidad por más de cinco (5) días. • Intervención por parte de un ente de control u otro ente regulador. • Perdida de la información crítica para la entidad que no se puede recuperar • Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal. • Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados.
MAYOR	• Impacto que afecte la ejecución presupuestal en un valor ≥ 20% • Perdida de cobertura en la prestación de los servicios de la entidad ≥ 20% • Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥ 20% • Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥ 20% del presupuesto general de la entidad	• Interrupción de las operaciones de la entidad por más de dos (2) días • Perdida de información crítica que puede ser recuperada de forma parcial o incompleta • Sanción por parte del ente de control u otro ente regulador • Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno • Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación del servicio a los usuarios o ciudadanos
MODERADO	• Impacto que afecte la ejecución presupuestal en un valor ≥ 5% • Perdida de cobertura en la prestación de los servicios de la entidad ≥ 10% • Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥ 5% • Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥ 5% del presupuesto general de la entidad	• Interrupción de las operaciones de la entidad por un (1) día • Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad • Inoportunidad en la información, ocasionando retrasos en la atención a los usuarios. • Reproceso de actividades y aumento de carga operativa • Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación • Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos. • Investigaciones penales, fiscales o disciplinarias.
MENOR	• Impacto que afecte la ejecución presupuestal en un valor ≥ 1% • Perdida de cobertura en la prestación de los servicios de la entidad ≥ 5% • Pago de indemnizaciones a terceros por acciones legales que puedan afectar el presupuesto total de la entidad en un valor ≥ 1% • Pago de sanciones económica por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥ 1% del presupuesto general de la entidad.	• Interrupción de las operaciones de la entidad por algunas horas • Reclamaciones o quejas de los usuarios, que implican investigaciones internas disciplinarias. • Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos.

INSIGNIFICANTE	• Impacto que afecte la ejecución presupuestal en un valor ≥ 0,5% • Perdida de cobertura en la prestación de los servicios de la entidad ≥ 1% • Pago de indemnizaciones a terceros por acciones legales que puedan afectar el presupuesto total de la entidad en un valor ≥ 0,5% • Pago de sanciones económica por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥ 0,5% del presupuesto general de la entidad.	• No hay interrupción de las operaciones de la entidad • No se generan sanciones económicas o administrativas • No se afecta la imagen institucional de forma significativa

Criterios para calificar el impacto – Riesgos de seguridad digital

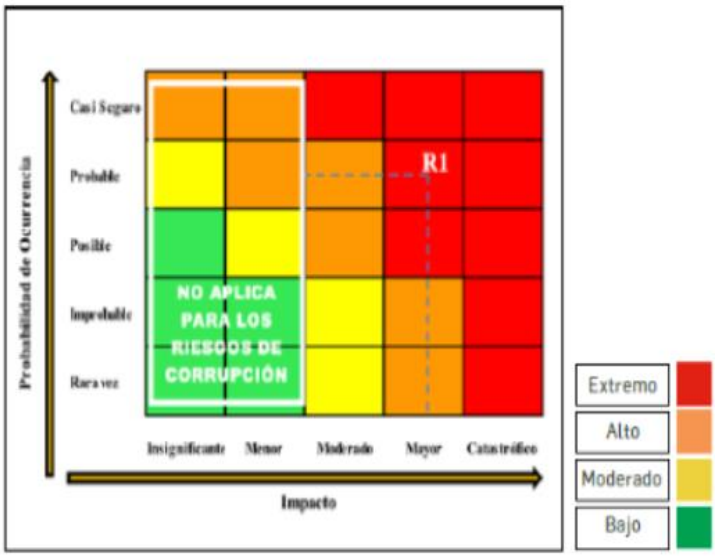
NIVEL	VALOR DEL IMPACTO	CRITERIOS DE IMPACTO PARA RIESGOS DE SEGURIDAD DIGITAL	
		IMPACTO (consecuencias) cuantitativo	IMPACTO (consecuencias) cualitativo
INSIGNIFICANTE	1	Afectación ≥ X% de la población Afectación ≥ X% del presupuesto anual de la entidad No hay afectación medioambiental	• Sin afectación de la integridad • Sin afectación de la disponibilidad • Sin afectación de la confidencialidad
MENOR	2	Afectación ≥ X% de la población Afectación ≥ X% del presupuesto anual de la entidad Afectación leve del medio ambiente requiere de ≥ X días de recuperación	• Sin afectación de la integridad • Sin afectación de la disponibilidad • Sin afectación de la confidencialidad
MODERADO	3	Afectación ≥ X% de la población Afectación ≥ X% del presupuesto anual de la entidad Afectación leve del medio ambiente requiere de ≥ X semanas de recuperación	• Afectación moderada de la integridad de la información debido al interés particular de los empleados y terceros. • Afectación moderada de la disponibilidad de la información debido al interés particular de los empleados y terceros. • Afectación moderada de la confidencialidad de la información debido al interés particular de los empleados y terceros.
MAYOR	4	Afectación ≥ X% de la población Afectación ≥ X% del presupuesto anual de la entidad Afectación leve del medio ambiente requiere de ≥ X meses de recuperación	• Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros. • Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. • Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.
CATASTROFICO	5	Afectación ≥ X% de la población Afectación ≥ X% del presupuesto anual de la entidad Afectación leve del medio ambiente requiere de ≥ X años de recuperación	• Afectación muy grave de la integridad de la información debido al interés particular de los empleados y terceros. • Afectación muy grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. • Afectación muy grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.

Criterios para calificar el impacto – riesgos de corrupción

No.	PREGUNTA: Si el riesgo de corrupción se materializa podría	RESPUESTA	
		SI	NO
1	¿ Afectar el grupo de funcionarios del proceso?		
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?		
3	¿Afectar el cumplimiento de misión de la entidad?		
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?		
6	¿Generar pérdida de recursos económicos?		
7	¿Afectar la generación de los productos o la prestación de servicios?		
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		
9	¿Generar pérdida de información de la entidad?		
10	¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?		
11	¿Dar lugar a procesos sancionatorios?		
12	¿Dar lugar a procesos disciplinarios?		
13	¿Dar lugar a procesos fiscales?		
14	¿Dar lugar a procesos penales?		
15	¿Generar pérdida de credibilidad del sector?		
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		
17	¿Afectar la imagen regional?		
18	¿Afectar la imagen nacional?		
19	¿Generar daño ambiental?		
Responder afirmativamente de UNA a CINCO preguntas(S) genera un impacto moderado Responder afirmativamente de SEIS a ONCE preguntas genera un impacto mayor			
Responder afirmativamente de DOCE a DIECINUEVE preguntas genera un impacto catastrófico			

MODERADO	Genera medianas consecuencias sobre la entidad
MAYOR	Genera altas consecuencias sobre la entidad
CATASTROFICO	Genera consecuencias desastrosas para la entidad

MAPA DE CALOR



Identificación de los elementos críticos (posibles contingencias) y riesgos relacionados con la información de las TICS.

En estos elementos se ubican a los procesos que permiten prestar servicio a los clientes internos o externos y si por algún motivo no se pueden realizar se pondría en riesgo el correcto funcionamiento de la entidad, la información financiera, contractual, de personal, archivo documental y de trámites, que permite cumplir los objetivos misionales, con la rendición de cuentas a los entes de control, con la transparencia y con las normas que enmarcan el manejo de lo público.

De esta forma se identifican los aspectos, las situaciones relacionadas con los procesos críticos, sus riesgos y el plan de contingencia para la continuidad:

1. **Red de comunicaciones local i/o de datos:**

Análisis de la situación: si en determinado momento hay fallas en la comunicación por la red local se puede asegurar que no se podrá prestar los servicios de ventanilla única, trámites en línea, registro de información en el sistema financiero, disponibilidad del uso de cuentas de correo a través de la intranet, acceso a la información y aplicativos que se encuentran en el servidor. En razón a esta posible situación se puede generar desinformación, falta de actualización de los sistemas de información, demora en la prestación del servicio, incumplimiento a las normas (transparencia, contractual, entes de control, etc.) y demora en los procesos internos (presupuesto, contabilidad, tesorería, nomina, contratos, tramites de propiedad horizontal, etc.).

Identificación del Riesgo: "Pérdida o afectación en la disponibilidad, integridad y confidencialidad de la Información".

Consecuencias:

a. Perdida de la información.
b. Insatisfacción del cliente.
c. Incumplimiento en la generación de información para usuarios internos y externos.
d. Pérdida de credibilidad para entidad.
e. Incumplimiento de la normatividad.

De acuerdo al mapa de riesgo de Gestión de la Información en el INVISBU su:

Probabilidad --------→ 1
Impacto----------→ 1
Nivel ----------→ Bajo

Posibles fallas:

Corte del cableado, conectores defectuosos, fallas en los switches, fallas en el servidor, corte del fluido eléctrico, etc.

Contingencia para la continuidad

- ✓ Se debe disponer probadores de comunicación de tal manera que en el menor tiempo posible se pueda revisar que exista o no comunicación.
- ✓ Disponer de cable de red, conectores, ponchadora para en el momento que se requiera se elabore un cable y se pueda reemplazar el cable defectuoso.
- ✓ Disponer de un switch de repuesto en el rack de comunicaciones; esto permitiría reemplazar el defectuoso y seguir prestando el servicio en un tiempo muy corto.
- ✓ Disponer de Equipo servidor o de equipos que permitan instalar rápidamente las aplicaciones y seguir prestando el servicio.
- ✓ Disponer de una UPS que le permita mantener el fluido eléctrico mientras se reestablece el corte en el edificio o ciudad.

2. Backup y copias de seguridad:

Análisis de la situación: si llegara a suceder un hecho poco común (inundación, terremoto, incendio, explosión, etc.) que no permitiera disponer de las instalaciones, ni de los equipos de cómputo, ni del edificio en donde funciona el INVISBU, muy seguramente se requeriría de copias de seguridad de la bases de datos que requieren los aplicativos (Eco Financiero, CGC y PQRS) para funcionar y así, con estos backups poder poner en funcionamiento los sistemas de información en otro lugar. Además puede acarrear demora en disponer de los servicios de información y de la función que cumple la entidad para los ciudadanos de esta municipalidad.

Identificación del Riesgo: "Incumplimiento en la realización de las copias de seguridad"

Consecuencias:

a. Perdida información

De acuerdo al mapa de riesgo de Gestión de la Información en el INVISBU su:

Probabilidad --------→ 1
Impacto----------→ 1
Nivel ----------→ Bajo

Posibles fallas:

Falta de planeación, falta de cronograma de copias de seguridad, falta de disponibilidad de recursos, incumplimiento del cronograma, falta de seguimiento a los indicadores de proceso, falta de seguimiento y control de los planes de seguridad.

Contingencia para la continuidad

- ✓ Elaborar un plan de copias de seguridad en donde encuentren consignados los procedimientos a seguir.
- ✓ Disponer de dispositivos de almacenamiento que faciliten realización de las copias y la mitigación del riesgo.
- ✓ Disponer de un hosting que tenga el espacio suficiente para mantener las copias

- ✓ Disponer de presupuesto que le permita la contratación de los servicios de hosting o de espacios en la nube o servidor externo.

3. Sistemas de Información o Aplicativos

Análisis de la situación: En caso de que se tengan aplicativos desactualizados, no disponer de mantenimiento adecuado, falta de licenciamiento, falta de integridad de la información, procedimientos obsoletos, falta de presupuesto, falta de equipos actualizados que no permitan el buen desempeño de los sistemas de información, falta de capacitación, falta de manuales que permitan generar el buen desempeño del personal que lo requiere, etc.

Identificación del Riesgo: "Desactualización de la infraestructura TIC"

Consecuencias:

a. Fallas en los equipos.
b. Deficiencias en la realización del trabajo.
c. Mala imagen corporativa, insatisfacción de usuarios internos y externos.
d. Falta de recursos.

De acuerdo al mapa de riesgo de Gestión de la Información en el INVISBU su:

e. Probabilidad --------→ 2
f. Impacto----------→ 3
g. Nivel ----------→ Moderado

Posibles fallas:

Bloqueo de los equipos de cómputo, Diseño errado de los Sistemas de información, Demora en el registro, proceso y resultados de la información, manuales obsoletos, desconocimiento de funcionamiento y operatividad del software, falta disponibilidad de recursos, falta de aplicación de las normatividad vigente, etc.

Contingencia para la continuidad

- ✓ Disponer recursos en el presupuesto anual que permitan la actualización de equipos de cómputo de última tecnología (Mantener política de equipos menores a 5 años) y el mantenimiento anual del sistema Eco financiero.
- ✓ Disponer de recursos para el licenciamiento del Software de aplicación del Sistema Financiero.
- ✓ Exigir a los terceros cuando se adquiere el software, que éste debe estar acorde a la normatividad vigente.
- ✓ Solicitar la capacitación y los manuales indicados para conocer y disponer del correcto uso de los aplicativos.

4. Dispositivos de Seguridad, Antivirus, Cortafuegos o Firewall (contra intrusos, virus, troyanos, ataques, etc.):

Análisis de la situación: Si una infraestructura de información no dispone de dispositivos de seguridad (corta fuegos) y antivirus que lo protejan contra acciones mal intencionadas; puede suceder que sus equipos (servidores y computadores de la red) estén vulnerables a robo de información, formateo de unidades de disco y disposición de software, que altere el correcto funcionamiento de sus impresoras y software en general. Además puede poner al descubierto pasabordos, claves y demás que pongan en riesgo los activos de la entidad; así como de sus cuentas bancarias.

Identificación del riesgo: "Desactualización de Software y de dispositivos relacionados con la seguridad de la información."

Consecuencias:

a. Fallas en los equipos.
b. Deficiencias en la realización del trabajo.
c. Mala imagen corporativa, insatisfacción de usuarios internos y externos.
d. Falta de recursos.
e. Mala planeación de requerimientos.
f. Deficiencia en el proceso de gestión de compra.

De acuerdo al mapa de riesgo de Gestión de la Información en el INVISBU su:

g. Probabilidad --------→ 2
h. Impacto----------→ 3
i. Nivel ----------→ Moderado

Posibles fallas: Bloqueo de equipos, información bloqueada, perdida de información, no poder entrar al equipo, se pueden realizar transacciones sin autorización, cambio sin consentimiento de las claves, secuestro de información, mal funcionamiento de impresoras, mal funcionamiento del software de gestión (Office), etc.

Contingencia para la continuidad

- ✓ Disponer de presupuesto para la compra y mantenimiento de dispositivos de seguridad de la red de datos.
- ✓ Comprar cortafuegos o firewall y antivirus que garanticen la filtración de intrusos y le den la seguridad a las transacciones en la red de datos.
- ✓ Cambio permanente de claves.
- ✓ Instalación de software la debe hacer el personal autorizado de las TICS.
- ✓ Revisión permanente con antivirus de USB, DVD, discos externos, correos, etc.
- ✓ Establecer protocolos para la gestión de compras que aseguren la agilidad de este proceso.

5. Servicio de Hosting o recursos en servidores externos

Análisis de la situación: Cuando se requiere trabajar con un sitio WEB se hace necesario por seguridad que sea en un servidor por fuera de las instalaciones de la Entidad ya que esto facilita y garantiza la seguridad de la información que dispone en la página WEB las 24 horas. Además permite disponer de las cuentas de correo institucionales protegidas y monitoreadas contra virus; también puede disponer de

espacio en disco para mantener copias de información más seguras y que minimizan el riesgo de la disponibilidad y el uso de la información.

Identificación del Riesgo: 1. "Desactualización de la infraestructura TIC" 2. "Pérdida o afectación en la disponibilidad, integridad y confidencialidad de la Información".

Consecuencias riesgo 1:

a. Fallas en los equipos.
b. Deficiencias en la realización del trabajo.
c. Mala imagen corporativa, insatisfacción de usuarios internos y externos.
d. Falta de recursos.

De acuerdo al mapa de riesgo de Gestión de la Información en el INVISBU su:

e. Probabilidad --------→ 2
f. Impacto----------→ 3
g. Nivel ----------→ Moderado

Consecuencias riesgo 2:

a. Perdida de la información.
b. Insatisfacción del cliente.
c. Incumplimiento en la generación de información para usuarios internos y externos.
d. Pérdida de credibilidad para la entidad.
e. Incumplimiento de la normatividad.

De acuerdo al mapa de riesgo de Gestión de la Información en el INVISBU su:

Probabilidad --------→ 1
Impacto----------→ 1
Nivel ----------→ Bajo

Posibles fallas: No disponibilidad de la página WEB, no disponibilidad del sitio externo para guardar copias de seguridad, **n**o poder enviar ni recibir correos corporativos, no poder correr aplicativos disponibles en la página WEB (PQRS), No poder cumplir con la ley de transparencia.

Contingencia para la continuidad

- ✓ Disponer de presupuesto anual para la contratación del servicio de hosting.
- ✓ Contratar empresas que tengan experiencia y cumplan los requisitos requeridos para el buen funcionamiento de las cuentas de correo institucionales, el correcto funcionamiento de la página WEB y que tengan disponibles las herramientas para el mantenimiento del sitio WEB.
- ✓ Contratar empresas que presten servicio en las horas en las que trabaja la organización.
- ✓ Contratar empresas que tengan a disposición personal técnico capacitado y con experiencia.
- ✓ Mantener copia periódica (Quincenal) de seguridad del sitio WEB.
- ✓ Disponer de personal técnico i/o profesional vinculado al INVISBU, que administre y haga el mantenimiento del sitio WEB.

Estrategias de Implementación de la Continuidad

- **Detección:** La continuidad de los servicios apoyados por las TICS se comprueba con el correcto funcionamiento de la página WEB, disponibilidad de la comunicación en la red de datos, servicio de correos y el correcto funcionamiento de los aplicativos en producción. Cualquier falla en alguno de estos elementos debe ser reportada al personal de las TICS i/o Subdirector Administrativo y Financiero.
  El monitoreo permanente de los elementos de la red de datos por parte del personal adscrito a las TICS, disminuirá el impacto de cualquier falla.
  El registro de las fallas en una bitácora de las TICS permitirá mejores análisis de cualquier evento.
- **Soporte:** Si cualquier persona vinculada a la entidad detecta una falla debe repórtala al personal adscrito a las TICS, que son las personas preparadas para abordar las anomalías y dar la posible solución.
- **Diagnóstico:** Quienes están capacitados para dar el diagnostico son las personas vinculadas al área de Tecnología de la Información de la Organización.
- **Escalamiento:** Cuando una falla o situación no pueda ser resuelta por el personal de Tecnología de la Información del INVSIBU, debe ser comunicada al Subdirector Administrativo y en su medida a la Dirección.
- **Restablecimiento del Servicio:** Una vez se adopten todas las medidas de contingencia expuestas en este documento; se podrá garantizar que el servicio se restablecerá en el menor tiempo posible una hora y en casos muy críticos en medio día.
- **Cierre:** Todo incidente o falla de la infraestructura de las TICS deberá ser registrada en una bitácora o documento (hoja de servicio) que permita el posterior análisis para la prevención de eventos de contingencia en el futuro.

Recomendaciones

- Cada funcionario debe velar por el buen uso los equipos asignados y no permitir su retiro por personas ajenas a la institución.
- Tener un sistema de control para entrada de personal ajeno a la entidad.
- Mantener el servicio de cámaras de seguridad.
- Recordar que el activo más importante de cualquier entidad pública es la información.
- Velar porque los usuarios internos protejan y le den buen uso a la información.
- Cumplir con la normatividad vigente en términos de manejo de bases de datos personales y uso de la información.
- Que los aplicativos tengan control de acceso y manejo de roles.
- Registrar en una bitácora cualquier anomalía de la infraestructura tecnológica.
- Mantener la diligencia en los procesos de gestión de compras.
- Disponer de presupuesto acorde a las necesidades de la organización.
- Estandarizar los procesos de contratación.
- Capacitar al personal de planta en los procesos relacionados con el cumplimiento de las normas ante los entes de control; garantizando de esta forma el cumplimiento de los mismos.
- Elaborar protocolos escritos de los procesos relacionados con los entes de control.