




Política de Continuidad de Procesamiento de Datos


Versión: 2.1

Confeccionó	Revisó	Aprobó
BDO Consultoría Externa	 Carla Leiva - CISO	 Francisco Canale - Director

POLÍTICA DE CONTINUIDAD DE PROCESAMIENTO DE DATOS	intiza
	Clasificación: Restringida
Tipo: Política	Fecha vigencia: 25/11/2024
Código: PO-TI-01- Continuidad de Procesamiento de Datos	Versión: 2.1

Contenido

1. Objetivo	2
2. Alcance	3
3. Responsabilidades	3
4. Desarrollo	4
4.1. Consideraciones Generales	4
4.2. Análisis de Riesgo	5
4.3. Elaboración de planes de continuidad del procesamiento	6
4.4. Pruebas de los planes de continuidad de procesamiento	7
4.5. Mantenimiento y reevaluación del plan	8
4.6. Esquema de Comunicación	9
4.7. Proveedores y Servicios Tercerizados	10
4.8. Lecciones Aprendidas	10
4.9. Capacitaciones y Plan de Concientización	10
5. Referencias	11
5.1. Normativa Relacionada	11
5.2. Definiciones	11
6. Historial de Versiones	12

POLÍTICA DE CONTINUIDAD DE PROCESAMIENTO DE DATOS	
	Clasificación: Restringida
Tipo: Política	Fecha vigencia: 25/11/2024
Código: PO-TI-01- Continuidad de Procesamiento de Datos	Versión: 2.1

1. Objetivo

Proveer un marco dentro del cual INTIZA, pueda minimizar la probabilidad de interrupciones del procesamiento relacionadas con los sistemas de información, minimizando el impacto de cualquier interrupción, haciendo foco en el mantenimiento de las operaciones de negocio al nivel más alto de servicio posible, asegurando un rápido restablecimiento de las operaciones normales luego de un incidente relativo a los sistemas.

2. Alcance


Esta política aplica a todos los recursos donde se dispone la información de INTIZA que almacenan, procesan o transmiten datos sensibles de negocio, incluyendo aplicaciones, servidores, redes y cualquier proceso o procedimiento por el cual estos sistemas son administrados y/o mantenidos.

También debe servir de guía para evaluar los planes de recuperación ante desastres de cualquiera de los socios de negocio de INTIZA.

3. Responsabilidades

Es responsabilidad de **Seguridad de la Información** mantener actualizada la presente política y asegurar que los procesos y actividades que deriven de la gestión de una contingencia se realicen en un marco de seguridad de la información aceptable.

Tecnología es responsable de establecer las herramientas necesarias para asegurar un rápido restablecimiento de las operaciones normales luego de un incidente relativo a los sistemas, y establecer un plan de continuidad de procesamiento de datos minimizando el impacto de cualquier interrupción.


POLÍTICA DE CONTINUIDAD DE PROCESAMIENTO DE DATOS	
	Clasificación: Restringida
Tipo: Política	Fecha vigencia: 25/11/2024
Código: PO-TI-01- Continuidad de Procesamiento de Datos	Versión: 2.1

El **Comité de Seguridad** tiene la responsabilidad de aprobar el plan de continuidad de procesamiento y velar por que el mismo se cumpla de acuerdo a lo establecido con el fin de garantizar la continuidad del negocio.

4. Desarrollo

4.1. Consideraciones Generales

- Asegurar la continuidad de las operaciones de INTIZA, tanto para soportar una crisis que deriva en una contingencia como para la vuelta a la normalidad en tiempo y forma.
- Fortalecer la resistencia del negocio ante interrupciones en las operaciones que fueran ocasionados por eventos maliciosos.
- Proteger y asegurar la imagen institucional de la empresa.
- Aumentar la disponibilidad de los recursos y las operaciones del negocio.
- Definir los lineamientos a seguir, antes, durante y después de una interrupción en las operaciones de la empresa.
- Responder de forma asertiva y oportunamente ante eventos que afecten los servicios de INTIZA.
- Posibilitar una respuesta adecuada y oportuna ante la materialización de un riesgo de seguridad o medio ambiente que provoque una brecha de continuidad en el negocio.
- Garantizar la preservación de los datos y funciones esenciales.
- Asegurar que el Plan de Continuidad sea actualizado en el tiempo, manteniendo así su vigencia sobre los procesos alcanzados.
- Atender los riesgos a los cuales está expuesto, en relación a contingencias que les puedan acontecer a sus proveedores críticos.

POLÍTICA DE CONTINUIDAD DE PROCESAMIENTO DE DATOS	
	Clasificación: Restringida
Tipo: Política	Fecha vigencia: 25/11/2024
Código: PO-TI-01- Continuidad de Procesamiento de Datos	Versión: 2.1

- Debe existir un Plan de Continuidad de Procesamiento de Datos el cual debe mantenerse por medio de revisiones y actualizaciones anuales o cuando lo amerite para garantizar su eficacia en el tiempo.
- Amerita hacer una revisión y/o actualización cuando se detecten:
 - Cambios de procesos, de productos y/o servicios.
 - Modificaciones a nivel de organización (Ejemplo: nuevos sectores, divisiones, sucursales.)
 - Cambios de sistemas.
 - Cambios importantes de volúmenes de empresa.
 - Cambios importantes de dotación (fundamentalmente en cuanto al “árbol de llamadas”).

4.2. Análisis de Riesgo

Se debe realizar un análisis de todas las amenazas que podrían interrumpir el funcionamiento de la infraestructura tecnológica de procesamiento de información identificada como crítica para el negocio.

Cada amenaza debe ser identificada y para cada una de ellas se debe evaluar la probabilidad de que ésta ocurra y el impacto que puede tener sobre el funcionamiento del equipo de procesamiento.

Estas actividades deben llevarse a cabo con la activa participación de los Responsables de cada una de las áreas donde se ejecutan los procesos de negocio y de la infraestructura tecnológica, para definir de forma correcta el impacto y los tiempos de recuperación.

El Análisis de Riesgo debe contemplar los siguientes aspectos:

Se debe realizar, al menos, una vez al año y después de implementar cambios significativos en el entorno (por ejemplo, adquisiciones, fusiones o reubicaciones, etc.).

POLÍTICA DE CONTINUIDAD DE PROCESAMIENTO DE DATOS	intiza
	Clasificación: Restringida
Tipo: Política	Fecha vigencia: 25/11/2024
Código: PO-TI-01- Continuidad de Procesamiento de Datos	Versión: 2.1

Debe identificar activos críticos, amenazas y vulnerabilidades.

Los resultados deben formar parte de un análisis formal y documentado de riesgo.

4.3. Elaboración de planes de continuidad del procesamiento

Los planes deben ser desarrollados para mantener o restablecer las operaciones de procesamiento en los plazos definidos una vez ocurrida una interrupción o falla en la infraestructura tecnológica de procesamiento de información de los procesos críticos de negocio.

El proceso de planificación de la continuidad del procesamiento debe considerar los siguientes puntos:

- Identificación y acuerdo con respecto a todas las responsabilidades y procedimientos de emergencia.
- Implementación de procedimientos de emergencia para permitir la recuperación y restablecimiento en los plazos definidos.
- Documentación de los procedimientos y procesos acordados.
- Instrucción adecuada del personal en materia de procedimientos y procesos de emergencia acordados, incluyendo el manejo de crisis.
- Prueba y actualización de los planes.

El proceso de planificación debe priorizar la infraestructura tecnológica de procesamiento identificadas como críticas para INTIZA. Deben considerarse los servicios y recursos que pueden permitir que esto ocurra, incluyendo dotación de personal, recursos que no procesan información, así como acuerdos para reanudación de emergencia en sitios alternativos de procesamiento de la información.

El plan de continuidad debe especificar claramente las condiciones para su puesta en marcha, así como las personas responsables de ejecutar cada componente del mismo. Cuando se

POLÍTICA DE CONTINUIDAD DE PROCESAMIENTO DE DATOS	intiza
	Clasificación: Restringida
Tipo: Política	Fecha vigencia: 25/11/2024
Código: PO-TI-01- Continuidad de Procesamiento de Datos	Versión: 2.1


identifican nuevos requerimientos o cambios en la forma de operación, deben modificarse de conformidad los procedimientos de emergencia establecidos.

El marco para la planificación de la continuidad del procesamiento debe tener en cuenta los siguientes puntos:

- Condiciones de implementación de los planes que describan el proceso a seguir antes de poner en marcha los mismos.
- Procedimientos de emergencia que describan las acciones a emprender una vez ocurrido un incidente que ponga en peligro la continuidad del procesamiento.
- Procedimientos de emergencia que describan las acciones a emprender para el traslado de actividades esenciales de la empresa o de servicios de soporte a ubicaciones transitorias alternativas, y para el restablecimiento del procesamiento de información de los procesos de negocio.
- Procedimientos de recuperación que describan las acciones a emprender para restablecer el procesamiento normal de INTIZA.
- Un cronograma de mantenimiento que especifique cómo y cuándo se debe probar el plan, y el proceso para el mantenimiento del mismo.
- Actividades de concientización e instrucción que estén diseñadas para propiciar la comprensión de los planes de continuidad del procesamiento y garantizar que los mismos sigan siendo eficaces.
- Descripción de los responsables de la ejecución de cada uno de los componentes del plan. Se deben mencionar alternativas cuando corresponda.
- Cada plan debe tener un propietario específico, el cual es responsable del mismo.

4.4. Pruebas de los planes de continuidad de procesamiento

Los planes de continuidad del procesamiento pueden fallar en el curso de las pruebas, frecuentemente debido a suposiciones incorrectas, negligencias o cambios en el equipamiento

POLÍTICA DE CONTINUIDAD DE PROCESAMIENTO DE DATOS	
	Clasificación: Restringida
Tipo: Política	Fecha vigencia: 25/11/2024
Código: PO-TI-01- Continuidad de Procesamiento de Datos	Versión: 2.1

o el personal. Por consiguiente deben ser probados al menos una vez al año para garantizar que se encuentren actualizados y sean eficaces.

Las pruebas también deben garantizar que todos los miembros del equipo de recuperación y demás personal relevante estén al corriente de los planes.

El cronograma de pruebas para los planes de continuidad del procesamiento debe indicar cómo y cuándo debe probarse cada elemento del plan.

Se debe coordinar la prueba de cada uno de los componentes del plan. Se deben utilizar diversas técnicas para garantizar que los planes funcionen en una situación real.

Estas deben incluir:

- Pruebas de discusión de diversos escenarios (discutiendo medidas para la recuperación del procesamiento utilizando ejemplo de interrupciones).
- Simulaciones (especialmente para entrenar al personal en el desempeño de sus roles de gestión posterior a incidentes o crisis).
- Pruebas de recuperación técnica (garantizando que los sistemas de información puedan ser establecidos con eficacia).
- Pruebas de recuperación en un sitio alternativo (ejecutando procesos de negocio en paralelo, con operaciones de recuperación fuera del sitio principal).
- Pruebas de infraestructura y servicios de proveedores (garantizando que los productos y servicios de proveedores externos cumplan con el compromiso contraído).
- Ensayos completos (probando que el personal, el equipamiento y la infraestructura pueden afrontar las interrupciones).

Estas técnicas deben reflejar la naturaleza del plan de recuperación desarrollado.

POLÍTICA DE CONTINUIDAD DE PROCESAMIENTO DE DATOS	intiza
	Clasificación: Restringida
Tipo: Política	Fecha vigencia: 25/11/2024
Código: PO-TI-01- Continuidad de Procesamiento de Datos	Versión: 2.1

4.5. Mantenimiento y reevaluación del plan

Los planes de continuidad del procesamiento deben mantenerse mediante revisiones y actualizaciones periódicas para garantizar su eficiencia permanente.

Se debe asignar la responsabilidad por las revisiones periódicas del plan de continuidad del procesamiento.

Algunas de las situaciones que pueden demandar la actualización de los planes son:

- Cambios en las disposiciones relativas al negocio
- Adquisición de nuevo equipamiento o cambios en la infraestructura tecnológica
- Actualización de los sistemas operacionales
- Cambios de distinta índole como:
 - Personal.
 - Direcciones o números telefónicos.
 - Procesos críticos identificados por el negocio.
 - Ubicación y recursos.
 - Contratistas, proveedores y clientes claves.

4.6. Esquema de Comunicación

Para satisfacer todas las necesidades de comunicación interna y externa, se debe establecer un esquema de comunicación ante eventos de contingencia y catástrofes que contenga:

- Globalmente, lo que se debe decir y a qué nivel de detalle,
- Quién o quiénes lo debe/n decir,
- Manejo de atención al cliente,
- Cómo, Cuándo y a quiénes deberán transmitir el mensaje
- Preguntas frecuentes a las que se deberá dar una respuesta.

POLÍTICA DE CONTINUIDAD DE PROCESAMIENTO DE DATOS	intiza
	Clasificación: Restringida
Tipo: Política	Fecha vigencia: 25/11/2024
Código: PO-TI-01- Continuidad de Procesamiento de Datos	Versión: 2.1

- Recursos Humanos será la encargada de la comunicación externa con entes gubernamentales y/o regulatorios, medios de información pública, entes de control público, etc. cuando sea necesario.

4.7. Proveedores y Servicios Tercerizados


- A la hora de la contratación de servicios y proveedores para procesos críticos, se deberá considerar acuerdos con proveedores que cuenten con planes de continuidad, que los mismos sean probados y documentados dejando evidencias a disposición de INTIZA para su revisión cuando lo considere oportuno.

4.8. Lecciones Aprendidas

- Como resultado de una declaración de “estado de contingencia”, se deberá documentar cómo ha sido determinado, supervisado, analizado, contenido el evento hasta retomar a su situación normal.
- En caso de que los eventos que interrumpieron las operaciones, no hayan ameritado una declaración de “estado de contingencia”, se deberá generar documentación correspondiente sobre la situación.
- Toda documentación, será resguardada por el responsable de Seguridad de la Información para posibles auditorías.

4.9. Capacitaciones y Plan de Concientización

- Se deben realizar capacitaciones a los colaboradores sobre lo que se espera de ellos en una situación crítica. De estas capacitaciones debe quedar evidencia asegurando que la persona haya comprendido sus obligaciones.

POLÍTICA DE CONTINUIDAD DE PROCESAMIENTO DE DATOS	
	Clasificación: Restringida
Tipo: Política	Fecha vigencia: 25/11/2024
Código: PO-TI-01- Continuidad de Procesamiento de Datos	Versión: 2.1


5. Referencias

5.1. Normativa Relacionada

Categoría	Título	Código
Plan	Plan de Continuidad de Procesamiento de datos	PL-TI-01
Procedimiento	Continuidad de Procesamiento de datos	PR-TI-05

5.2. Definiciones

Término	Descripción
Gestión de Continuidad del Negocio (BCM-Business Continuity Management)	Proceso de Gestión holístico que identifica las amenazas potenciales para una organización y el impacto en las operaciones de negocio que esas amenazas podrían causar si se materializan.
Plan de continuidad del negocio (BCP-Business Continuity Plan):	Conjunto de procedimientos documentados, recursos y sistemas que conducen a una respuesta después de una interrupción. Un plan documentado y probado con el fin de responder ante una emergencia de manera adecuada, logrando así el mínimo impacto a la operación del negocio.
Plan de Contingencia	Es un subconjunto de un plan de continuidad de negocio, que contempla cómo reaccionar ante una contingencia que pueda afectar la disponibilidad o los servicios ofrecidos por los sistemas

POLÍTICA DE CONTINUIDAD DE PROCESAMIENTO DE DATOS	
	Clasificación: Restringida
Tipo: Política	Fecha vigencia: 25/11/2024
Código: PO-TI-01- Continuidad de Procesamiento de Datos	Versión: 2.1

	informáticos. Una contingencia puede ser un problema de corrupción de datos, suministro eléctrico, un problema de software o hardware, errores humanos, intrusión etc.
--	--

6. Historial de Versiones

Versión	Fecha	Resumen de Cambios
1.0	01/11/2021	Creación de la política de Continuidad del Negocio.
1.0	02/05/2022	Aprobado por Comité de Dirección: MI-DI-03- Minuta de Comité de Dirección N° 3
2.0	13/07/2022	Se modifica código y nombre del documento, objetivo, alcance y responsabilidades. Se agrega contenido de detalle.
2.0	11/10/2022	Aprobado por Comité de Dirección: MI-DI-06- Minuta de Comité de Dirección N° 6.
2.1	22/11/2024	Se revisó el documento confirmando su vigencia.
2.1	25/11/2024	Aprobado por Comite.