# PLAN DE RECUPERACIÓN DE DESASTRES

**TIPO DE DOCUMENTO:** Procedimiento

**CÓDIGO:** PRO GSI 100

## I. AUTORIZACIONES

| *Elaboró:* | *Revisó:* | *Autorizó:* |
|---|---|---|
| | | |
| Ing. Salvador Santiago Araujo<br><br>Gerente Administrativo | *Lic. Irais Dafne Mendoza Sánchez*<br><br>*Director General Adjunto* | *C.P. Jerónimo Javier Mendoza Lara / Lic. Irais Dafne Mendoza Sánchez*<br><br>*Director General / Director General Adjunto* |

Última revisión: Octubre 2025

No. de versión: 2

Fecha de emisión: Octubre 2021

Revisó: DGE

Aprobó: DGE

ÍNDICE

CONTENIDO PÁGINA



## II. HISTORIAL DE CAMBIOS

| Versión | Descripción de Cambios | Autor | Fecha |
|---|---|---|---|
| 1 | Versión inicial. | RFML / AFR | Octubre 2021 |
| 2 | Adecuaciones Generales | SSA | Enero 2022 |

## III. Abreviaciones y definiciones

Abreviaciones:

| | |
|---|---|
| DGE | Director General / Director General Adjunto |
| SGSI | Sistema de Gestión de Seguridad de la Información |
| GAD | Gerente Administrativo |

Definiciones:

| | |
|---|---|
| Integridad: | Propiedad de la información relativa a su exactitud y completitud. |
| Confidencialidad: | Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. |
| Disponibilidad: | Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada. |
| Acción correctiva: | Acción tomada para eliminar la(s) causa(s) de una no conformidad y evitar que vuelva a ocurrir. |
| Riesgo: | Efecto de la incertidumbre. |

## 1. INTRODUCCION

El presente documento contempla el plan de recuperación de TI para las áreas operativas y administrativas de la empresa, realizado como parte para la implementación de las normas y gestión de la seguridad de información en el centro de datos de CONSULTORES E INVESTIGADORES EN ADMINISTRACIÓN S.C., CIA INTEGRACIÓN S.R.L. DE C.V., AEQUITAS ADMINISTRADORA DE ACTIVOS S.R.L. DE C.V.

## 2. OBJETIVO

Los objetivos del plan de recuperación de TI para las áreas operativas y administrativas de CONSULTORES E INVESTIGADORES EN ADMINISTRACIÓN S.C., CIA INTEGRACIÓN S.R.L. DE C.V., AEQUITAS ADMINISTRADORA DE ACTIVOS S.R.L. DE C.V.

- Minimizar el grado de la interrupción, el daño y el impacto asociado a los procesos críticos del negocio, frente al escenario de contingencia definido.
- Proporcionar los mecanismos para una rápida y adecuada restauración de las operaciones tecnológicas en las instalaciones alternas a ser definidas por la dirección general de CONSULTORES E INVESTIGADORES EN ADMINISTRACIÓN S.C., CIA INTEGRACIÓN S.R.L. DE C.V., AEQUITAS ADMINISTRADORA DE ACTIVOS S.R.L. DE C.V.

## 3. ALCANCE

El presente plan de recuperación de TI aplica para las áreas operativas y administrativas dentro del SGC y SGSI se encuentra cubriendo lo siguiente:

- Procesos críticos de CONSULTORES E INVESTIGADORES EN ADMINISTRACIÓN S.C., CIA INTEGRACIÓN S.R.L. DE C.V., AEQUITAS ADMINISTRADORA DE ACTIVOS S.R.L. DE C.V.
- Soportados por el centro de datos, lo cuales fueron identificados en el análisis y apreciación de riesgos de acuerdo con las normas UNE EN ISO 9001:2015 y UNE EN ISO / IEC 27001:2013.
- Sistemas de Información existentes dentro de los centros de Datos localizados en las Sedes Nezahualcóyotl (corporativo), Insurgentes Sur, Toluca y que brindan soporte a los procesos críticos del negocio.

## 4. DESCRIPCIÓN DEL DRP

Supuestos del Plan

El presente plan de recuperación de desastres será desarrollado con base en los siguientes supuestos:

- La recuperación se realizará en el centro de datos alternos que la empresa disponga y que la dirección general y/o gerencia administrativa autorice.
- La infraestructura de contingencia debe encontrarse operativa, para lo cual el centro de datos alterno debe encontrarse en línea y operando adecuadamente, lo cual debe ser controlado a través del monitoreo continuo.
- Al momento del desastre, todos los participantes del equipo de sistemas se encontrarán disponibles para las tareas encomendadas.
- La documentación técnica se encontrará actualizada y disponible.
- El plan ha sido distribuido, mantenido y actualizado; y el personal se encuentra capacitado para su uso.
- El tipo de contingencia considerado para el presente trabajo es la detención o destrucción (total o parcial) de los Centros de Datos de las sedes principales de CONSULTORES E INVESTIGADORES EN ADMINISTRACIÓN S.C., CIA INTEGRACIÓN S.R.L. DE C.V., AEQUITAS ADMINISTRADORA DE ACTIVOS S.R.L. DE C.V, ubicados en:

    - **Oficina Nezahualcóyotl:** Av. Lago de Xochimilco No. 283, Col. Ampliación Vicente Villada, Municipio Ciudad Nezahualcóyotl, Estado de México, C.P. 57760.
    - **Oficina de Insurgentes Sur:** Insurgentes Sur No. 686, Piso 9, Col. Del Valle, Delegación Benito Juárez, Ciudad de México, C.P. 03100.
    - **Oficina Toluca:** Hermenegildo Galeana No. 204, Despacho 2, Col. Centro, Municipio Toluca, Estado de México, C.P. 50000.

- El evento de desastre puede referirse a desastres naturales, sociales o por fallas tecnológicas, se deberá seguir el **PLAN DE PROTECCIÓN CIVIL CIA PRO DIR 001.**
- Los equipos de comunicación y los equipos de procesamiento de información ubicados en los centros de datos de las sedes principales de la empresa, están disponibles en todo momento para realizar sus funciones normales.
- Las operaciones deben ser restablecidas en un centro de datos alterno a ser definido por la dirección general y gerencia administrativa.

**Equipos de Recuperación de Desastres**

Esta sección identifica a los equipos de personas involucradas en el esfuerzo de recuperación del evento de desastre y sus responsabilidades asociadas. Las pautas consideradas para la conformación de estos equipos han sido los siguientes:

- Todo equipo debe estar conformado por un líder y un alterno.

- Ninguna persona debe estar participando en más de un equipo cuyas tareas durante la recuperación de un desastre, sean concurrentes.
- Todas las personas identificadas en el equipo de recuperación de desastres deben conocer las responsabilidades que tienen que asumir. De esta manera se minimiza las posibilidades de inoperatividad de los equipos debido a la ausencia de sus integrantes y/o al desconocimiento de sus responsabilidades.

Se ha conformado el siguiente Equipo de Recuperación de Desastres TI:

## Gerente Administrativo

Tiene asignado las siguientes responsabilidades:

1. Encargado de coordinar, dirigir y decidir respecto a acciones o estrategias a seguir en un escenario de contingencia dado.
2. Tomar la decisión de activar el plan de recuperación de desastres TI.
3. Proveer liderazgo general a los equipos de personas involucrados en el proceso de recuperación.
4. Guiar al personal necesario durante la situación de contingencia y supervisar sus actividades.
5. Evaluar la extensión del desastre y sus consecuencias potenciales sobre la infraestructura tecnológica.
6. Notificar, y mantener enterados, a la alta dirección acerca del evento de desastre, el progreso de la recuperación y posibles problemas ocurridos durante la ejecución del plan.
7. Documentar los eventos de desastres y las actividades realizadas para lograr la recuperación de las operaciones.
8. Monitorear la ejecución de los procedimientos de recuperación y asegurar que el cronograma y las prioridades establecidas se cumplan.
9. Supervisar / vigilar la recuperación de infraestructura de TI en el centro de datos alternos.
10. Contactar a los proveedores para el hardware y/o software de reemplazo para sistemas afectados.
11. Asistir a las reuniones del estado de la recuperación y comunicar al personal las necesidades y prioridades.
12. Declarar el evento de término de la ejecución de las operaciones del plan de recuperación de desastres, cuando las operaciones del centro de datos afectado hayan sido restablecidas.

## Coordinador de Sistemas TI

Tiene asignado las siguientes responsabilidades:

1. Evaluar el daño en la plataforma tecnológica básica de la empresa, coordinar y dirigir las acciones necesarias para su recuperación en el centro de datos alterno y su restauración a condiciones normales.
2. Recuperar la plataforma base de los sistemas críticos de la empresa, de acuerdo con la prioridad de recuperación definida.
3. Asegurar que toda la documentación relacionada con estándares, operaciones, registros vitales, programas de aplicación, etc., se encuentren almacenados en un ambiente seguro.
4. Mantener los procedimientos de operaciones actualizados para soportar cualquier sistema (aplicativo) fuera de la empresa.
5. Mantener actualizado y en un lugar seguro la configuración del sistema alterno.
6. Supervisar la instalación del hardware y software base, así como configurar las últimas versiones de los sistemas operativos, en los ambientes del centro de datos alterno.
7. Recuperar las cintas de respaldo del almacenaje externo y entregarlas al sitio de recuperación.
8. Habilitar los procedimientos de respaldos y restablecer los controles normales de operación en el centro de datos primario luego de restablecidos los servicios en dicho ambiente.
9. Mantener, recuperar y/o restaurar los enlaces de red y comunicaciones entre la sede principal y el centro de datos alterno.
10. Mantener actualizado el diagrama actual de conexiones de dispositivos, el diagrama alterno y el inventario de equipos.

11. Evaluar el daño en las redes de comunicación de datos y coordinar las estrategias de recuperación con los proveedores de servicios.

## Auxiliar de Sistemas

Tiene asignado las siguientes responsabilidades:

1. Levantar los servicios de base de datos, con la data restaurada, válida, íntegra, probada y disponible para los usuarios, en el centro de datos alternos.
2. Informar a los usuarios hasta qué momento se tienen datos confiables.
3. Velar por el funcionamiento adecuado de las bases de datos.
4. Supervisar el correcto funcionamiento de los diferentes sistemas de aplicación.
5. Asegurar que la documentación de los aplicativos en producción se mantenga actualizada y que la documentación de operaciones contemple las actividades de respaldo de los aplicativos.
6. Establecer los requerimientos de sistema operativo, archivos utilitarios, librerías y documentación indispensable para la operatividad de los aplicativos.
7. Mantener informados a los usuarios clave del negocio acerca del avance de las actividades de recuperación y el restablecimiento de cada uno de los procesos críticos que son de su responsabilidad.
8. Validar con el usuario del negocio acerca del adecuado desempeño de las aplicaciones posterior al restablecimiento de las operaciones en el Centro de Datos alterno.

## Coordinador de Sistemas de Gestión

Tiene asignado las siguientes responsabilidades:

1. Supervisar el cumplimiento de los controles que permitan asegurar la integridad, confidencialidad y disponibilidad de la información durante la situación de contingencia.
2. Documentar con el Coordinador de Sistemas TI y Gerente administrativo, las acciones llevadas a cabo, así como el resultado de estas acciones, esto se documentará en el **formato de incidentes FOR GSI 024**.

# 5. PLAN DE PRUEBAS

Este plan está compuesto, de una serie de actividades orientadas a mantener actualizado y vigente el Plan de Recuperación de Desastres TI. Estas pruebas están enmarcadas dentro del **FOR GSI 050 Simulacro**, y se compone de las siguientes partes:

1. Definir el propósito de la prueba.
2. Definir la prueba.
3. Designar el equipo de prueba.
4. Estructurar los aspectos a probar.
5. Ejecutar las pruebas.
6. Analizar los resultados y modificar el Plan de Recuperación de Desastres TI, si fuese necesario.

Estrategias de prueba

Existen varias estrategias que pueden ser adoptadas para probar el plan:

| Tipo de Prueba | Descripción |
|---|---|
| Prueba de Recorrido | El objetivo de esta prueba es hacer seguimiento a los documentos del plan disponibles para validar su adecuada definición y factibilidad de aplicación en la empresa. |
| Verificación Manual | El objetivo de esta prueba es asegurar la disponibilidad de los materiales de recuperación requeridos según se estableció en el plan. Esta prueba requiere revisar toda la data requerida, suministros y/u otras copias impresas de documentos que se encuentran en la actualidad respaldados y correctamente resguardados externamente. |
| Ensayo Estructurado | El objetivo de esta prueba es liderar el equipo hacia una recuperación simulada a fin de determinar la suficiencia del plan.<br><br>La prueba se debe conducir como sigue:<br><br>• Todos los líderes de equipo se reúnen en una habitación donde se les hará entrega del escenario a probar.<br>• Cada uno debe trabajar sus procedimientos de recuperación prestando, particular atención en la interacción con los otros equipos.<br>• Los puntos identificados se anotarán y se les hará seguimiento. |
| Convocatoria no anunciada del equipo de recuperación TI | El objetivo de esta prueba es asegurar que la lista de equipos de movilización de recuperación se encuentre al día y que los equipos puedan ser movilizados en el momento requerido. Esta prueba debe ser conducida en tiempos diferentes (fuera y durante horas de trabajo) a manera de identificar cualquier defecto en el plan. |
| Prueba Paralela | El objetivo de la prueba paralela es verificar el correcto funcionamiento del centro de datos alterno, validando que los equipos y aplicaciones funcionen correctamente, soporten la carga de trabajo estimada en contingencia y que se cumpla con los tiempos estimados de recuperación.<br><br>Esta prueba se realiza solo en el centro de datos alterno sin afectar las operaciones del centro de datos primario.<br><br>Al igual que en las otras pruebas, se deben tomar notas de fallas y posibles mejoras identificadas para poder actualizar y mejorar el plan.<br><br>Se debe involucrar a personal de las áreas de negocio para que las pruebas incluyan la aprobación y observaciones de estos con respecto a sus expectativas de funcionalidad y rendimiento. |

| | |
|---|---|
| Prueba Total | Al igual que en la prueba paralela, se busca verificar el correcto funcionamiento del centro de datos alterno, sin embargo, la prueba total es más completa, e incluye la desactivación del Centro de Datos primario para mayor realismo de la prueba.<br><br>Este tipo de pruebas deben realizarse en momentos de carga de trabajo baja para el negocio y de preferencia en fines de semana largos, del mismo modo se debe involucrar al personal de TI y personal vital involucrado de las áreas de negocio. |

## 6. METODOLOGÍA BIA

El Análisis de Impacto en el Negocio (BIA) es un proceso que tiene por objetivo determinar, de acuerdo con la misión de la empresa, las funciones críticas del negocio y sus recursos críticos asociados.

Esto se logra al:

- Identificar todos los procesos de negocio de la organización.
- Identificar todas las aplicaciones que soportan esos procesos.
- Determinar el tiempo de recuperación objetivo en el ciclo de vida de cada proceso.
- Determinar si el proceso es crítico para el negocio.
- Estimar la pérdida potencial y el tiempo de recuperación.
- Determinar los niveles de importancia de los procesos vitales para el negocio.

El desarrollo del Análisis de Impacto en el Negocio (BIA) se describe en las siguientes fases:


Análisis de Datos

Durante esta fase se realizó la tabulación de los resultados, desarrollando las siguientes actividades:

- Identificar los valores de RTO y RPO por cada uno de los procesos de negocios.
- Identificar y tabular los resultados del impacto financiero y operacional.
- Priorizar los procesos de negocio de acerado al RTO obtenido.

- Presentar los resultados a la dirección general.
- Obtener la aprobación de los resultados por parte de las áreas usuarias y la dirección general.

Consolidación y Análisis de Datos a nivel Empresa

Durante esta fase se consolidó los resultados obtenidos en la fase anterior, presentando a manera de gráfico el resultado del Análisis de Impacto de Negocio, definiendo luego las estrategias de recuperación y respaldo para cada uno de los activos de información asociados.

## 7. PRIORIDAD DE RECUPERACIÓN (ANÁLISIS DE DATOS)

La prioridad de recuperación de los sistemas se define de acuerdo con los resultados del BIA desarrollado en la organización.

Al identificar los procesos críticos, se ha llegado a la siguiente lista de procesos cuya recuperación debe realizarse de acuerdo con la prioridad indicada (RTO) en la siguiente tabla:

| Proceso de Negocio | Tolerancia RTO (horas) | Tiempo de RPO % |
|---|---|---|
| Proceso de Recursos Humanos | 2 | 1 |
| Proceso de Sistemas | 1 | 0 |
| Proceso de Contabilidad y Tesorería | 2 | 1 |
| Proceso de Compras | 2 | 1 |
| Proceso de Investigación de crédito | 1 | 0 |
| Proceso de Gestión Domiciliaria | 1 | 0 |
| Proceso de Cobranza Punta – Punta | 1 | 0 |
| Proceso de Recuperación de Cartera | 1 | 0 |

Donde el RTO es: Tiempo de Recuperación Objetivo (Recovery Time Objective por sus siglas en inglés), indica el tiempo que puede transcurrir desde la declaración de contingencia al punto de reanudación de las operaciones del negocio.

Donde el RPO es: Punto de Recuperación Objetivo (Recovery Point Objective por sus siglas en inglés), índica en % cuanta información podría ser perdida (tolerancia de pérdida) en caso de presentarse una interrupción en el proceso de negocio.

Con el objetivo de agrupar los procesos cuyo RTO justifique una misma estrategia de recuperación y agrupar los procesos cuyo RPO justifique una misma estrategia de respaldo de información se aplica la siguiente escala:

| Escala | Codificación | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| RTO (hrs) | de 1 a 2 | de 3 a 4 | de 5 a 8 | de 9 a 24 | De 25 a 72 | de 73 a más |
| RPO % | 0 | de 1 a 2 | de 3 a 4 | de 5 a 8 | de 9 a 24 | de 25 a más |

La escala indica, por ejemplo, que para procesos donde el RTO está entre 1 y 2 horas se le asigna un factor de uno; para un proceso donde el RTO está entre 3 y 4 horas se le asigna un factor de dos y así sucesivamente. De esta manera se logra generar la siguiente tabla ordenando los procesos por criticidad en el RTO:

| Procesos de la empresa | Siglas | Tolerancia sin Sistema (RTO) | Tiempo Máx. de Pérdida de Datos (RPO%) |
|---|---|---|---|
| Proceso de Recursos Humanos | RRHH | 2 | 1 |
| Proceso de Sistemas | TI | 1 | 0 |
| Proceso de Contabilidad y Tesorería | CONTA | 2 | 1 |
| Proceso de Compras | COM | 2 | 1 |
| Proceso de Investigación de crédito | INV CRE | 1 | 0 |
| Proceso de Gestión Domiciliaria | GES DOM | 1 | 0 |
| Proceso de Cobranza Punta – Punta | CPP | 1 | 0 |
| Proceso de Recuperación de Cartera | REC CAR | 1 | 0 |

Si bien se cuenta con los procesos del negocio con los factores (escalas) de RTO y RPO, se debe determinar, dentro de cada escala, que proceso se recupera primero y cuál después. Es decir, un segundo nivel de criticidad de estos.

Para estimar esta criticidad, en cada proceso, se utiliza el cuestionario BIA. Particularmente la sección referida al impacto operacional cualitativo. Para el impacto operacional cualitativo se solicitó a la Dirección General indicar la severidad de cada uno de los impactos operacionales, mostrados a continuación, concernientes a su área de negocio en un rango de 1 a 5. Donde 1 es leve y 5 es muy severo.

| # | Impacto Operacional | Valor |
|---|---|---|
| 1. | Competitividad | 1 A 5 |
| 2. | Control financiero | 1 A 5 |
| 3. | Credibilidad frente al estado | 1 A 5 |
| 4. | Empleados resignados | 1 A 5 |
| 5. | Imagen de la compañía | 1 A 5 |
| 6. | Imagen de la gerencia | 1 A 5 |
| 7. | Incremento del riesgo | 1 A 5 |
| 8. | Moral | 1 A 5 |
| 9. | Obligaciones legales | 1 A 5 |
| 10. | Productividad | 1 A 5 |

| # | Impacto Operacional | Valor |
|---|---|---|
| 11. | Cumplimiento Regulatorio | 1 A 5 |
| 12. | Relación con proveedores | 1 A 5 |
| 13. | Relaciones con la ciudadanía | 1 A 5 |
| 14. | Relaciones con terceros | 1 A 5 |
| 15. | Relaciones laborales | 1 A 5 |
| 16. | Reportes financieros | 1 A 5 |
| 17. | Servicio al cliente | 1 A 5 |
| 18. | Servicio de proveedores | 1 A 5 |
| 19. | Violaciones legales / fiscales | 1 A 5 |
| 20. | Otros | 1 A 5 |

Esta información se coloca en la tabla a continuación (se presenta en dos tablas para efectos de mejor visualización) para obtener los promedios de criticidad por cada proceso del negocio:

| | RRHH | TI | CONTA | COM | INV CRE | GES DOM | CPP | REC CAR |
|---|---|---|---|---|---|---|---|---|
| Competitividad | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 |
| Control financiero | 3 | 5 | 5 | 4 | 5 | 5 | 5 | 5 |
| Credibilidad frente al estado | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 |
| Empleados resignados | 0 | 5 | 0 | 0 | 5 | 5 | 5 | 5 |
| Imagen de la compañía | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 |
| Imagen de la gerencia | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 |
| Incremento del riesgo | 3 | 5 | 5 | 4 | 5 | 5 | 5 | 5 |
| Moral | 4 | 5 | 5 | 5 | 5 | 5 | 5 | 5 |
| Obligaciones legales | 4 | 5 | 5 | 1 | 5 | 5 | 5 | 5 |
| Productividad | 4 | 5 | 4 | 3 | 5 | 5 | 5 | 5 |
| Cumplimiento Regulatorio | 4 | 5 | 5 | 2 | 5 | 5 | 5 | 5 |
| Relación con proveedores | 3 | 5 | 4 | 5 | 5 | 5 | 5 | 5 |
| Relaciones con la ciudadanía | 5 | 5 | 3 | 4 | 5 | 5 | 5 | 5 |
| Relaciones con terceros | 3 | 5 | 4 | 2 | 5 | 5 | 5 | 5 |
| Relaciones laborales | 5 | 5 | 4 | 2 | 5 | 5 | 5 | 5 |
| Reportes financieros | 0 | 5 | 5 | 5 | 5 | 5 | 5 | 5 |
| Servicio al cliente | 4 | 5 | 4 | 3 | 5 | 5 | 5 | 5 |
| Servicio de proveedores | 2 | 5 | 2 | 5 | 5 | 5 | 5 | 5 |
| Violaciones legales / fiscales | 5 | 5 | 5 | 3 | 5 | 5 | 5 | 5 |
| Otros factores | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| TOTAL | 70 | 96 | 81 | 69 | 96 | 96 | 96 | 96 |
| Criticidad | 0.70 | 0.96 | 0.81 | 0.69 | 0.96 | 0.96 | 0.96 | 0.96 |

La criticidad se obtiene dividiendo los valores colocados por el usuario entre el máximo puntaje.

Por ejemplo, en el caos de los Procesos del PRONAMA (PRO) la criticidad es de 34/100 = 0.34.

Si se aplica la criticidad obtenida a los procesos ya clasificados, de acuerdo con la escala mencionada anteriormente, se obtiene el orden de recuperación:

| Proceso de Negocio | Siglas | Criticidad | Tolerancia (RTO) | Tiempo (RPO) | Prioridad |
|---|---|---|---|---|---|
| Proceso de Investigación de crédito | INV CRE | 0.96 | 1 | 0 | 1 |
| Proceso de Gestión Domiciliaria | GES DOM | 0.96 | 1 | 0 | 1 |
| Proceso de Cobranza Punta – Punta | CPP | 0.96 | 1 | 0 | 1 |
| Proceso de Recuperación de Cartera | REC CAR | 0.96 | 1 | 0 | 1 |
| Proceso de Sistemas | TI | 0.96 | 1 | 2 | 1 |
| Proceso de Contabilidad y Tesorería | CONTA | 0.81 | 3 | 2 | 2 |
| Proceso de Recursos Humanos | RRHH | 0.70 | 2 | 2 | 3 |
| Proceso de Compras | COM | 0.65 | 4 | 3 | 4 |

Si bien el BIA contempla factores de tipo cuantitativo, en varios de los casos, los usuarios no pudieron determinar el costo asociado de no contar con su proceso operativo ante el escenario de un desastre. Debido a nuestra experiencia, la aproximación mediante un enfoque cualitativo permite realizar una priorización adecuada de la criticidad de los procesos, mostrada anteriormente.

Los requisitos especiales del negocio están formados por los tiempos de recuperación indicados por los usuarios (RTO) y el impacto operacional. Así mismo, los registros vitales fueron indicados por los usuarios como condiciones especiales.

## 8. Aplicaciones asociadas a los procesos

Seguidamente, para el orden de recuperación de los procesos obtenido, se asocian las aplicaciones necesarias para el funcionamiento de estos.

| Cod | Procesos de Negocio | Aplicación |
|---|---|---|
| INV CRE | Proceso de Investigación de crédito | • Opti-Risk<br>• ERP<br>• Office 365<br>• Portal RPPyC<br>• Correo Electrónico |
| GES DOM | Proceso de Gestión Domiciliaria | • ERP<br>• Correo Electrónico<br>• Office 365 |
| CPP | Proceso de Cobranza Punta – Punta | • Bluemessagin<br>• Office 365<br>• Bonsaif<br>• Sicob<br>• Correo Electrónico |
| REC CAR | Proceso de Recuperación de Cartera | • Office 365<br>• Bonsaif<br>• Sicob<br>• Correo Electrónico |
| TI | Proceso de Sistemas | • Sistemas Operativos<br>• Antivirus<br>• Bases de Datos<br>• Aplicativos Desarrollos Internos<br>• CIA- Desk<br>• Office 365<br>• Microsoft Exchange<br>• Sicob |
| CONTA | Proceso de Contabilidad y Tesorería | • Portal SAT<br>• ASPEL<br>• Office 365<br>• Correo Electrónico |

| Cod | Procesos de Negocio | Aplicación |
|---|---|---|
| RRHH | Proceso de Recursos Humanos | • Circulo Laboral<br>• Portales Bolsas de Empleo<br>• Correo electrónico<br>• WhatsApp<br>• Office 365<br>• File Maker |
| COM | Proceso de Compras | • Portales E-Commerce proveedores<br>• Office 365<br>• Correo Electrónico |

## 9. ESTRATEGIAS POSIBLES DE RECUPERACIÓN

Debido a los tiempos de recuperación (RTO) mencionados anteriormente, es necesario contar con un Centro de Datos alterno que garantice la recuperación de los procesos críticos de la organización en el menor tiempo posible.

La ubicación del centro de datos alterno, y los servidores que debe contener el mismo, puede estar dentro de las instalaciones de la empresa o en un ambiente administrado por un tercero (Hosting).

Teniendo estas consideraciones, el Centro de datos alterno contaría:

| Servidor | Características |
|---|---|
| Servidor CIASC (1) | Procesador Intel Xeon Dual-Core, 6 GB RAM, 1 Disco 500 GB, 4 Interfase de Red. |
| Servidor CIASC (2) | Procesador Intel Xeon Dual-Core, 8 GB RAM, 1 Disco 500 GB, 4 Interfase de Red. |

Así mismo, el centro de datos alterno necesita contar con los siguientes equipos de comunicación y respaldo:

| Equipo de Comunicación | Detalle |
|---|---|
| Switch del CD Alterno | Switch el cual permite la conexión entre los servidores albergados en el Centro de datos alterno y Firewall del Centro de datos alterno. Características técnicas: Cisco 10/100/1000 Mbps Capa 3. |
| Firewall del CD Alterno | Firewall para proteger los servidores del centro de datos alterno. Dicho equipo debe poseer los servicios de VPN habilitados. |
| Router del CD Alterno | Rutear el tráfico desde el centro de datos alterno hacia las redes IP Características técnicas: 3 interfaces FastEthernet, 2 puertos Channelized E1/PRI, Cisco IOS Software o el recomendado por el proveedor en turno. |

| | |
|---|---|
| Solución de bakcup | La solución de backup permitirá respaldar y restaurar la información de la compañía en el centro de datos alterno. Características técnicas: PC de 64bits para uso del software DataProtector. Liberia con 2 bocas y 60 slots (incluye cables de conexión). |

## 10. PROCEDIMIENTO DE ACTIVACIÓN DEL PLAN

Este procedimiento tiene como objetivo evaluar el desastre al cual se ve enfrentado el centro de datos primario de la empresa, tomando las acciones correspondientes en caso de una situación de emergencia.

Equipo de evaluación del desastre, se encuentra conformado por:

- Gerente Administrativo.
- Coordinador de Sistemas TI.
- Auxiliar de Sistemas.

El siguiente diagrama muestra los criterios que deberán ser usados para activar el plan de recuperación de desastres TI:

Debe notarse que una interrupción no es solamente un evento que reduce la efectividad de los sistemas, es un evento extraordinario que causa una pérdida de procesos de negocio clave y tiene un impacto alto en la organización.

Situaciones que pueden convertirse en una emergencia:

- Incendios
- Terremoto
- Sobre carga / falta de energía
- Inundaciones
- Huelgas
- Falla en los sistemas ambientales
- Mal tiempo

En una situación de emergencia, se deberá proceder de la siguiente manera:

| Acción | Descripción | Responsabilidad | Referencia |
|---|---|---|---|
| Recibir Notificación | Cuando se presente una situación de emergencia, ésta deberá ser notificada al personal de sistemas. | Todos los empleados de la empresa | • CIA-Desk<br>• Correo Electrónico<br>• Llamada Telefónica<br>• Cualquier medio de comunicación disponible para con el área de |

| Acción | Descripción | Responsabilidad | Referencia |
|---|---|---|---|
| | | | sistemas y gerencia administrativa |
| Confirmar Notificación | Cuando la notificación de una contingencia potencial es recibida, se debe obtener una descripción breve de la naturaleza del incidente y cualquier tipo de daño.<br>Si es necesario, se debe confirmar que la notificación es verídica a través de un medio secundario.<br>El medio secundario puede ser otra persona que presenció el hecho y de ser posible documentarlo en correo electrónico. | Personal de Sistemas | N/A |
| Contactar servicios de emergencia | Si la situación lo amerita, se deberá efectuar el contacto con los servicios de emergencia. Situaciones que pueden ser consideradas de emergencia son mencionadas anteriormente. | Personal de Sistemas | Directorio de contacto con autoridades. |
| Reunión de coordinación | Coordinar una reunión a la brevedad posible con el Equipo de Recuperación, con la finalidad de hacer una evaluación preliminar de los daños.<br>Dependiendo de la criticidad del desastre, esta reunión se puede realizar en el local del Centro de Datos primario o en un lugar cercano al mismo.<br>Notificar a la brigada de protección civil interna de la empresa. | Comité de Plan de Recuperación de Desastres | N/A |
| Evaluar el Incidente | Evaluar el incidente de desastre y determinar la cantidad de tiempo requerido para completar la reparación. | Equipo de Evaluación del Desastre | **Formato de incidentes de SI FOR GSI 024**. |

| Acción | Descripción | Responsabilidad | Referencia |
|---|---|---|---|
| | El daño ocasionado a la infraestructura y a las instalaciones deberá ser evaluado y documentado. | | |
| Declarar la Contingencia | En caso de que el tiempo requerido para completar la reparación de los daños sea mayor al tiempo de recuperación requerido por el negocio, se declara la situación de emergencia y se da por activado el plan de recuperación de desastres. | Equipo de Evaluación del Desastre | **Formato de incidentes de SI FOR GSI 024.** |
| Alistar los recursos requeridos para el Centro de Datos alterno | Proveer transporte para el equipo de recuperación, personas y suministros requeridos para el restablecimiento de las operaciones en el centro de datos alterno. | Gerente Administrativo / Dirección General | Autos Utilitarios de la empresa. |
| Alertar personal involucrado | Se debe alertar a todos los miembros del Equipo de Recuperación que no se encuentren presentes al momento de la declaración de la situación de emergencia. Progresivamente avisar y orientar al resto del personal de la empresa. | Personal de Sistemas / Brigada de Protección Civil Interna (en caso de ser necesario) | Directorio del Equipo de Recuperación de Desastres |
| Ejecutar el Procedimiento General de Recuperación | Iniciar las actividades de recuperación en el centro de datos alterno de acuerdo con los procedimientos de recuperación definidos más adelante.<br>Este incidente debe ser registrado dentro del **Formato de incidentes de SI FOR GSI 024.** | Coordinador de Recuperación de TI | **Formato de incidentes de SI FOR GSI 024.** |

## 11. PROCEDIMIENTO GENERAL DE RECUPERACIÓN

Este procedimiento general tiene como objetivo la activación del centro de datos alterno para el restablecimiento de la totalidad de operaciones tecnológicas requeridas para garantizar la continuidad de los procesos críticos de la empresa, identificados como resultado del BIA.

Es importante mencionar que existen procesos como la recuperación de la central telefónica, internet, el correo y dominio que forman parte de las acciones a realizar y han sido colocados de acuerdo con su dependencia con el resto de los procesos del negocio.

A continuación, se detallan las acciones que conforman el procedimiento general de recuperación:

| Acción | Descripción | Responsabilidad | Referencia |
|---|---|---|---|
| Contactar al Equipo de Recuperación de TI | El Equipo de Recuperación debe ser notificado y movilizado a las instalaciones del Centro de Datos alterno. | Personal de Sistemas | Directorio del Equipo de Recuperación de Desastres |
| Notificar al proveedor de comunicaciones | Notificar al proveedor de comunicaciones acerca de la situación de desastre e indicar que puede haber cambios en la configuración. Detallar la información que se ha perdido y debe ser recuperada. Dejar constancia de la notificación. | Gerente Administrativo | Directorio de Proveedores / **Formato de incidentes de SI FOR GSI 024.** |
| Activar el Centro de Datos alterno | Declarar el Centro de Datos alterno como Centro de Datos de contingencia. Se debe revisar el checklist de Requisitos en el Centro de Datos Alterno.<br>Adicionalmente, se deberá tener en cuenta los insumos, adicionales al HW y SW críticos, para el correcto funcionamiento de este. | Coordinador de TI / Gerente Administrativo | Requisitos en el Centro de Datos Alterno |
| Identificar la pérdida de plataforma tecnológica | Utilizar el Inventario de Hardware para identificar la infraestructura tecnológica perdida en el Centro de Datos primario y generar informe. | Coordinador de Sistemas TI / Gerente Administrativo | **GLPI**. |

| Acción | Descripción | Responsabilidad | Referencia |
|---|---|---|---|
| Determinar los equipos que pueden ser reutilizados | Determinar equipos que puedan ser reutilizados luego de la contingencia. Revisar su operatividad, y confiabilidad, para validar que la misma no se haya visto afectada como consecuencia del evento de desastre ocurrido en el Centro de Datos primario. Generar informe con los equipos a reutilizar. (documento de salida). | Coordinador de Sistemas TI / Gerente Administrativo | **GLPI** |
| Determinar necesidades adicionales y coordinar compras de emergencia | Determinar los elementos adicionales que son necesarios para facilitar la recuperación de los procesos críticos. Estos artículos se deben comprar inmediatamente. Es importante definir los requerimientos necesarios para dejar el centro de datos de contingencia operativos. | Gerente Administrativo | N/A |
| Recuperar copias de seguridad de aplicaciones | Recuperar, de ser necesarias las copias de seguridad, ya sean del Centro de Datos y restaurar la información. | Coordinador de Sistemas TI | N/A |
| Preparar la plataforma tecnológica para la recuperación de los procesos | De ser necesario coordinar, la instalación de software base, aplicar parches, restaurar los últimos backups y aplicar scripts de recuperación, sobre la plataforma tecnológica del Centro de Datos alterno (documento de salida). | Coordinador de Sistemas TI / Gerente Administrativo | N/A |