

	POLÍTICA DE CONTINUIDAD DE NEGOCIO	PL - GSI - 04	
		Revisión	2
		Página	1 de 8
	POLÍTICA		

Política de Continuidad de Negocio

INFORMACIÓN PÚBLICA

	POLÍTICA DE CONTINUIDAD DE NEGOCIO		PL - GSI - 04	
			Revisión	2
	POLÍTICA		Página	2 de 8

INDICE

I. INTRODUCCIÓN	3
1.1. Presentación	3
1.2. Objetivo	3
1.3. Referencias	3
1.4. Alcance.....	3
1.5. Responsables.....	3
II. REGLAS DE LA POLÍTICA.....	4
1. Propósitos del Plan de Continuidad del Negocio.....	4
2. Establecer un sistema de administración de continuidad del negocio.....	4
3. Evaluación del Riesgo y el Impacto.....	4
4. Recopilación de antecedentes.	5
5. Estrategias de Continuidad y Recuperación.....	5
6. Organización y documentación del Plan	6
7. Acciones durante el desastre	6
8. Entrenamiento	6
9. Procedimientos de Pruebas	7
III. CONTROL DE CAMBIOS.....	8

	POLÍTICA DE CONTINUIDAD DE NEGOCIO		PL - GSI - 04	
			Revisión	2
	POLÍTICA		Página	3 de 8

I. INTRODUCCIÓN

1.1. Presentación

Esta Política define las reglas y criterios de seguridad que rigen la confección del Plan de Continuidad del Negocio para Novared. Dicho Plan debe permitir la más pronta recuperación de los servicios críticos frente a desastres donde todas o parte de sus operaciones, servicios computacionales y/o servicios de comunicaciones se vuelven inutilizables.

1.2. Objetivo

Novared debe contar con un Sistema de Gestión de Continuidad del Negocio, formalmente escrito, divulgado, probado y actualizado, que contemple los principales procedimientos para la recuperación de los servicios críticos frente a desastres identificables.

1.3. Referencias

PR-GSI-03 Plan de Contingencias
 PR-GCN-01 Plan de Gestión de Crisis de Novared Chile
 PR-GSI-09 Plan de Restauración
 PR-GSI-07 Plan BCPIT - DRP Novared

1.4. Alcance

- Eventos que puedan afectar los recursos computacionales, materiales, humanos o de comunicaciones, definidos como críticos para Novared.
- Riesgos sobre recursos computacionales materiales, humanos y de comunicaciones que puedan producir desastres para el servicio Novared.
- Plan de Continuidad del Negocio, con procedimientos específicos y prácticas generales para Novared.

1.5. Responsables

- En el ámbito estratégico, el Comité de Crisis es el encargado de aprobar el resultado y conclusiones de la Evaluación de Riesgo y del Plan de Continuidad del Negocio.
- En el ámbito táctico, un Comité Ejecutivo formado por el Gerente de Ingeniería y Soporte, el Gerente de Servicios Gestionados, debe efectuar la Evaluación de Riesgo y luego desarrollar el Plan de Continuidad del Negocio.

	POLÍTICA DE CONTINUIDAD DE NEGOCIO		PL - GSI - 04	
			Revisión	2
	POLÍTICA		Página	4 de 8

- Al nivel operativo, se establecen grupos de respuesta ante incidentes específicos, los que deben responder por la ejecución de las acciones definidas en el plan, para cada unidad, función o servicio y se encuentran definidos en el Plan de Gestión de crisis de Novared Chile.

II. REGLAS DE LA POLÍTICA

1. Propósitos del Plan de Continuidad del Negocio.

1.1 Los propósitos fundamentales del Plan de Continuidad del Negocio son:

- Asegurar la recuperación de los procesos de los servicios de Novared ante eventos que afecten la continuidad del servicio
- Minimizar el tiempo de restauración de servicios
- Minimizar la toma de decisiones durante un incidente
- Mejorar la confiabilidad de los sistemas en escenarios de incidentes
- Proveer directrices para las pruebas
- Disponer de planes alternativos para los usuarios

2. Establecer un sistema de administración de continuidad del negocio

2.1 Debe existir un proceso administrado para el desarrollo y la mantención de la continuidad del negocio.

2.2 Este proceso debe considerar:

- Evaluación de impacto
- Evaluación de riesgo
- Estrategias de recuperación
- Desarrollo de un plan de continuidad
- Entrenamiento
- Prueba del plan de continuidad
- Mantención del plan de continuidad

3. Evaluación del Riesgo y el Impacto

3.1 Identificar los escenarios de desastre conocidos que se pudieran manifestar, a fin de contemplar procedimientos y controles de mitigación específicos para ellos.

3.2 Se debe preparar un análisis de riesgo y un análisis del impacto del negocio que incluya la evaluación frente a los posibles eventos identificados.

3.3 La evaluación de riesgo debe determinar cuáles son las funciones críticas y una ponderación de la criticidad, incluyendo tiempo máximo de no-disponibilidad tolerable por cada función.

	POLÍTICA DE CONTINUIDAD DE NEGOCIO		PL - GSI - 04	
			Revisión	2
	POLÍTICA		Página	5 de 8

4. Recopilación de antecedentes.

4.1 Para cada función crítica identificada, deben recopilarse los siguientes antecedentes mínimos:

- Ubicación de sitios alternativos.
- Recursos.
 - Inventario de hardware.
 - Inventario de software.
 - Inventario de sistemas.
- Contactos.
 - Nómina de Personal clave.
 - Nómina de Personal de respaldo.
 - Nómina de proveedores y sus contactos.
 - Nómina de números telefónicos críticos.
- Información.
 - Información utilizada.
 - Registros relevantes.
 - Ubicaciones de los respaldos de datos.
- Documentación.
 - Políticas y procedimientos.
 - Inventario de formularios.
 - Seguros y contratos vigentes.
 - Nómina de regulaciones aplicables.
 - Checklist para notificaciones.
 - Documentación de aplicaciones.

5. Estrategias de Continuidad y Recuperación

- Se deben evaluar las alternativas posibles y adoptar la más adecuada en función de su precio/rendimiento para el procesamiento específico en cada escenario de desastre contemplado, y prácticas genéricas para el resto de los casos.
- Se deben considerar aspectos como:
 - Instalaciones.
 - Hardware y software.
 - Comunicaciones.
 - Archivos de datos.
 - Servicios a clientes.
 - Equipos humanos de emergencia involucrados.
- Procedimientos documentados de las actividades críticas automáticas y manuales
- Formación constante del personal
- Segregación de habilidades claves, con el fin de evitar la concentración y dependencia del personal
- Disponibilidad de trabajo remoto de manera segura

	POLÍTICA DE CONTINUIDAD DE NEGOCIO		PL - GSI - 04	
			Revisión	2
	POLÍTICA		Página	6 de 8

- Sistemas de Alimentación eléctrica Ininterrumpido
- Controles medioambientales en los Centros de datos
- Seguridad física de acceso a sectores críticos de la empresa
- Planes de Recuperación de Desastres (DRP) en base a escenarios de fallas
- Esquema de almacenamiento y respaldo de data (Backups)
- Servicios y suministros prestados por diferentes proveedores de TI
- Análisis de riesgo de eventos simultáneos a los Centros de Procesamiento de Datos Alterno

6. Organización y documentación del Plan

6.1 Se deben construir los procedimientos específicos para los escenarios de desastre reconocidos que componen el Plan, y a la vez un conjunto de prácticas generales a ser consideradas frente a escenarios no contemplados.

6.2 Los procedimientos deben incluir, por ejemplo:

- Propósito.
- Responsables de su ejecución.
- Alcance.
- Material de referencia.
- Documentación de los formularios que se emplearán durante la ejecución del procedimiento.
- Checklist de autorizaciones.
- Políticas aplicables al procedimiento.
- Esquema de revisión de cumplimiento

7. Acciones durante el desastre

7.1 En todo desastre se deben cumplir las siguientes etapas, las que deben ser registradas.

- Detección y escalamiento inicial del evento de seguridad.
- Ponderación de la gravedad.
- Declaración formal del evento como desastre.
- Activación de procedimientos ad-hoc del Plan para el escenario identificado.
- Procedimiento de retorno a la normalidad.
- Evaluación post-desastre del cumplimiento y efectividad del Plan.

8. Entrenamiento

8.1 Se debe entrenar adecuadamente a los involucrados en los planes de continuidad de negocio para que puedan llevar a cabo los procedimientos definidos

	POLÍTICA DE CONTINUIDAD DE NEGOCIO		PL - GSI - 04	
	POLÍTICA		Revisión	2
			Página	7 de 8

9. Procedimientos de Pruebas

9.1 El Plan debe ser cuidadosamente probado y evaluado en forma periódica, anualmente a lo menos.

9.2 Los procedimientos de pruebas deben estar documentados.

9.3 Las pruebas se deben orientar a:

- Determinar la factibilidad y compatibilidad de las instalaciones y los procedimientos de respaldo.
- Identificar áreas donde sea necesario modificar el Plan.
- Proveer entrenamiento al personal involucrado.
- Demostrar la capacidad de la organización para recuperarse.
- Efectuar correcciones necesarias.

INFORMACIÓN PÚBLICA

	POLÍTICA DE CONTINUIDAD DE NEGOCIO		PL - GSI - 04	
			Revisión	2
	POLÍTICA		Página	8 de 8

III. CONTROL DE CAMBIOS

Revisión	Elaborado por	Fecha	Revisado por	Fecha	Aprobado por	Fecha	Modificaciones
0	ESG	Febrero-2019	Hermann Obermoller	Febrero-2019	Rodrigo Sain	Febrero-2019	Definición de la política, como parte de los procesos de mejora interna
NN	ESG	Agosto-2019	Hermann Obermoller	Agosto-2020	Rodrigo Sain	Agosto-2020	Se revisa procedimiento- sin cambios
NN	ESG	Junio-2021	Hermann Obermoller	Junio-2021	Rodrigo Sain	Junio-2021	Se revisa procedimiento- sin cambios
NN	ESG	Julio-2022	Hermann Obermoller	Julio-2022	Rodrigo Sain	Julio-2022	Se revisa procedimiento- sin cambios
1	ESG	Julio-2023	Hermann Obermoller	Julio-2023	Rodrigo Sain	Julio-2023	Se revisa procedimiento- se actualiza referencias
2	ESG/Consultoría Externa	Diciembre 2024	Hermann Obermoller /ESG	Diciembre 2023	Comité de Seguridad	Enero 2024	Se actualiza documento de acuerdo a SGCN

DOCUMENTO VIGENTE

INFORMACIÓN