PROPUESTA DE UN MODELO DE PLAN DE CONTINUIDAD: UN ESTUDIO DE CASO

Dante Carrizo
Departamento de Ingeniería y Cs de la Informática, Universidad de Atacama
Copiapó, 1530000, Chile

Andrés A. Alfaro
Departamento de Ingeniería y Cs de la Informática, Universidad de Atacama
Copiapó, 1530000, Chile.

Rodrigo Loyola
Departamento de Ingeniería y Cs de la Informática, Universidad de Atacama
Copiapó, 1530000, Chile.

RESUMEN

Contexto, este trabajo se enmarca en la presentación de un estudio de caso de implementación de una variante del modelo de continuidad de negocio, el objetivo es presentar una variante del modelo Business Continuity Institute (BCI), a través de un caso de estudio, ejecutado en la minera Del Cobre Método, la variante de la propuesta (BCI-v) presenta siete fases para la creación y desarrollo de un Plan de Continuidad del Negocio, a través de BCI-v, la institución logra estar preparada para cualquier eventual emergencia, sabiendo como responder a un acontecimiento, a través de este modelo se pretende dar una guía para ante cualquier catástrofe, la empresa disminuir sus riesgos y continuar con su funcionamiento.

.

1. INTRODUCCIÓN.

En una encuesta de 94 organizaciones de Australia en 1999-2000, la mayoría de los organizaciones afirmaron que el tiempo más largo que podría estar fuera de acción es de menos de 24 horas. Además el 30% de estas organizaciones, dijo que su mayor tiempo fuera de servicio fue de menos de 8 horas [7]. Esto es quizás un instructivo para reflejar que en los posteriores años el mundo ha experimentado grandes ataques terroristas en las ciudades capitales, invasión de Irak, tsunamis en China. etc. Chile en los últimos años fue afectado por varias catástrofes siendo una de los más importantes el terremoto del 2010 que afectó principalmente el centro-sur del país, además de tsunamis, temblores e inundaciones, junto con algunos incendios provocando cortes de luz, desconexiones. etc. Debido a estos acontecimientos se debe llegar a pensar en la implementación de un Business Continuity Planninges. La creciente dependencia y disponibilidad de la sociedad en los sistemas informáticos genera una necesidad por su continuo funcionamiento. El desarrollo de sistemas, combinados con una dependencia estrecha de las organizaciones y su continua utilización, hace relevante la gestión de continuidad del negocio, que busca minimizar la probabilidad y la magnitud de las posibles interrupciones del negocio, y abarca los planes de recuperación de desastres para proteger contra la principal pérdida de los servicios de TI y continuar con su funcionamiento.

Este trabajo contiene una introducción al BCI, para luego presentar el BCI-v, que será mostrado a través de un caso de estudio realizado en la Minera del Cobre

2. BACKGROUND.

Hacia principios de los años setenta, Norman L. Harris, Edward S. Devlin y Judith Robey, tratando de encontrar un método de planificación y gestión que evitara la continua atención de problemas de forma improvisada, dieron lugar al nacimiento de una actividad que en un principio se llamó Disaster Recovery Planning, es decir, Planificación de la Operación ante Desastres. Posteriormente esa misma actividad se denominó Contingency Planning, es decir, Planificación ante Contingencias. Hasta ese momento, las actividades de planificación y prevención estaban dirigidas hacia las operaciones informáticas que en mayor parte de los casos se encontraban centralizadas en el Departamento de Informática. Con el paso del tiempo y la aparición de la informática distribuida, que extiende por toda la organización las funciones se transformaron en medios informáticos y telemáticos, en donde hoy en día no se habla que solo se integran las aplicaciones de una empresa, sino que se incorpora el concepto de empresa ampliada para entrar a formar parte de una cadena de valor de la organización. Esa actividad varió su alcance y vino a llamarse Business Continuity Planning, es decir, lo que se podría traducir literalmente como Planificación de la Continuidad del Negocio. La palabra negocio, tiene directa relación con el mercado y dado que hoy todas las organizaciones se relacionan con este de alguna u otra forma, siendo estas empresas privadas o públicas, las que dependen del correcto funcionamiento de las Tecnologías de la Información y de las Comunicaciones (TIC). Hablar de Continuidad del Negocio sería limitar mucho el alcance, por lo que sería más correcto hablar de Continuidad del Servicio, sin embargo, dentro del ámbito de los profesionales de las Tecnologías de la Información, "Continuidad de Negocio" ha venido a transformarse en un término comúnmente aceptado para todas las organizaciones, en el ámbito públicos como el privado [2].

En resumen, Business Continuity Management es un proceso de dirección que identifica los impactos potenciales que amenazan a la organización y proporciona el marco adecuado para construir y reforzar la capacidad de dar una respuesta efectiva

que proteja los intereses, la imagen y el valor de las actividades realizadas por la misma [2].

Es necesario conocer algunos elementos o conceptos en la cuales están basada la BCI, estos son; los activos de una organización "son todas aquellas cosas a las que la empresa les da valor" [5], una amenaza es "el intento de hacer daño" [4], las vulnerabilidades son "condiciones de la organización que pueden hacer que una amenaza se manifieste" [6], el riesgo se define como "la probabilidad que una amenaza pueda explotar una vulnerabilidad y causar daño a los activos de una organización." [1].

3. VARIANTE DEL MODELO BUSINESS CONTINUITY PLANNING.

A continuación presentaremos BCI-v, que es un modelo basado en [3], estas modificaciones, se realizaron en torno a las necesidades de la empresa lo que derivó en esta nueva variante del modelo BCI, que se mostrara a continuación.

Fase 1: Iniciación y Gestión de Proyecto.

El propósito de esta fase es conseguir que el desarrollo e implantación de un Plan de Continuidad de Negocio sea un proyecto estratégico de toda la organización, involucrando a todas las unidades y áreas de la empresa.

Junto con el alcance del plan y recolectar la información necesaria se debe determinar qué áreas, unidades, dependencias o instalaciones relacionadas con el Departamento de TI que van a ser incluidas en el plan.

Fase 2: Análisis de Riesgo e Impacto.

El objetivo de esta fase es proporcionar a la dirección la información necesaria para que pueda tomar decisiones en el desarrollo de su estrategia de recuperación. Para ello, los riesgos deben ser identificados, eliminados o reducidos. Se debe determinar el grado de criticidad de dichas funciones en la razón de las necesidades de la organización y el tiempo máximo a partir del cual la interrupción de cada una de ellas es inaceptable.

Para analizar y determinar el Riesgo dentro de una organización se debe:

- **Determinar los activos relevantes para la organización:** Para ello se clasifican con un código, y nombre.
- **Determinar a qué amenazas están expuestos aquellos activos:** Para ello se propone una tabla de descripción de amenazas (véase tabla 7). Para poder completar la Tabla 7 se tiene que determinar la amenaza, los activos que están expuestos a dicha amenaza y las dimensiones que se describen en la Tabla 1 (ver Tabla 1), además de una descripción del tipo de amenaza.
- **Estimar el impacto y riesgo:** Para ello se propone una matriz de impacto y riesgo (véase Tabla 8). Para completar esta matriz se consideran las definiciones de la Tabla 2.
- **Establecer los tiempos de vuelta a la normalidad:** Para poder realizar el establecimiento de los tiempos de vuelta a la normalidad, hay que determinar los lapsos de tiempo que podrían ser críticos desde el momento en que el activo sufre un evento por alguna amenaza o un alto de su servicio.

Tabla 1: Dimensiones de Seguridad.

Tipo	Descripción
Disponibilidad	Propiedad o característica de los activos consistentes en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.
Integridad de los datos	Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.
Información confidencial	Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.
Autenticidad	Propiedad o característica consistente en que una organización es quien dice ser o bien que garantiza la fuente de la que derivan los datos.
Trazabilidad	Propiedad o característica consistente en que las actuaciones de una organización pueden ser atribuidas exclusivamente a dicha organización.

Tabla 2: Tabla resumen del contenido de la Matriz de Impacto y Riesgo.

Activos	
Nombre	Corresponde al nombre del activo que se encuentra definido dentro de del área e empresa en cuestión.
Tipo	Corresponde a la clasificación de activo a la cual pertenece. (véase Tabla 6)
Criticidad	Corresponde al criterio de jerarquizar los activos, en función de su impacto global, pudiendo tomar los valores Bajo **(B)**, Medio **(M)** o Alto **(A)**.
Exposición	
Amenaza	Corresponde a la amenaza asignada desde el Listado de Amenazas a un activo específico. A modo de ejemplo Tabla 6
Rango de Vulnerabilidad	Corresponde al grado de exposición que queda el activo en relación a la materialización de la amenaza asignada, pudiendo tomar los valores Bajo **(B)**, Medio **(M)** o Alto **(A)**.
Rango de Impacto	**Impacto Alto (A):** Cuando ante una eventualidad se encuentran imposibilitadas para realizar sus funciones normalmente. **Impacto Medio (M):** Cuando la falla de ésta ocasiona una interrupción en las operaciones del Área o Empresa, por un tiempo mínimo de tolerancia. **Impacto Bajo (B):** Cuando la falla de ésta no tiene un impacto en la continuidad de las operaciones del Área o Empresa.
Probabilidad	Posibilidad de ocurrencia de la amenaza asignada al activo, pudiendo tomar los valores Bajo **(B)**, Medio **(M)** o Alto **(A)**.
Resumen Nivel de Riesgo	Proximidad de un daño que puede causar la amenaza asignada al activo. Pudiendo tomar los valores Bajo **(B)**, Medio **(M)** o Alto **(A)**.

Fase 3: Desarrollo de la Estrategia de Continuidad.

En esta etapa se definen las posibles opciones para decidir la estrategia de operación para la recuperación de las funciones del área o empresa y de negocio dentro de los límites definidos como objetivos.

La primera acción es el almacenamiento y respaldo de la información. Dentro de esta estrategia se busca establecer o definir la frecuencia, ubicación, estándares y el modo en que se realizarán los respaldos, la Tabla 3 presenta los procedimientos de respaldo de la información que contiene la empresa.

Tabla 3: Procedimientos de Respaldo de la Información

Tipos	Descripción
Procedimientos de respaldos diarios	Deberá ejecutar diariamente, de Lunes a Viernes
Procedimientos de respaldo semanal	Se ejecutará al término de cada semana
Procedimientos de respaldo mensual	Se ejecutará, el último día hábil del mes o dentro de los cinco primeros días hábiles del mes siguiente
Procedimientos de respaldo anual	Se ejecutará, el último día hábil del mes del año o dentro de los cinco primeros días hábiles del mes siguiente como máximo, al término de la jornada.
Procedimientos para respaldo de sistemas específicos	Estos respaldos deben ser periódicos y deben ser solicitados por el usuario.
Procedimientos para respaldos eventuales	Son respaldos que no corresponden a los temporales, a respaldos temporales y son solicitados deben ser solicitados al área correspondiente, y serán resguardadas en un lugar específico.
Procedimientos para restauración de información	En los casos que un usuario requiera restaurar información respaldada, esta se encontrara disponible previa autorización del encargado, además se debe dejar constancia del procedimiento.

Como segundo paso, se debe disponer de un centro de control alternativo, propio o subcontratado, en el que se realizarán las operaciones que permitan la continuidad de las funciones críticas en un periodo inferior al definido por los umbrales de respuesta y recuperación.

Si se mantiene un centro de datos o servidores de procesamiento de datos, la estrategia es asegurar la continuidad de estos servicios, a través de diferentes alternativas, hasta que dure la emergencia.

Y por último definir las medidas de prevención, el propósito de las medidas de prevención es la determinación de controles y métodos para detectar y prevenir daños a los diversos activos del área o empresa en cuestión. Está orientado cien por ciento a la parte física (hardware) de los sistemas.

Fase 4: Organización de Equipos de Emergencia y Recuperación.

Esta fase se refiere a los equipos que interviene dentro del Plan de Continuidad de negocio, participando desde la gestión plan hasta la recuperación de las actividades normales del negocio.

Los equipos de recuperación son grupos de personas que se encargan de una serie de actividades para conseguir un proceso de recuperación efectivo, esto quiere decir la vuelta a la normalidad en el funcionamiento de la empresa. Cada equipo deberá estar constituido por un jefe y a su vez estos equipos pueden contener sub-equipos. Como parte de la estrategia general, es esencial que las responsabilidades principales sean asignadas al equipo adecuado.

Por lo general, las responsabilidades de recuperación van en paralelo con las actividades del día a día, sin embargo, la asignación de responsabilidades puede depender del lugar donde se realice la recuperación, la logística y el tiempo.

Fase 5: Desarrollo e Implementación de los Planes de Continuidad de Negocio.

El aspecto más importante de la continuidad del negocio es la inmediata notificación al responsable apropiado de cualquier suceso que pueda causar una interrupción en las operaciones informáticas, independiente de su dimensión. Como primer paso, tan pronto como reciba la notificación de un incidente, el coordinador del Plan tomará acción según se especifica en la lista de actividades de la gestión del mismo, desencadenando la puesta en marcha de los distintos procedimientos de acción.

Estos procedimientos se han clasificado en cuatro grandes grupos, cada una con una denominación genérica como se muestra en la Tabla 4.

Tabla 4: Procedimientos para un Plan de Acción.

Procedimientos	Descripción
Procedimientos de emergencia	Son acciones inmediatas al incidente que tratan de proteger la integridad de las personas (si está amenazada), contener la progresión del incidente y pararlo en la medida de lo que sea posible
Procedimientos de respuesta	Son acciones de cada unidad, área específica de este o servicio que tienden a sustituir los procedimientos habituales de trabajo por otros alternativos
Procedimientos de recuperación	Son los procedimientos que permiten volver a utilizar datos, aplicaciones, sistemas, etc.
Planificar la vuelta la normalidad	Es una actividad va orientada hacia el establecimiento y desarrollo de todo tipo de acciones con el fin de volver al estado normal de las tareas y actividades de la empresa.

Para establecer el nivel del plan a seguir en el supuesto de un desastre, se observarán las siguientes directrices presentadas en la Tabla 5, teniendo en cuenta su gravedad en función del periodo de interrupción previsto.

Tabla 5: Tabla de Definición de Desastres.

Tipo	Descripción
Desastre menor	Aquel que provoca una parada que no sobrepase las dos horas establecidas como mínimo
Desastre mayor	Aquel que provoca una parada de más de dos horas y que no sobrepase las horas hábiles de trabajo.

Desastre catastrófico	Cuando el sistema informático vaya a estar fuera de servicio más de las horas hábiles o fuera del horario normal de trabajo y que no sobrepase una semana.

Fase 6: Entrenamiento, Pruebas y Mantenimiento de los Planes de Continuidad de Negocio.

El objetivo de esta fase es planificar cómo mantener actualizado el plan y al mismo tiempo cómo conseguir que el personal esté preparado para utilizarlo correctamente.

El programa de mantenimiento del plan debe contar al menos con tres elementos:

- **Revisiones periódicas:** El plan de Continuidad de Negocio debe ser actualizado constantemente.
- **Ejercicios de entrenamiento**: Todo el personal TI debe entrenarse en los procesos de recuperación del Plan de Contingencia.
- **Pruebas:** Para asegurar que todo funciona según lo previsto.

Después de cada revisión o ejercicio, los diversos componentes del plan deben ser actualizados, con las experiencias obtenidas por ejercicios anteriores.

Fase 7: Lista de Distribución.

El objetivo principal de esta etapa es registrar de manera óptima, clara y ordenada la distribución de los Planes de Contingencias a las distintas áreas o equipos que intervienen. Para esto se propone una lista de distribución que contenga el número correlativo del plan de continuidad de negocio, además del nombre y cargo de la persona o trabajador a la que se le entregó el ejemplar (véase Tabla 10).

4. PROPUESTA.

El modelo BCI-v se aplicó a un estudio de caso, en una empresa minera, pero por motivos de privacidad, se cambiará el nombre de la empresa por "Minera el Cobre".

Fase 1: Iniciación y Gestión del Proyecto.

El alcance del plan presentado a la dirección del área de Informática de Minera el Cobre, se divide en cinco puntos los que abarcan desde:

- Acciones a seguir en el caso de producirse una emergencia en el área de operaciones.
- Plan de contingencia que su vez de divide en dos tipos:
  - Plan Continuidad de Negocio Genérico de Informática Minera el Cobre, enfocado en Emergencias Catastróficas.
  - Plan de Continuidad de Negocio de Informática Minera el Cobre, enfocado a Emergencias Potenciales.
- Definición de espacios o áreas abarcará el plan.
- Composición de los equipos encargados de llevar a cabo el plan de contingencia.
- Categorización de los tipos de incidentes que se pueden provocar por una contingencia.

Fase 2: Análisis de Riesgo e Impacto.

Se deben clasificar los activos desde un punto de vista macro a un entorno más detallado, con efecto de poder realizar el análisis de riesgo de manera óptima y clara.

Tabla 6: Clasificación de algunos activos Minera del Cobre

Tipo	Código
Servicios	[S]
Datos / Información	[D]
Aplicaciones / Software	[SW]
Equipos informáticos	[HW]
Instalaciones	[L]

La detección de las amenazas a las que podrían estar expuesto los activos del Área de informática de Minera el Cobre, se clasificaron según lo expuesto arriba.

A modo de ejemplo, la Tabla 7 presenta una descripción de una posible amenaza, los activos que estarían expuestos y las dimensiones.

Tabla 7: Descripción de Amenazas.

[N.1] Fuego	
Tipos de activos: • Equipos informáticos (Hardware)	**Dimensiones:** 1. Disponibilidad
Descripciones: Incendios: posibilidad de que el fuego acabe con recursos del sistema.	

La Tabla 8 presenta un ejemplo de la información general de riesgos informáticos, del Área de Informática de Minera el Cobre, sintetizado en una matriz que muestra los niveles de exposición a los riesgos. Cabe destacar que esta matriz fue completada con los datos requeridos por la Tabla 2.

Tabla 8: La matriz de Impacto y riesgo de seguridad informática.

ACTIVOS			EXPOSICION				
Nombre	Tipo	Criticidad (A,M,B)	Amenaza	Rango de Vulnerabilidad	Rango Impacto (A,M,B)	Probabilidad (A,M,B)	Nivel de Riesgo (A,M,B)
- Oficina de Telecomunicaciones	L	A	N.1	B	M	B	B

Este análisis de la matriz de riesgo, se realizó con cada uno de los activos y con cada una de las amenazas asignadas, según el catálogo de amenazas, listado de amenazas y activos de Informática Minera el Cobre y la tabla asociada con cada uno de los valores obtenidos.

Y por último, se establecen los tiempo de vuelta a la normalidad, por ejemplo: si las comunicaciones se caen, éstas deben estar arriba dentro de las 4 primeras horas, mientras que un Sistema Local Operacional, tiene que estar funcionando dentro de las 2 primeras horas. El correo electrónico puede estar hasta un día sin funcionamiento, pasando más allá de ese

umbral comienzan los problemas de funcionamiento del flujo de información que debe existir dentro de toda la Minera.

Fase 3: Desarrollo de las Estrategias de Continuidad.

Para esta fase, fue definir la estrategia de respaldo y almacenamiento de la información que se genera en la Minera el Cobre. Esta estrategia contiene un manual de procedimientos que define los tiempos y modos en que se realizarán los backup, además del hardware donde se almacenarán estos respaldos y buenas prácticas para este procedimiento.

En base a lo anterior, se plantea y propone, que la Unidad de Operaciones del área de Informática de la Minera sea la responsable de cumplir las siguientes normas tendientes a proteger la seguridad de la información de los sistemas.

- Respaldo de forma segura (cintotecas o lugares alternativos) dejando por escrito fecha y hora de ejecución de los procedimientos, en orden correlativo que permita continuar con la operación de los sistemas en alguna instalación de respaldo alternativos. Junto con ello definir lugares de almacenamiento de información y por ultimo estos espacios deben estar protegidos con los medios de prevención de riesgos adecuados para estos recintos.

Para los procedimientos de respaldos de la información, la Unidad de Operaciones del Área de Informática de la Minera el Cobre deben observarse las rutinas establecidas dependiendo del tipo de almacenamiento de información. Estos procesos se describen en la Tabla 3.

Además, se procede a asegurar la disponibilidad del Centro de Procesamiento de Datos tanto en Hardware como para Software. Para ello se duplica o multiplica el número de elementos, llegando a formar un clúster o agrupación de servidores. Los servidores que participan en el clúster se darán respaldo mutuamente en forma activa, permanente e independientemente, logrando de esta manera minimizar el riesgo de la falla en el servidor. Además de un disco espejo que escribe simultáneamente en ambos sobre un mismo canal, si alguno de los discos falla, el otro es capaz de mantener operando el sistema sin perder información o interrumpir al usuario y para el software se dispone de una sistema que detecte y ejecute procedimientos para recuperar fallas, no se pretende evitarlas, sino recuperarlas en menos tiempo posible

Se definen las medidas de prevención que son de dos tipos:

- Controles Físicos de Acceso como: personal de seguridad, llaves, alarmas, sistemas de vigilancia entre otros.

- Mecanismo Correctivos y Preventivos como: corrientes reguladas, controles de medio ambiente y detección de fuego que minimicen el daño y faciliten la recuperación

Fase 4: Organización de Equipos de Emergencia y Recuperación.

En función del tamaño de Informática Minera el Cobre y con el objetivo de clarificar las distintas funciones, se han definido varios equipos para poder asignar tareas del plan de contingencia, siendo el número y funciones de cada equipo ajustadas a las necesidades específicas de la organización.

Al momento de realizar los Planes de Continuidad de Negocio, dependiendo de la magnitud de la contingencia, actuarán ciertos equipos tanto para los procedimientos de respuesta, como los de recuperación.

A modo de ejemplo, en la Tabla 9 se detalla la conformación del equipo de Gestión de Instalaciones, que es un sub equipo del Equipo de Logística.

Tabla 9: Miembros de equipo de instalaciones

Miembros equipo de Gestión de instalaciones
Jefe Informática Minera el Cobre
Técnico en telecomunicaciones de informática Minera el Cobre
Administrador de redes locales de informática Minera el Cobre

Fase 5: Desarrollo e Implementación de los Planes de Continuidad de Negocio.

A continuación se presentan los planes de acción para la continuidad del negocio de informática Minera el Cobre enfocados tanto en emergencias catastróficas como emergencias potenciales. Estos dos planes de acción se basan en los procedimientos de Plan de acción (véase tabla 4), teniendo en cuenta el tipo de desastre (véase tabla 5).

Plan Continuidad de Negocio Genérico de Informática Minera el Cobre, enfocado en Emergencias Catastróficas.

El plan de acción comienza con la activación de procedimientos de emergencia que muestran el flujo de notificaciones y acciones iniciales según el acontecimiento. Luego se procede a la evaluación de daños. Una vez sea permitido el acceso al edificio se realizará una inspección in situ de las áreas afectadas para evaluar el daño. Entonces se procede a la respuesta frente a la situación a través de un conjunto de procedimientos de respuesta ante emergencia. A modo de ejemplo se muestra el procedimiento N° 11, del Plan de Continuidad del Negocio.

Tabla 10: Procedimiento N°11 del Plan de Continuidad del Negocio

N° 11. Procedimientos del área de Informática Minera el Cobre
11.1. Procedimientos Generales. Los integrantes de esta área serán responsables de las siguientes acciones:
A. Presentarse en el Centro de Control según instrucciones recibidas durante la alerta.
B. Coordinar con el equipo de Reacondicionamiento, la estimación del tiempo necesario para la reconstrucción del Centro de Proceso de Datos.

Luego de la emergencia viene la recuperación, basándose en la reconstrucción de los registros perdidos, tanto de información como del equipamiento de inmuebles y equipo de los lugares de trabajo afectados, para luego reanudar las operaciones normales después de sufrido el corte o alto de éstas.

- **Plan de Continuidad de Negocio de Informática Minera el Cobre, enfocado a Emergencias Potenciales.**

El Plan de Acción contempla el Análisis de Riesgo e Impacto realizado en etapas anteriores, en donde nace la necesidad de creación de medidas y aporte de recursos hacia una posible materialización de un riesgo, en el que están asociadas y estudiadas posibles amenazas que se puedan concretar. A continuación, a modo de ejemplo en la Tabla 11 se detalla uno de los procedimientos de Emergencia.

Tabla 11: Procedimiento de Emergencia: Caída Sistema Local de Medio Ambiente.

Caída Sistema Local de Medio Ambiente.	
Esta emergencia es provocada principalmente por el corte en la comunicación de la Red WAN, que conecta la comunicación existente desde la Planta con el resto la ciudad, país y el mundo. La forma en que se podría detectar la caída del sistema Local de Medio Ambiente se puede producir por medio de señales de alerta, la cual podría ser entre otras:	
Activación de procedentes de emergencia	El ente fiscalizador comunica al área medio ambiente de la Minera el Cobre la no existencia de conectividad y de datos actualizados en tiempo real sobre lo entregado por el sistema.
Evaluación de Daños	Por tratarse de un activo de alta criticidad, el cual al momento de ser envuelto en alguna emergencia, tiene directo impacto en a la Planta entera, se debe realizar una reunión de Gerencia con el área involucrada, ya sean medio ambiente, empresa contratista e Informática.
Procedimiento de respuesta	El técnico de telecomunicaciones, al verificar que no se tiene continuidad del servicio, realiza un pedido técnico al principal proveedor de comunicaciones, siendo la Empresa Nacional de Telecomunicaciones, generando una orden y número de boleta asignado al tipo de problema asociado
Procedimiento de recuperación	Al momento de cerrarse la boleta de orden de servicio con el proveedor de comunicaciones, se verifica en conjunto que la conectividad del enlace este se encuentra completo funcionamiento tanto física como lógicamente. Finalmente la empresa contratista entrega el servicio interrumpido funcionando en forma normal

Fase 6: Entrenamiento, Pruebas y Mantenimiento de los Planes de Continuidad de Negocio.

Para ello se realizan una serie de ejercicios de entrenamiento, pruebas técnicas, simulacros y a su vez la actualización constante para el manteniendo de plan de continuidad de negocio.

Fase 7: Lista de Distribución.

Finalmente, Tabla 10, presenta un extracto de la lista de distribución que mantiene del plan de continuidad del negocio los trabajadores de informática Minera el Cobre

Tabla 10: Lista de Distribución del plan de continuidad de negoción

N°	Asignado a	Cargo
1.0	Cristian Rojas	Jefe Informática
1.1	Juan Morales G	Administrador de Redes Locales
2.0	Víctor Pérez S.	Jefe de área Contrato

5. CONCLUSIÓN.

Un plan de continuidad de negocio es clave para asegurar que una empresa puede protegerse contra los riesgos que son inherentes a su entorno y poder continuar con sus funciones. Las empresas son cada vez más dependiente de la disponibilidad y resguardo de información con el fin de prestar servicios a los clientes. Esta propuesta basada en el modelo de Ciclo de vida Plan de Continuidad de Negocio en [3], nos proporciona diferentes fases secuenciales, para la creación de un modelo que ayude a la empresa o institución, disponer de una estrategia que permita continuar con el funcionamiento y prever de cualquier situación extraordinaria que pueda interferir el desarrollo de sus procesos o actividades. El estudio de caso presentado en este trabajo nos muestra la creación e implementación de un Plan de continuidad del Negocio, haciendo hincapié en los procesos y actividades en cada una de ellas, por lo tanto deja abierta la puerta para seguir perfeccionando y adaptando este modelo. Con el fin de obtener una herramienta que permita hacer frente a cada incertidumbre que se ven expuestas las empresas y de esta forma protegerlas para su continuo funcionamiento.

6. REFERENCIAS.

[1] Barnes, James. A Guide to Business Continuity Planning. Wiley, London. 2001.

[2] Loyola Rodrigo, Propuesta de plan de contingencia de negocio en el área de informática de Enami, Paipote, Universidad de Atacama, 2011.

[3] Martínez Juan Gaspar, "Planes de Contingencia, La continuidad del negocio en las organizaciones",Ediciones Díaz de Santos, 2004

[4] Meredith,William "Business Impact Analysis" Business Continuity Management. Wiley. 2002.

[5] O´Hehir, Michael. "What is Business Continuity Planning Strategy?" Business Continuity Management, 2002.

[6] [Sheffi, Yossi. The Resilient Enterprise. M.I.T Press, 2005 Cambridge, Mass.

[7] William J. Caelli, Lam-For Kwok, and Dennis Longley, A Business Continuity Management Simulator, IFIP AICT 330, pp. 9–18, 2010.