

POLÍTICA DE CONTINUIDAD DEL NEGOCIO

SISTESEG
Bogotá
Colombia

Bogotá, 20 de Diciembre de 2007

SISTESEG

Política Continuidad del Negocio [BS 7799 Control A.11.1]

1.1 Audiencia

Esta política aplicará para todo el personal que labore en, o, para SISTESEG, con el fin de poder garantizar la continuidad del negocio, en caso de un evento que afecte la operación normal.

1.2 Introducción

El plan de Continuidad, tiene como objetivo proteger los procesos críticos del negocio, contra desastres o fallas mayores, junto con las posibles consecuencias que se puedan tener, como pérdidas de tipo financiero, credibilidad, productividad, etc. debido a la no disponibilidad de los recursos de la organización. El Plan de Continuidad del Negocio, busca mitigar el riesgo a dichas fallas o desastres, mediante un plan que permita la pronta recuperación de la operación, en caso de presentarse algún evento que afecte el flujo normal de las actividades de SISTESEG.

1.3 Definiciones

Plan de continuidad del negocio (BCP-Business Continuity Plan): 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 de SISTESEG.

Plan de Contingencia: Es un subconjunto de un plan de continuidad de negocio, que contempla como reaccionar ante una contingencia que pueda afectar la disponibilidad o los servicios ofrecidos por los sistemas informáticos. Una contingencia puede ser un problema de corrupción de datos, suministro eléctrico, un problema de software o hardware, errores humanos, intrusión etc.

Plan de recuperación frente a desastres: Es aquella parte del plan de contingencia y del plan de continuidad de negocio, que aborda aquellas contingencias que, por su gravedad, no permiten continuar prestando el servicio desde el centro local y debe continuarse el servicio desde un nuevo centro. Este plan debe contemplar la vuelta atrás cuando, tras arreglar las consecuencias del desastre, el servicio pueda ser reanudado en el centro local.

Business Impact Assessment (BIA): El propósito del BIA es crear un documento que ayude a entender el impacto que un desastre pueda tener sobre un negocio en particular. Contempla tres objetivos fundamentales:

- ❖ Priorizar procesos críticos del negocio.
- ❖ Calcular el “Maximun Tolerable Downtime”, (MTD) el cual es el tiempo máximo sin servicio que una organización puede soportar y seguir siendo una compañía que cumple con sus objetivos de negocio. Normalmente es encontrado que este tiempo es mucho menor de lo esperado.

1.4 Objetivo

Evitar interrupciones a los procesos críticos del negocio como consecuencia de fallas o desastres.

1.5 Enunciado de la Política General

"Debido a que cualquier interrupción en los procesos de negocio afecta la operación, es responsabilidad de las directivas de la organización aprobar un plan de continuidad de negocio que cubra las actividades esenciales y críticas de SISTESEG.

Se deben incluir controles para identificar y reducir riesgos, limitar las consecuencias de los diferentes incidentes y por último asegurar la recuperación inmediata de las operaciones esenciales.

Como parte fundamental del soporte al negocio, todos los sistemas de información deben poseer planes de contingencia y recursos necesarios que aseguren la continuidad de los procesos de negocio.

1.6 Elementos adicionales a la política general

Aspectos de la Continuidad del Negocio a ser considerados en la definición de las políticas funcionales:

- Respaldo de información
- Seguridad física
- Mantenimiento del plan
- Pruebas del plan
 - Simulaciones
 - Intentos de restauración

1.7 Políticas relacionadas

Política de seguridad física

1.8 Roles y responsabilidades

Esta política es responsabilidad de ser aprobada por las directivas de SISTESEG, luego de un estudio previo y detallado de sus posibles consecuencias, con el fin de garantizar la continuidad del negocio en caso de un evento que afecte la operación normal de los procesos críticos.

1.9 Violaciones a la política

En este caso especial, si las directivas de la organización de SISTESEG se comprometen a desarrollar este plan, será responsabilidad de ellos, no faltar a este compromiso y tener en cuenta que al no realizar dicho plan, la compañía pudiera estar expuesta a procesos legales y contractuales, que pudieran poner en riesgo el futuro de la operación de SISTESEG.

1.10 Revisión de la política

Esta política debe ser modificada si existieran cambios en los procesos de negocio de SISTESEG o en su infraestructura tecnológica, de no haber cambios, se debe realizar su revisión anualmente.

1.11 Referencias

Las diferentes recomendaciones sobre la ejecución detallada de un Plan de Continuidad de Negocio se apoyan en el BCI (Business Continuity Institute) y el ISO 17799.

<http://www.thebci.org/>

<http://www.business-continuity-world.com/>

1.12 Aspectos específicos sobre la política de Continuidad del Negocio.

1.12.1 INICIO DEL PLAN DE CONTINUIDAD DEL NEGOCIO. (BS 7799-2 Control A 11.1)

Las directivas de SISTESEG son las responsables de dar inicio al plan de continuidad del negocio.

El Plan de Continuidad del Negocio (BCP-Business Continuity Plan), es esencial para poder continuar las actividades críticas del negocio de SISTESEG, en el evento de una falla inesperada, que pudiera seriamente interrumpir los procesos y actividades importantes de la operación de la compañía.

El proyecto del Plan de Continuidad del negocio necesita ser iniciado y formalmente aprobado, por las directivas de SISTESEG.

Es importante considerar lo siguiente:

- Se debe establecer la necesidad del Plan de continuidad.
- Se debe obtener el compromiso de las directivas de SISTESEG y presentarles un reporte inicial que informe como el BCP cumplirá sus objetivos.
- Para que el plan de continuidad sea eficaz, hemos organizado el plan en torno a un concepto de Equipo Directivo de Emergencia (EDE) que está formado por miembros altamente cualificados del equipo directivo procedentes de áreas vitales dentro de la organización. Los componentes del equipo tienen cometidos y responsabilidades concretas cuando se produce un desastre en cualquier instalación de SISTESEG y se pone en práctica el Plan de Recuperación de Desastres. El EDE está formado por personas procedentes de las áreas siguientes: Recursos Humanos, Administración y Financiera y Tecnología. Los integrantes de la Gestión del Proyecto y de la Gestión del Nivel Directivo coordinan los esfuerzos del EDE. El EDE es un grupo de gestión flexible y móvil que puede ocuparse de cualquier plan de recuperación que sea necesario en cualquier sitio donde este SISTESEG.
-

1.12.2 DESARROLLO Y ADMINISTRACION DEL PLAN DE CONTINUIDAD DEL NEGOCIO (BS 7799-2 Control A 11.1.1)

Las directivas de la organización deben desarrollar un Plan de Continuidad del Negocio que cubra los aspectos críticos y esenciales de la actividad de la compañía.

El Plan de Continuidad del Negocio (BCP), es esencial para poder continuar con las actividades críticas del negocio de SISTESEG, en el evento de una falla inesperada.

El Plan de Continuidad del negocio es un proyecto con características de detalle y complejidad, independiente del entorno tecnológico y probablemente contendrá una serie de acciones críticas enfocadas a lograr el retorno a la operación normal.

- Recomendaciones adicionales al desarrollo y administración del plan de continuidad del negocio:
- Entender plenamente los riesgos a que está enfrentado SISTESEG, incluyendo e identificando los procesos críticos del negocio.
- Entender el posible impacto que una interrupción a la operación normal pueda tener.
- Considerar la adquisición y renovación de una póliza de seguros de protección de activos como parte del plan de continuidad de negocio.
- Formular y documentar una estrategia de continuidad del negocio de acuerdo a los objetivos y prioridades.
- Formular y documentar una estrategia consistente con los objetivos y prioridades acordadas, y a su vez, se debe documentar el plan de continuidad del negocio de acuerdo a la estrategia anteriormente definida.

1.12.3 EVALUACIÓN DE RIESGO DEL PLAN DE CONTINUIDAD DEL NEGOCIO (BS 7799-2 Control A 11.1.2)

Dentro del plan de continuidad de negocio se debe realizar una evaluación formal de riesgo, o análisis de impacto sobre el negocio (BIA-Business Impact Assessment), con el fin de determinar los requerimientos del Plan de Continuidad del Negocio e identificar eventos que puedan causar interrupciones a los procesos de negocio.

Es importante considerar que se deben evaluar y analizar todos los procesos de negocio y no limitarse exclusivamente a los recursos e infraestructura asociado a los sistemas de información.

1.12.3.1 Recomendaciones adicionales

El Plan de Continuidad del Negocio (BCP), es esencial para poder continuar con las actividades críticas del negocio de SISTESEG, en el evento de una falla inesperada, que pudiera seriamente interrumpir los procesos y actividades importantes de la operación de la compañía.

La evaluación de riesgo en el BCP analiza la naturaleza de la ocurrencia de eventos inesperados, su impacto potencial y la probabilidad de que estos eventos lleguen a ser incidentes críticos para el negocio.

Aspectos de la seguridad de la información a ser considerados cuando se implementan estas políticas son:

- Comprender que así el proyecto formal del Plan de continuidad del Negocio se haya iniciado, si los recursos humanos o financieros son insuficientes, es muy probable que el plan no tenga éxito.
- Si se subestima el impacto a corto y mediano plazo de un incidente de seguridad se puede tener un nivel no adecuado de respuesta que afecte la elaboración de un Plan de Continuidad de Negocio.
- Los pasos involucrados en el análisis de impacto hacia el negocio (BIA) comprenden:
- Técnicas de obtención de información

- Seleccionar las personas a entrevistar
- Adecuación de los cuestionarios a realizar
- Análisis de la información
- Determinar los tiempos críticos de las diferentes funciones del negocio
- Determinar los tiempos máximos tolerables de caída por proceso (MTD- Maximum Tolerable Downtime)
- Priorizar la recuperación de las funciones críticas del negocio
- Documentar y preparar reportes de recomendaciones

1.12.4 CARACTERÍSTICAS DEL PLAN DE CONTINUIDAD DE NEGOCIO. (BS 7799-2 Control A 11.1.3-4)

Con el fin de garantizar su consistencia a lo largo de las diferentes unidades de negocio, el plan de continuidad de negocio debe considerar:

- Condiciones para su activación
- Una estrategia de recuperación de desastres teniendo en cuenta aspectos como:
 - Costos de las diferentes alternativas
 - Costos de servicios alternos
 - Prioridades y tiempos de recuperación
 - Negocios, usuarios, servicios, aspectos técnicos e información.
- Identificación de las responsabilidades y procedimientos de emergencia.
- Implementación de procedimientos de emergencia para permitir la recuperación en un tiempo limitado.
- Procedimientos de contingencia y procedimientos de regreso a la operación normal
- Documentación de procedimientos y procesos acordados.
- Educación apropiada sobre manejo de emergencias.
- Cronograma de pruebas del plan de continuidad del negocio.
- Responsabilidades individuales de ejecución y propietarios de cada plan

1.12.5 ENTRENAMIENTO Y CONCIENTIZACIÓN DEL PLAN DE CONTINUIDAD DEL NEGOCIO. (BS 7799-2 Control A 11.1.4)

Todo el personal de SISTESEG debe conocer el Plan de Continuidad del Negocio y su respectiva función dentro de él, una vez se haya realizado su aprobación.

1.12.5.1 Recomendaciones Adicionales

El Plan de Continuidad del Negocio (BCP), es esencial para poder continuar con las actividades críticas del negocio de SISTESEG, en el evento de una falla inesperada, que pudiera seriamente interrumpir los procesos y actividades importantes de la operación de la compañía.

Para que el Plan de Continuidad del Negocio pueda ser ejecutado exitosamente, todo el personal no sólo debe estar conciente de su existencia, sino conocer su contenido, junto con las actividades y responsabilidades de cada parte.

Aspectos de la seguridad de la información a ser considerados cuando se implementan estas políticas son:

- Aun cuando el Plan de Continuidad de Negocio haya sido probado, aun puede fallar, si el personal no está lo suficientemente familiarizado con sus contenidos.
- Cuando en el Plan de Continuidad del negocio, las personas involucradas olvidan su percepción de la cercanía del riesgo, se puede presentar cierta apatía, la cual disminuye su importancia, y la necesidad de una participación activa en él.
- Se deberá crear un plan de concientización sobre la importancia del BCP para SISTESEG, y el compromiso de todos los empleados para garantizar su éxito.

1.12.6 PRUEBA DEL PLAN DE CONTINUIDAD DEL NEGOCIO (BS 7799-2 Control A 11.1.5)

El Plan de Continuidad del Negocio necesita ser probado periódicamente, con el fin de garantizar que la compañía entienda claramente como debe ser ejecutado.

El hecho de probar el Plan de Continuidad del negocio en la organización, evalúa su viabilidad, y garantiza que los empleados estén familiarizados con el plan y sus procedimientos.

A continuación controles adicionales sobre las pruebas del BCP:

- Si la prueba del Plan de Continuidad del Negocio no reproduce las condiciones reales, el valor de tales pruebas es limitado y deficiente.
- Las fallas en el análisis del plan de pruebas del BCP, ocasionarán una disminución de la validez de la prueba. Los diferentes tipos de prueba incluyen:
 - Pruebas sobre la mesa de los diferentes escenarios (Por medio del uso de listas de verificación y análisis paso a paso)
 - Simulaciones
 - Pruebas de recuperación técnicas
 - Pruebas de recuperación en sitio alterno
 - Prueba de servicios externos (Energía, comunicaciones etc.)
 - Prueba completa, con el fin de evaluar personal, equipos, recursos físicos, para entender su capacidad de soportar interrupciones. Esta prueba implica detener las operaciones de SISTESEG y no es recomendable ya que puede originar un desastre real.
- Una vez aprobado y desarrollado, el plan de continuidad de negocio debe ser probado con el fin de mostrar su eficacia, y nivel de actualidad. El periodo de pruebas sobre la mesa de los diferentes escenarios, no debe ser mayor a 6 meses.

1.12.7 MANTENIMIENTO Y ACTUALIZACIÓN DEL PLAN DE CONTINUIDAD DE NEGOCIO. (BS 7799-2 Control A 11.1.5.2)

El Plan de Continuidad del Negocio debe estar actualizado y revisado periódicamente.

El mantenimiento y actualización del Plan de Continuidad del Negocio es muy importante si se requiere una operación exitosa en un momento dado.

- Se requiere probar las implicaciones por cambios en el BCP, de lo contrario su ejecución puede resultar en una serie de fallas y debilidades.
- Si el Plan de Continuidad del Negocio no es actualizado periódicamente, su éxito puede ser cuestionable. Los cambios incluyen:

- Adquisiciones de nuevos equipos
- Actualizaciones en los sistemas operacionales
- Personal
- Direcciones o números telefónicos
- Estrategias de negocio
- Ubicaciones físicas
- Leyes
- Contratistas, proveedores de servicio y clientes muy importantes
- Procesos nuevos o eliminados
- Riesgo (Operacional y financiero)