

Plan de Continuidad de Operaciones

Indice de Contenidos

1. Certificación Estándar Internacional DRII (Disaster Recovery Institute International)	3
2. Certificación Norma BS 25999	4
3. Certificación Norma ISO 22399	6
4. Certificación Seguridad de la Información Norma ISO 27001	7

1. Certificación Estándar Internacional DRII (Disaster Recovery Institute International)

1.1. Generalidades

El Plan de Continuidad de Operaciones de esta empresa está basado en el DRII (*Disaster Recovery Institute International*), y constituye el conjunto de prácticas profesionales para la **Gestión de Continuidad de Negocio**, cuyo objetivo principal es permitir a las operaciones comerciales de la empresa, el seguir operando bajo condiciones adversas, al implantar estrategias adecuadas, objetivos de recuperación, planes de gestión de crisis y estrategias de gestión de riesgos.

Este conjunto de prácticas abarca áreas como son:

- Iniciación y Gestión del proyecto
- Evaluación y control de riesgo
- Análisis de impacto del negocio
- Estrategias de la Gestión de Continuidad del Negocio
- Respuesta a emergencias y operaciones
- Elaboración y Aplicación de planes de Continuidad de Negocio
- Sensibilización y capacitación del personal
- Ejercicio y mantenimiento de los planes de Continuidad del Negocio
- Comunicaciones en las crisis y Coordinación con agencias externas.

Plan Continuidad de Operaciones BCM (Business Continuity Management)

En la empresa se han aplicado las mejores prácticas profesionales según el **DRI International**, las cuales resumimos a continuación y desarrollamos más adelante en este mismo documento:

INICIO Y ADMINISTRACIÓN DEL PROYECTO

Estos criterios han permitido establecer la necesidad de la Administración de Continuidad de Negocios de los procesos o funciones, incluyendo la capacidad de recuperación, objetivos de recuperación, planes de continuidad del negocio y de manejo de crisis, incluyendo el apoyo de la Dirección y organizar y manejar el desarrollo de la función o proceso, ya sea en colaboración con, o como un componente clave de una iniciativa integrada de manejo de riesgos.

EVALUACIÓN Y ANÁLISIS DE RIESGO

La evaluación y análisis del riesgo ha permitido determinar los eventos y los factores externos que pueden afectar en forma adversa a la empresa y sus instalaciones con una interrupción o un desastre, el daño que dichos eventos pueden causar y los controles necesarios para prevenir o minimizar los efectos de pérdidas potenciales. Proporcionar un análisis de costo beneficio para justificar la inversión en controles para mitigar los riesgos.

ANÁLISIS DE IMPACTO AL NEGOCIO

El análisis e identificación de los impactos que resultan de escenarios de interrupciones y desastres que puedan afectar a la empresa y las técnicas que pueden utilizarse para cuantificar y cualificar dichos impactos ha permitido a la empresa el establecer las operaciones críticas, sus prioridades de recuperación y sus interdependencias, de tal manera que puedan establecerse los Objetivos de Tiempo de Recuperación (RTOs).

DESARROLLO DE ESTRATEGIAS BC/DR

Nos permitido determinar y guiar en la selección de alternativas de estrategias de recuperación del negocio para la recuperación del negocio y tecnologías de información dentro del objetivo de tiempo de recuperación, mientras que se mantienen las funciones críticas de la compañía.

PREPARACIÓN Y RESPUESTA DE EMERGENCIA

Se ha desarrollado e implementado procedimientos para respuesta y estabilización de la situación después de un incidente o evento, incluyendo el establecimiento y manejo del Centro de Operaciones de Emergencia a ser usado como un centro de comando durante una emergencia.

DESARROLLO E IMPLEMENTACIÓN

Se ha diseñado, desarrollado e implementado planes de Continuidad y Gestión de Crisis que cumplen con la recuperación de las actividades del negocio dentro de un marco de tiempo aceptable.

CONCIENTIZACIÓN Y CAPACITACIÓN

Hemos preparado un programa para crear conciencia corporativa y mejorar las habilidades requeridas para desarrollar, implementar, mantener y ejecutar el Plan para la continuidad del negocio.

MANTENIMIENTO Y ACTUALIZACIÓN DE PLANES

Se ha planificado y coordinado ejercicios de los planes además de evaluar y documentar los resultados.

Se han desarrollado procesos para mantener actualizada la capacidad de recuperación y la documentación de los planes según la dirección estratégica de la organización.

Igualmente se ha verificado que los planes son efectivos al compararlos contra un estándar adecuado, y reporta los resultados de manera clara y concisa.

COMUNICACIÓN DE CRISIS

Se ha desarrollado, coordinado, evaluado y probado planes para comunicarse con involucrados internos (empleados, gerentes, etc.) involucrados externos (clientes, accionistas, proveedores, etc) y los medios de comunicación (prensa, radio, televisión, Internet, etc.)

COORDINACIÓN CON AUTORIDADES EXTERNAS

Se han establecido los procedimientos necesarios para coordinar las actividades de respuesta, continuidad y restauración con las agencias externas (locales, estatales, nacionales, respuesta de emergencia, defensa, etc.) mientras se asegura el cumplimiento con estatutos y regulaciones aplicables.

2. Certificación Norma BS 25999

2.1. Generalidades

El Plan de Continuidad de Operaciones de esta empresa está basado en la **Norma BSI 25999** (*Sistema de Gestión desarrollado por el British Standard Institution*).

La gerencia del plan de continuidad del negocio es un proceso de gestión abarcadora que identifica los riesgos y sus potenciales impactos en los procesos de la organización.

Asimismo, provee una estructura para mantener la flexibilidad y la continuidad de los procesos

organizacionales, con la capacidad de una efectiva respuesta en la protección de los intereses principales de las organizaciones, tales como: información, visión, marca, activos de valor, etc.

Esta empresa tiene conciencia acerca de la importancia de la buena planeación en todas las áreas de negocio dentro de la organización, por lo que se ha preparado para la Continuidad del Negocio, Recuperación de Desastres y Respuesta de Emergencia basándose y aplicando la Norma BS 25999, norma británica para la gestión de continuidad de negocio que abarca todo el ciclo de vida de la gestión de continuidad de negocio:

- “**El código de buenas prácticas**” que nos ha proporcionado recomendaciones de buenas prácticas y
- “**La especificación**” que nos ha permitido incorporar procesos de mejora continua para incrementar la recuperación de la organización ante una contingencia o desastre, y cumplir con los requerimientos regulatorios de continuidad de negocio, reducir esfuerzos y costos derivados de la ejecución de auditorías internas y de proveedores, justificar gastos de implantación y obtener la confianza de los directivos, clientes, accionistas en la “*supervivencia*” del negocio.

Plan Continuidad de Operaciones BCM (*Business Continuity Management*)

Hemos aplicado las mejores prácticas profesionales según **Norma BS 25999**, las cuales resumimos a continuación y desarrollamos más adelante en este mismo documento:

BS 25999-1:2006 – Código de Práctica

Gestión de Continuidad del Negocio.
Política de Gestión de Continuidad del Negocio.
Gestión del Programa de Continuidad del Negocio.
Entendiendo la Organización.
Desarrollo e Implementación de Respuestas a BCM.
Determinando Estrategias de Continuidad del Negocio.
Ejercitando, Manteniendo y Analizando el plan de BCM.
Fijando el BCM en la Cultura de la Organización.

BS 25999-2:2007 – Especificación

Planeación del Sistema de Gestión de BCM.
Implementando y Operando el Sistema.
Monitoreo y Revisión del Sistema.
Mantenimiento y Mejora del Sistema.

Beneficios de la aplicación del programa de BCM en la Organización

Los beneficios de haber desarrollado y aplicado un programa eficaz de BCM mediante la BS 25999 en la organización son los siguientes:

- Nos proporciona una estructura común, basada en mejores prácticas internacionales para gerencia de un proceso de continuidad de negocios.
- Nos ha capacitado para identificar proactivamente los impactos de una interrupción operativa.
- Nos ha permitido disponer de una respuesta efectiva ante interrupciones, minimizando su impacto.
- Nos permite disponer de un método probado de restaurar la capacidad para proveer productos y servicios críticos a un nivel y tiempo aceptable.
- Mantiene la capacidad de gestionar riesgos no asegurables.
- Fomenta el trabajo entre equipos.

- Nos capacita para demostrar una respuesta creíble a través de ejercicios y simulacros.
- Mejora nuestra reputación y la imagen exterior de la empresa.
- Permite un mejor posicionamiento estratégico y competitivo a través de la capacidad demostrada de mantener en caso de incidentes, la entrega de productos y servicios.
- Nos permite disponer de una comprensión holística y mas clara de los negocios de la organización (concepción de cada realidad como un todo distinto de la suma de las partes que lo componen) a fin de poder identificar oportunidades de mejora.
- Demuestra que estamos observando en la Organización los requisitos legales y las regulaciones aplicables.

Resultados de la aplicación del programa de BCM en la Organización

Los resultados obtenidos al haber desarrollado y aplicado un programa eficaz de BCM mediante la BS 25999 en la organización son los siguientes:

- Hemos identificado y protegido los productos y servicios claves, asegurando su continuidad.
- Disponemos de la capacidad de gestión de incidentes para proporcionar una respuesta eficaz.
- Nos ha permitido desarrollar, documentar y entender adecuadamente las relaciones con otras organizaciones, órganos de regulación o departamentos gubernamentales, autoridades locales y de servicios de emergencia.
- Ahora disponemos de personal capacitado, para responder eficazmente a un incidente o interrupción mediante la realización de ejercicios y simulacros apropiados.
- El personal de la empresa recibe el soporte y comunicación adecuadas en el caso de una interrupción para continuar las operaciones.
- Aseguramos la cadena de suministro de la organización, porque estamos preparados para interrupciones y sabemos como actuar.
- Protegemos la reputación de la organización.
- Nos permite cumplir no solo con nuestras obligaciones legales y reglamentarias, sino con nuestro compromiso profesional y de servicio.

3. Certificación Norma ISO 22399

3.1. Generalidades

El Plan de Continuidad de Operaciones de esta empresa está basado en la **Norma ISO 22399**, que presenta los principios y elementos generales para la preparación en caso de un incidente y tener continuidad operativa en la organización.

La implantación de este sistema de gestión en la continuidad de operaciones, ha permitido orientar a la organización para desarrollar criterios propios y personalizados y el diseño más adecuado del Sistema de Gestión implantado:

- Identificando objetivos.
- Comprendiendo los obstáculos, los riesgos y perturbaciones que pueden obstaculizar los objetivos críticos.
- Evaluando el riesgo y la tolerancia para entender los resultados de los controles y las estrategias de mitigación.
- Permitiendo alcanzar los objetivos en caso de que se produzca un incidente.
- Permitiendo el establecimiento de procedimientos de actuación.
- Definiendo las funciones, responsabilidades y recursos para responder a un incidente.
- Cumpliendo con las disposiciones legales y reglamentarias.
- Estableciendo medios de comunicación y
- Promoviendo un cambio cultural dentro de la organización.

Plan Continuidad de Operaciones BCM (Business Continuity Management)

El Plan de Continuidad desarrollado e implantado, constituye el conjunto de prácticas profesionales para la **Gestión de Continuidad de Negocio**, cuyo objetivo principal es permitir a las operaciones comerciales de la empresa, el seguir operando bajo condiciones adversas, al implantar estrategias adecuadas, objetivos de recuperación, planes de gestión de crisis y estrategias de gestión de riesgos.

Hemos aplicado las mejores prácticas profesionales según la **Norma ISO 22399**, las cuales desarrollamos más adelante en este mismo documento.

4. Certificación Seguridad de la Información Norma ISO 27001

4.1. Generalidades

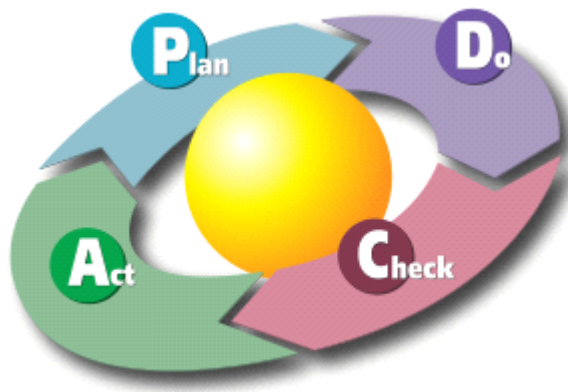
El Plan de Continuidad de Operaciones de esta empresa está basado en la **Norma ISO 27001**, que es una norma internacional auditable que define los requisitos para un sistema de gestión de la seguridad de la información (SGSI).

La norma ha permitido adoptar a la organización un enfoque por procesos para establecer, implantar, operar, supervisar, revisar, mantener y mejorar el SGSI desarrollado.

Sistema de Gestión de Seguridad de la Información (Sistemas GSI)

El sistema de gestión desarrollado e implantado, constituye el conjunto de prácticas profesionales para la **Gestión de la Seguridad de la Información**, no considerando otros aspectos de la empresa, ya que el objetivo principal es permitir mantener la eficacia del Sistema de Información de la Organización, permitiendo el seguir operando bajo condiciones adversas, al implantar estrategias adecuadas, objetivos de recuperación, planes de gestión de crisis y estrategias a tener en cuenta:

- La implantación de la ISO 27001:2005 ha supuesto una inversión en el futuro de la compañía.
- Ha permitido implantar un Sistema de Gestión “*basado en el riesgo*”, para ayudar a la organización, planificación e implementación de un **Sistema de Gestión de Seguridad de la Información (ISMS)**.
- Supone un apoyo notable a la organización, al proveer una aproximación estructurada y proactiva hacia la seguridad de la información:
 - a) Garantizando que las personas, procedimientos, procesos y tecnología apropiados, están en su lugar para proteger informaciones, bienes y activo.
 - b) Ayudando a minimizar posibles daños a organizaciones que pueden ser causadas por acciones deliberadas o accidentales.
- Nos permite implementar un Ciclo de mejora Continua (**Ciclo PDCA**).



El ciclo PDCA (*acrónimo de Plan, Do, Check, Act*), o "Círculo de Deming", es la estrategia implantada en la empresa, que nos permite en cuatro pasos, implementar el concepto de **"Mejora continua"** :

Plan (Planificar)

- Identificar el proceso que se quiere mejorar
- Recopilar datos para profundizar en el conocimiento del proceso
- Análisis e interpretación de los datos
- Establecer los objetivos de mejora
- Detallar las especificaciones de los resultados esperados
- Definir los procesos necesarios para conseguir estos objetivos, verificando las especificaciones

Do (Hacer)

- Ejecutar los procesos definidos en el paso anterior
- Documentar las acciones realizadas.

Check (Verificar)

- Pasado un periodo de tiempo previsto de antemano, volver a recopilar datos de control y analizarlos, comparándolos con los objetivos y especificaciones iniciales, para evaluar si se ha producido la mejora esperada
- Documentar las conclusiones

Act (Actuar)

- Modificar los procesos según las conclusiones del paso anterior para alcanzar los objetivos con las especificaciones iniciales, si fuese necesario
- Aplicar nuevas mejoras, si se han detectado errores en el paso anterior
- Documentar el proceso

Beneficios de implantar en la Organización un Sistema ISO 27001:

- Nos permite tener responsabilidad reducida debido a las políticas y a los procedimientos no implementados o reforzados
- Nos supone la oportunidad de identificar y eliminar flaquezas
- Implica a la Gerencia, participando de la Seguridad de la Información
- Garantiza seguridad a todas las partes interesadas
- Mejor consciencia de la seguridad
- Une recursos con otros sistemas de gerencia

- Mecanismo para medir la gestión del sistema

Razones para adoptar la ISO 27001

- Eficacia mejorada de la Seguridad de la Información
- Diferenciación del Mercado
- Satisfacer exigencias de los clientes
- Único patrón con aceptación global
- Responsabilidades enfocadas al equipo de trabajo
- Atendimento de Requisitos Legales (compliance)