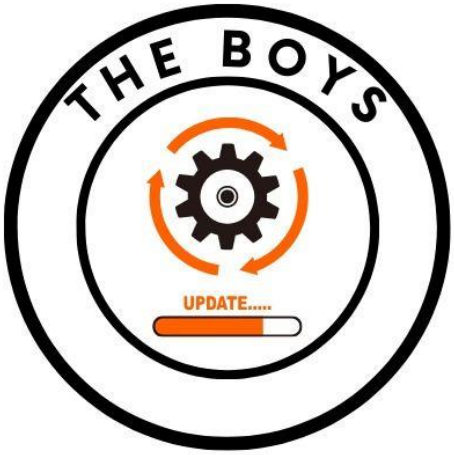

Plan de Continuidad de Negocio (BCP)

PROYECTO FINAL

4o semestre Año 2022

INFORMACIÓN DEL DOCUMENTO

Nombre de Proyecto:	Proyecto Final	
Preparada por:	Diaz, Ariadna Lopez, Federico Torena, Nahuel Vazquez, Christofer Santana, Joaquín	**Fecha:** 13/ 10 / 2022

Versiones

Ver. No.	Fecha Ver.	Actualizado por:	Descripción
1.0	22/10/2022	The Boys	Sprint 3
1.1	05/11/2022	The Boys	Sprint 4

CONTENIDO

Objetivo general

Proponer un BCP para poder detectar amenazas y vulnerabilidades, minimizar riesgos e implementar controles para mejorar la capacidad de reacción ante posibles desastres aplicando una adecuada estrategia de recuperación.

Objetivos específicos

- Proponer un BCP para el departamento de tecnología de la organización basado en análisis de riesgos y en las buenas prácticas dictadas por instituciones de seguridad y por el estándar internacional ISO 22301.

Marco teórico

Este capítulo incluye conceptos y fundamentos teóricos necesarios para llevar a cabo el presente proyecto. Inicia con un glosario de términos basado en definiciones de diferentes guías prácticas, continúa con normas y estándares referentes al BCP. Posteriormente, se presenta el BCP y sus tipos, finalmente se habla de su metodología y sus fases.

Glosario de términos

Ciberseguridad: También conocida como seguridad de tecnologías de la información, se enfoca en proteger los activos de información a través de estrategias y normas para tratar las amenazas que ponen en riesgo la información en sistemas interconectados.

Activos: Se consideran a los recursos que dan soporte a las actividades de negocio de una empresa. Son necesarios para que ésta funcione correctamente y alcance los objetivos planteados.

Procesos críticos: Conjunto de tareas o actividades esenciales para mantener el funcionamiento del negocio.

Contingencia: Evento o suceso no deseado que puede interrumpir las operaciones o actividades de una organización.

Alternativas de recuperación: Conjunto de actividades predefinidas que se las lleva a cabo ante la ocurrencia de un desastre o contingencia.

Incidente: Evento que esta fuera del funcionamiento normal de un proceso u operación, este evento provoca interrupción y baja la calidad de los servicios.

Vulnerabilidades: Falta de control o baja capacidad asociada a un recurso o proceso que puede ser explotada y provoca daño en dichos procesos.

Amenazas: Eventos que aprovechando una vulnerabilidad pueden desencadenar interrupción en las actividades o procesos críticos, pueden provocar incidentes y pérdidas a la empresa.

Disponibilidad: Cualidad o condición de un recurso, proceso y servicio que se encuentre a disposición cuando lo requiera la organización.

Normas y Estándares

ISO 22301: (ISO 22301, 2012) Sistemas de Gestión de Continuidad de Negocio (SGCN). Es la norma internacional certificable para la Gestión de la Continuidad de Negocio y ha sido desarrollada para ayudar a las organizaciones a minimizar el riesgo de interrupciones en sus actividades.
La norma ISO 22301 se integra y se alinea con las normas: ISO 27001 (Gestión de Seguridad de la Información), ISO 9001 (Sistemas de la Gestión de la Calidad) e ISO 20000 (Gestión de servicios de TI), con el objetivo de facilitar la colaboración entre estándares y permitir la asociación en la implantación y operación del sistema de gestión de continuidad de negocio.

Esta norma adopta el ciclo Plan-Do-Check-Act (PDCA) como marco de referencia para el sistema de gestión de continuidad de negocio en todas sus etapas, lo cual hace ideal y ajustable a cualquier tipo y tamaño de empresa.

A continuación, la descripción de las actividades del ciclo.

Plan: Establecimiento de políticas, objetivos, controles, procesos, y procedimientos relacionados a la continuidad de negocio, los cuales entregan valor al negocio.

Do: Planificación de procesos de implementación y operación.

Check: Monitoreo, medición, evaluación, y revisión de resultados que contrasten los objetivos y políticas de continuidad, por lo que se pueden determinar y autorizar acciones correctivas y de mejora.

Act: La realización de acciones autorizadas para garantizar que el SGCN entregue sus resultados y mejore.

Plan de Continuidad de Negocio

En el presente capítulo se desarrollará el plan de continuidad de negocio propuesto en base a guías de implementación (INCIBE) y el estándar ISO 22301. Primero, se define el alcance del proyecto, luego se realiza el análisis de la organización, donde, se conoce el presente de la empresa en temas de continuidad, se identifican aplicaciones, servicios y procesos críticos; después se realiza el análisis de impacto en el negocio, así como también, el análisis de riesgos, identificación de amenazas y vulnerabilidades. Con todo lo anterior, se determinan las estrategias de continuidad, las cuales permitan la recuperación del negocio y disminuyan el impacto negativo de la materialización de eventos no deseados. Finalizando con un el plan de mantenimiento y concienciación del BCP.

Determinación del alcance

Alcance del BCP y explicación de las exclusiones

Definición del alcance del BCP. El alcance que se plantea en el presente proyecto es proponer un plan de continuidad de negocio para el área de IT, este plan tiene como objetivo obtener una óptima capacidad de reacción al producirse un incidente que afecte a las

operaciones del área tecnológica de la empresa. Esto conlleva a disminuir pérdidas de información, monetarias y de imagen para la organización.

Procesos y servicios. Este plan considera los servicios que brinda The Boys a todas las áreas de la organización dentro de su cadena de valor. Además, se toma en consideración los procesos y activos críticos asociados a cada actividad que se realizan en las diferentes áreas de la organización para mejorar su continuidad.

Redes e infraestructura de TI. La siguiente tabla muestra los servicios tecnológicos que se brinda.

SERVICIOS
Aplicación móvil
Aplicación web
Ofimática
Administración de base de datos
Correo electrónico
Internet y Navegación Web
Servidor de archivos
Servicio de respaldos de información
Data Center
Servicio de telefonía IP
Servicio de CCTV
Servicio de impresión
Servidor de dominio
Firewall

Alcance del BCP. El plan de continuidad de negocio será enfocado inicialmente al área de IT.

Responsabilidades para la gestión de la continuidad del negocio. Responsabilidades generales:

- El personal de IT a cargo del plan de continuidad es el responsable de que sea implementado de acuerdo a esta política y proporcionará todos los recursos necesarios.
- El comité de crisis, será el encargado de declarar la situación de crisis y dará el paso a la ejecución del plan de continuidad.

Análisis de la organización

Determinación del contexto de la organización
En los siguientes apartados se presenta la información recabada sobre el contexto.

Análisis de impacto en el negocio (BIA)

Los objetivos de este análisis son: identificar los procesos críticos de la organización, evaluar el impacto operacional que ocasionarían dichos eventos, además establecer los recursos y tiempos de recuperación del negocio. Esta metodología se basa en la norma ISO 22301.

Identificación de actividades de negocio y procesos. En este apartado se identifican las actividades de negocio así también como los procesos que aportan a la producción en la organización y la consecución de sus objetivos.

Identificación de áreas y procesos.

AREA	PROCESOS
Guacheras	Gestión de animales
Zona de galpones y depósitos forrajeros	Almacenamiento-logística
Oficinas	Altas y bajas de activos Análisis y contabilización de facturas
Centro de Datos	Administración de base de datos Gestión de funcionamiento de la infraestructura física y virtual de servidores (Base de datos, Almacenamiento, Aplicaciones web), Gestión de respaldo de servidores

Evaluación de Impactos operacionales

Tomando en cuenta las actividades de negocio es necesario evaluar el impacto que estas ocasionarían en caso de una interrupción.

Valoración del impacto.

Nivel	Detalle
A	La operación es crítica para el negocio, al no contar con esta, el negocio no puede realizarse.
B	La operación es una parte integral del negocio, sin ésta el negocio no podría operar normalmente, pero no es crítica.
C	La operación no es una parte integral de las operaciones de negocio.

Procesos	Servicios	Nivel de impacto
Administración de base de datos	Gestor Base de datos	B
Gestión de respaldo de servidores	Servicio de respaldos de información	A
Gestión de funcionamiento de la infraestructura física y virtual de servidores	Infraestructura de red	A
Gestión de Terneras y Guacheras	Servidor de aplicaciones	B
Protección de la Red Interna	Firewall	A
Comunicación interna mediante telefonía	Servicio de Telefonía Ip	C
Monitoreo mediante cámaras de seguridad de los edificios	Servicio CCTV	C
Autenticación de Usuarios en los sistemas	Servidor de dominio	A

Identificación de procesos críticos y establecimiento de tiempos de recuperación

Una vez identificado el impacto se procede a identificar los procesos críticos en base al impacto que tienen en caso de que ocurra una interrupción. En esta parte también se definió el tiempo máximo de inactividad que un proceso crítico puede estar detenido antes que se produzcan consecuencias irreversibles para el negocio, y se lo define en días. Además, a los procesos críticos se les asigna una ponderación de prioridad, es decir que proceso debe ser restaurado con mayor rapidez y en un orden específico, donde 1 es lo más prioritario y 4 lo menos.

Procesos críticos	Nivel de impacto	Días	Prioridad
Respaldo de servidores	A	2	2
Gestión de funcionamiento de la infraestructura física y virtual de servidores	A	1	1
Protección de la Red Interna	A	1	1
Autenticación de Usuarios en los sistemas	A	1	1

Identificación de recursos

Este punto es clave para identificar los recursos que apoyan a las actividades de negocio críticas. Así se puede dimensionar el impacto que provocaría la interrupción de los servicios que se requieren para que los usuarios realicen sus actividades.

Servicios	Nivel de impacto	Prioridad
Red Interna	A	1
Aplicación Mobile	A	2
Ofimática	B	2
Administración de base de datos	A	1
Correo electrónico	B	2
Aplicación web	A	2
Navegación Web	B	3
Servidor de archivos	B	2
Servicio de telefonía IP	B	2
Servidor de dominio	A	1
Firewall	A	1
Data Center	A	1

Asignación de los RTO y RPO a los recursos

Según la categoría anterior, en la tabla se muestran los recursos tecnológicos más importantes (nivel de impacto A) para el mejoramiento de su continuidad, mostrara la asignación del RTO (Tiempo de recuperación objetivo) y el RPO (Punto de recuperación objetivo) a los recursos principales.

Servicios	Nivel de impacto	Prioridad	RTO (Horas)	RPO (Horas)
Red Interna	A	1	4	8
Data Center	A		2	5
Firewall	A	1	2	10
Servidor de dominio	A	1	2	8
Administración de base de datos	A	1	4	8
Aplicación Mobile	A	2	3	8
Aplicación web	A	2	3	8

Definición y Ejecución del Plan de Pruebas

El plan de pruebas está enfocado principalmente a simular situaciones de contingencia en caso de incidencias producidas sobre equipos, información y procesos, manejados en situaciones reales y cuyos respaldos si pueden ser empleados y replicados en una hipotética situación de contingencia.

Con el fin de garantizar la ejecución integral de la prueba, se diseñará un conjunto de casos de pruebas funcionales. los cuales probarán, verificarán y observarán cualquier incidencia que se origine durante dicha prueba, a fin de retroalimentar cualquier acción que pueda corregir el plan.

Las pruebas relacionadas a este plan, se deberán ejecutar semestralmente con el fin de evaluar la preparación de la entidad, ante la ocurrencia de un siniestro y realizar los ajustes necesarios

Personal responsable de la coordinación e implementación de la prueba y verificación:
Personal TI

Los objetivos de la prueba y verificación son los siguientes:

- Implementar planes de recuperación para cada actividad.
- Garantizar que, en situación de contingencia, la organización podrá recuperarse en los tiempos establecidos.
- Verificar si el personal a cargo está familiarizado con el plan de continuidad.
- Asegurar que todos los recursos necesarios del plan estén disponibles.
- Garantizar que la información del plan se mantiene actualizada.

Método de prueba y verificación:

- Planificar las pruebas en horarios fuera de oficina y con procesos que no afecten al trabajo productivo de la organización.
- Simular el ambiente de un evento o desastre no deseado.
- Aplicar la respuesta a la contingencia.
- Disparar el plan de continuidad de negocio
- Evaluar y revisar los resultados obtenidos.
- Realizar las recomendaciones de mejora.

Concienciación

El personal de TI será el público objetivo de la fase de concienciación. Las necesidades formativas o de concienciación para público objetivo serán temas que tengan que ver con continuidad de negocio (riesgos, medidas preventivas y seguimiento) y seguridad de la información. La organización puede hacer uso de diferentes medios para difundir los temas de concienciación mencionados. La primera opción es difundir a través de la Intranet corporativa, además se enviarán correos electrónicos y también charlas de concientización para lograr la asimilación y adopción del mensaje que se quiere transmitir. Incluso se puede extender la fase de concienciación a terceros o proveedores los cuales sean aliados estratégicos de la empresa. Todo lo anterior mencionado es con el objetivo de lograr una comunicación efectiva con los involucrados y que sean conscientes de la importancia de un plan de continuidad de negocio en todas sus fases.