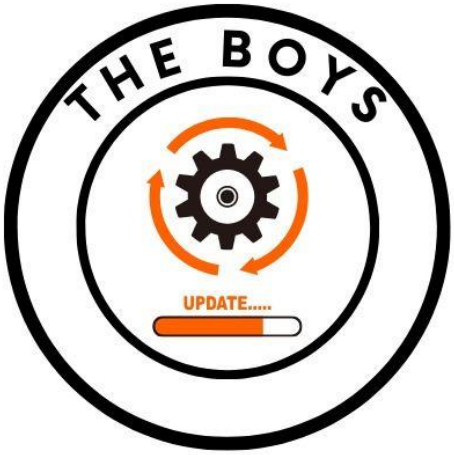

Plan de Recuperación de Desastres (DRP)

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:** 05/ 11 / 2022

Versiones

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

CONTENIDO

Análisis de Riesgos

Para poder realizar el análisis de riesgos, identificamos los activos de TI más críticos para el negocio, debido a que de este modo podemos enfocarnos en lo que realmente puede ser afectado si se llegase a efectuar algunas amenazas.

DISPOSITIVOS	UBICACIÓN
Servidor de base de datos	Data Center
Servidor de Aplicaciones	Data Center
Servidor Active Directory	Data Center
Sistema de respaldo	Data Center
Firewall	Data Center

Listado de amenazas a considerar

AMENAZA	TIPO
Huracanes	Naturales
Incendios	Naturales / Accidentales
Tornados	Naturales
Tormentas tropicales	Naturales
Desbordamiento de ríos	Naturales
Hundimiento de tierra	Naturales
Tormentas eléctricas	Naturales
Cambios climáticos	Naturales
Temperaturas extremas	Naturales
Insectos	Biológicas
Roedores	Biológicas
Contaminación	Biológicas
Explosiones	Accidentales
Corto circuito	Accidentales
Rotura de los conductos de electricidad	Accidentales
Colapso de estructuras	Accidentales
Fallas de suministro eléctrico	Accidentales
Interrupción de sistemas de información	Accidentales
Problemas financieros	Accidentales
Robo	Premeditadas
Vandalismo	Premeditadas
Sabotajes	Premeditadas
Defectos de fábrica	Premeditadas
Fallos energía eléctrica	Informáticos
Telecomunicaciones	Informáticos
Fallo en las aplicaciones	Informáticos
Fallos en los sistemas operativos	Informáticos

Para esta propuesta se tomaron los siguientes riesgos, los cuales se consideran que son los más propensos a materializarse:

AMENAZAS	CONSECUENCIA	PROBABILIDAD	RIESGO
Espionaje remoto	SIGNIFICATIVA	POCO PROBABLE	BAJO
Robo de información	SIGNIFICATIVA	POCO PROBABLE	MEDIO
Robo de información mediante uso de hardware	SIGNIFICATIVA	POCO PROBABLE	MEDIO
Robo de información mediante uso de software	SIGNIFICATIVA	POCO PROBABLE	MEDIO
Destrucción de información	SIGNIFICATIVA	POCO PROBABLE	MEDIO
Alteración no autorizada de los datos	SIGNIFICATIVA	POCO PROBABLE	MEDIO
Fuego	CATASTRÓFICA	POCO PROBABLE	MEDIO
Daño por agua	SIGNIFICATIVA	POCO PROBABLE	MEDIO
Destrucción de equipos o medios	CATASTRÓFICA	POCO PROBABLE	MEDIO
Corrosión	LEVE	POCO PROBABLE	BAJO
Fenómenos climáticos	CATASTRÓFICA	MUY POSIBLE	ALTO
Falla de los equipos	SIGNIFICATIVA	MUY POSIBLE	ALTO
Mal funcionamiento de los equipos	SIGNIFICATIVA	PROBABLE	MEDIO
Falla en el sistema de aire acondicionado	MODERADO	PROBABLE	MEDIO
Pérdida del suministro de energía	SIGNIFICATIVA	MEDIANA	MEDIO

Las vulnerabilidades detectadas durante el análisis de riesgo pueden ser mitigadas con diferentes tipos de controles. Al hacer esto se reduce en algunos casos la probabilidad de que se genere del riesgo, entre los controles más básicos con los cuales debe contar están:

Cableado estructurado
Sistema de corriente eléctrica regulado
Sistemas de resplado de energía (UPS)
Backup diario de toda la información
Detectores de humendad, agua, fuego y humo
Piezas de hardware de respaldo
Firewall físico o lógico
Antivirus
Almacenamiento externo de copias de seguridad

Matriz de estrategias

TIPO DE SITIO ALTERNO	COSTO	EQUIPAMIENTO DE HARDWARE	COMUNICACIÓN	TIEMPO CONFIGURACIÓN	SITIO
COLD	Bajo	Ninguno	Ninguno	Largo Entre 24 y 72 horas	Centro de Computo Alterno
WARM	Medio	Parcial	Parcial / Completo	Medio Entre 8 y 24 horas	Centro de Computo Alterno / Nube
HOT	Alto	Completo	Completo	Corto Entre 4 y 8 horas	Centro de Computo alterno / Nube
MIRROR	Muy Alto	Completo	Completo	Ninguno 0 horas	Centro de Computo Alterno / Cloud

Elección de Estrategias de Recuperación

Luego de analizar los costos que podrían generar implementar una estrategia de recuperación se optara por implementar un sitio preparado (Hot Site) para que si ocurre algún tipo de desastre sea del tipo que sea tengamos una rápida respuesta de recuperación. Para esto mediante investigaciones concluimos que lo mejor en estos casos es tener un sitio que se considere seguro dentro del edificio y que este pronto con toda la infraestructura física y lógica necesaria para iniciar la recuperación luego de un desastre lo más rápido posible. Es cierto que tener un sitio que cuente con una infraestructura que sea capas de abarcar todos los servicios del negocio lleva un costo mas elevado al momento de cotizar el hardware y software necesarios, pero esto nos garantiza de que las operaciones del negocio se puedan reinstaurar con mayor velocidad. Para esto se incorporarán nuevos Racks, servidores, firewall, switches y cableado para tener montado los servicios necesarios en caso de una urgencia. También como una tercera estrategia se utilizará un servicio cloud tercerializado como puede ser Azure o AWS

Es necesario realizar el respaldo por cada equipo cada una semana, y en los sectores que se maneje información más delicada 2 o 3 veces por semana dependiendo de la cantidad de información.

EQUIPOS DE RECUPERACION

Equipo de TI

Función Principal

Recuperar y restaurar el ambiente operativo de sistemas en lo relacionado con hardware, software y comunicaciones en el sitio alterno, garantizando el soporte informático al negocio.

Funciones o Tareas

Previas al Desastre:

- Tener un inventario actualizado de los equipos.
- Identificar y documentar los procedimientos de respaldo y recuperación
- Probar los procedimientos de respaldo/recuperación en el sitio alterno y en el sitio principal
- Revisar y analizar los resultados de las pruebas e implantar las modificaciones según sea necesario
- Verificar la disponibilidad del sitio alterno.

Durante el Desastre:

- Restaurar el ambiente operativo en el sitio alterno de recuperación
- Proporcionar asistencia al usuario final en los sistemas de información según se requiera.
- Evaluar el equipo y las instalaciones dañadas para su reparación o reemplazo.
- Preparar listas detalladas de los equipos que requieren reparación o reemplazo.
- Ejecutar los procedimientos necesarios o para trasladar los equipos a un nuevo ambiente y de ser necesarios, adquirir otros nuevos.
- Asegurar que el procesamiento normal pueda llevarse a cabo tan pronto como el sistema, equipos y comunicaciones requeridos, estén disponibles.

Posterior al Desastre:

- Evaluar la efectividad del plan de recuperación para su área de responsabilidad.
- Evaluar la efectividad del equipo de trabajo durante la contingencia.
- Informar sobre el impacto del daño.

INTEGRANTES	
FUNCION	NOMBRE
Administrador de Red	Joaquín Santana
Administrador de Red	Federico López
Administrador de Red	Nahuel Torena
Administrador de Red	Ariadna Diaz

En base al Análisis de impacto de negocio revisado en el documento de continuidad de negocio y considerando que primero se deberá tener todo el equipamiento de red, así como los principales servidores de soporte a los sistemas, se tiene que reponer lo siguiente.

Prioridad de recuperación 1

SERVIDORES MINIMOS PARA LA CONTINGENCIA
Windows Server 2012r2 (Controlador de dominio)
Windows Server 2012r2 (Servidor de aplicaciones Wildfly)
Windows Server 2012r2 (Servidor de Base de Datos Oracle)
Veeam (Sistema de Backup)

Prioridad de recuperación 2

SERVIDORES MINIMOS PARA LA CONTINGENCIA
Servidor de correo electrónico
Servidor de Archivos
Servicio de telefonía IP

SITIO ALTERNO

De acuerdo a la estrategia y a la alternativa de solución elegida, se procede a definir las condiciones mínimas de infraestructura y equipamiento que debe cumplir el sitio alterno en caso de ocurrencia de una contingencia.

Sala de Servidores

- 1 Rack
- 1 Switch (24 Puertos)
- 1 UPS APC modelo 3000VA Smart
- 1 Firewall (Fortinet)
- 1 Estación de trabajo
- Sistema de refrigeración (AA),

Plan de Pruebas de DRP

Objetivos del Plan de Pruebas.

Practicar los procedimientos ante un incidente o desastre. Identificar áreas que necesitan mejorar. Permitir al DRP permanecer activo, actualizado, entendible y usable. Demostrar la habilidad de recuperación.

Alcance de las pruebas

Las pruebas deben ejecutarse durante un tiempo en el que las afectaciones de la operación normal sean mínimas y debe comprender elementos críticos y simular condiciones de proceso, aunque se realicen fuera del horario laboral. Las pruebas deben incluir las siguientes tareas

- Verificar la totalidad y precisión del plan.
- Evaluar el desempeño del personal involucrado.
- Medir el desempeño de los sistemas operativos

Durante esta etapa se debe establecer un programa de pruebas con escenarios simulados, planeados en el tiempo

Servicio Afectado	Consecuencia	Afectado por
Data Center	No disponibilidad	Incendio, daño del sistema de aire acondicionado, daño eléctrico
Red	No disponibilidad de los servicios de red	Swicth core, Firewall, cableado.
Servidores	No disponibilidad por fallas	Servidores críticos
Base de datos, almacenamiento y respaldo	No disponibilidad de datos e información	Corrupcion de la BD, borrado o perdida de datos, fallas en el almacenamiento, falla total de respaldos

Actividades de notificación, evaluación y activación del DRP.

Los usuarios deben reportar el incidente cuando:

- No se pueden utilizar los sistemas de información de la organización.
- No hay red de comunicaciones.
- No tengan salida a Internet
- No se puedan loguear a su estación de trabajo
- No puedan consultar información a la base de datos.

El personal de vigilancia debe reportar el incidente cuando:

- Suena la alarma del DC.
- Hay inundación en cualquier piso.
- Hay un amago de incendio en el piso donde se encuentre ubicado el DC
- Cualquier otro evento que afecte o pueda afectar el DC.

En cualquiera de los casos, debe escalarlo a los funcionarios responsables. El profesional especializado del servicio afectado, debe realizar un diagnóstico sobre el incidente presentado, teniendo en cuenta:

- Naturaleza e impacto del incidente.
- Estrategias definidas en el DRP aplicables u otras soluciones potenciales.
- Tiempo estimado de solución del incidente.

El equipo de TI, coordina la ejecución de las actividades para recuperar los servicios en el DC Alterno, teniendo en cuenta:

- Enrutamiento y activación de las comunicaciones hacia el DC alterno.
- Detención de la replicación de datos.
- Verificación de la disponibilidad de información en el DC alterno.
- Activación servicio de controladores de dominio y sistema operativo en servidores.
- Activación servicio de bases de datos y aplicaciones.

El equipo de TI, verifica la disponibilidad de los servicios desde el DC alterno, teniendo en cuenta:

- Acceder a los sistemas de información.
- Realizar pruebas sobre los sistemas de información.

Si es un evento que afectó las comunicaciones.

- Configurar el switch de contingencia, en caso de falla en el switch core.
- Contactar al proveedor de comunicaciones, en caso de falla en el router de enlaces con ISP.
- Enrutar el tráfico por los demás switch en caso de una falla de la fibra óptica de uno de ellos.
- Configurar el firewall de contingencia, en caso de falla del equipo principal.
- Configurar el servidor de contingencia
- Activar los servidores de contingencia.
- Recuperación de información y bases de datos desde los respaldos, en caso de corrupción de la base de datos, y borrado o pérdida de datos.
- Utilizar los discos de contingencia ante una falla.
- Configurar el servidor de contingencia como servidor de respaldo, en caso de falla del principal.