UNIVERSIDAD NACIONAL DE INGENIERÍA
RECINTO UNIVERSITARIO "SIMÓN BOLÍVAR"
FACULTAD DE ELECTROTECNIA Y COMPUTACIÓN

TRABAJO MONOGRÁFICO

"Plan de gestión de la continuidad de negocio en los servidores de bases de datos del departamento de informática de la empresa ACME"

PARA OPTAR AL TÍTULO DE
INGENIERO EN COMPUTACIÓN

ELABORADO POR:
Br. Luis Manuel Menocal López
Br. Moisés Enrique Zeledón Rocha

TUTOR:
MSc. Gabriel Rafael Lacayo Saballos.

MANAGUA, NICARAGUA
ABRIL 2022

Agradecimientos

A Dios por haberme dado la vida, salud y sabiduría para lograr terminar con éxito esta etapa.

A mi madre y padre por su amor, trabajo y sacrificio incondicional en este largo y arduo camino, gracias a ellos he logrado llegar hasta aquí y convertirme en lo que soy.

A mi esposa por su amor, apoyo y por estar siempre a mi lado en las buenas y en las malas.

A mis hermanas y hermanos por estar en cada momento de mi vida, por animarme y apoyarme siempre en cada una de las dificultades.

A mi tutor MSc. Gabriel Rafael Lacayo Saballos que nos apoyó en todo momento.

A John y Dana McPherson por todo el cariño y apoyo incondicional que me brindaron a lo largo de mi ciclo Universitario.

Luis Manuel Menocal López

Dedicatoria

Dedico este trabajo primeramente a Dios por darme la sabiduría, inteligencia y las fuerzas necesarias para poder sacar adelante este proyecto y alcanzar la meta de obtener nuestro título profesional.

A mi hijo Miguel Ángel por ser el motor de mi vida, por tanta alegría y fuerza que me dio para seguir adelante en este trabajo.

A mi madre Bertha María y mi padre Manuel Ángel, por todo el sacrificio y apoyo en todo este tiempo.

A toda mi familia por todo el apoyo que me han dado.

Luis Manuel Menocal López

Agradecimientos.

A mi madre por apoyarme en todo momento y saber aconsejarme.

A mi compañero Luis Menocal por haberme tenido paciencia y apoyado durante el transcurso de la carrera y este trabajo de culminación.

Al tutor MSc. Gabriel Rafael Lacayo Saballos por haberme tutorado a lo largo del desarrollo y culminación de este documento, así como de su apoyo, consejo y tiempo dedicado.

Moisés Enrique Zeledón Rocha

Dedicatoria.

A mi madre que ha sabido formarme con buenos hábitos y valores lo cual me ha ayudado a salir adelante y mantenerme en el camino correcto.

A todos mis amigos que de una u otra forma me apoyaron para realizar este trabajo, por sus consejos, paciencia y toda la ayuda que me brindaron para concluir este documento.

Moisés Enrique Zeledón Rocha

RESUMEN

El presente proyecto monográfico efectuado en la empresa ACME, tuvo como fin el desarrollo de un plan de continuidad a los servidores de base de datos, con el cual se pudo identificar los riesgos asociados a los activos de los sistemas de base de datos de la empresa ACME.

En el proceso de identificación de los riesgos se utilizó el método de herramientas de observación y recolección de información como un cuestionario al personal del área de base de datos, para identificar las principales amenazas que afectan a los servidores de base de datos, con el fin de determinar el nivel de riesgo que alcanza cada amenaza.

A partir de los resultados obtenidos en el análisis y evaluación de riesgos, se presentarán estrategias que ayuden a preservar la continuidad de las operaciones del departamento de informática de la empresa ACME ante posibles escenarios de interrupción que afecten a los sistemas de base de datos.

.

ÍNDICE

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE TABLAS

ÍNDICE DE GRAFICOS

INTRODUCCIÓN

Las empresas, para asegurar el cumplimiento de sus operaciones, se apoyan en los procesos de tecnología con el fin de asegurar que los servicios brindados tanto a sus clientes internos como externos y demás partes interesadas, se den con la eficiencia que se requiere; así mismo, para que los servicios que ofrecen, con la oportunidad y calidad planificadas.

En tal sentido, uno de los aspectos de mayor importancia, es la salvaguarda de la información que se produce, procesa y administra, por ello, se deben evitar riesgos de pérdida de información o servicios por fallas de cualquier índole. Es así como el Plan de Continuidad se convierte en un mecanismo sustantivo para mantener en operación el conjunto de procesos, procedimientos, asegurar los recursos físicos, técnicos y humanos que interactúan ante la presencia de un incidente.

Un plan de continuidad, es un instrumento de gestión para el buen gobierno de las Tecnología de la Información y las Comunicaciones que tiene como fin, garantizar la continuidad de los servicios de TI.

El presente trabajo monográfico tiene como finalidad elaborar un plan de continuidad de negocio en los servidores de base de datos con el propósito de evaluar e identificar en qué casos los controles son suficiente o que procesos requieren ser mejorados, para posteriormente emitir las estrategias pertinentes y de esta manera mejorar los procesos en cuanto a la continuidad de los servidores de bases de datos en la empresa ACME[1].

[1] Por petición de la empresa a la cual se está realizando el estudio y debido a la naturaleza de datos críticos (integridad, disponibilidad y confidencialidad de la información que maneja), se ha tomado la decisión de utilizar un alias como alternativa de uso al nombre real de la empresa, siendo el alias a emplear a partir de este punto: ACME.

ANTECEDENTES

En los últimos dos años la empresa ACME ha sufrido incidentes que han dejado paralizados varios sistemas importantes para la continuidad del negocio, entre ellos se menciona un incidente ocasionado por fallas en el sistema de climatización, por desconexión accidental del cable de enlace de datos y por agotamiento de recursos en los servidores de base de datos.

Una empresa como ACME no puede tener control total sobre las amenazas, por lo que requiere establecer medidas de protección para que en caso de ocurrir una amenaza cause la mínima afectación posible.

Es por ello que a medida que las tecnologías de información y comunicación (TIC) fueron tomando mayor impulso y relevancia en el país, sumado a la necesidad surgida en la empresa ACME por automatizar sus servicios de cara a los clientes a fin de lograr una mejor atención, es a partir del año 2010 que surgen nuevos proyectos y con ellos la obligación de administrarlos de la mejor manera posible.

A partir del año 2014, para reforzar el buen funcionamiento de los sistemas de la empresa y brindar un mejor servicio a los clientes, el departamento de informática en común acuerdo con la dirección superior de la empresa ACME llevó a cabo el proyecto de un Centro de Datos alterno ubicado en las afueras de Managua. Este centro de datos alterno tiene como objetivo ayudar a mitigar el tiempo de pérdida de servicios en caso de fallas en el centro de datos principal.

En estos últimos 6 años de la existencia del departamento de informática, se ha logrado un crecimiento significativo en la actualización de métodos y procesos que ayuden a preservar la disponibilidad de los sistemas, pero aún existen factores que impiden que el nivel empresarial pueda crecer mucho más.

JUSTIFICACIÓN

El departamento de informática no cuenta con registros previos de auditoría y planes de continuidad a los sistemas de bases de datos, únicamente se realizan ventanas de mantenimientos que son programadas cuando ocurre una falla en algún sistema o equipo de hardware determinado, no hay controles previamente establecidos que regulen los mantenimientos continuos y los procedimientos apropiados que ayude a mitigar interrupciones con el fin seguir brindando los servicios a la población en general.

Por las razones anteriormente expuestas surge la necesidad de elaborar un plan de continuidad en los servidores de base de datos, con el objetivo de adoptar estrategias que ayude a mitigar cualquier interrupción que afecten los sistemas de bases de datos de la empresa ACME.

Con el desarrollo de este plan de continuidad se evaluará la eficiencia que la empresa posee, con el fin de determinar recomendaciones que mejoren sus operaciones.

El resultado de este estudio servirá de referencia para la toma de decisiones encaminadas a mejorar la administración y control de los sistemas de bases de datos, además mitigaría los riesgos de pérdidas de servicios. Esto permitirá a la empresa tener un rendimiento óptimo en sus labores diarias mejorando su desempeño de una manera más eficiente y aportando a la estabilidad empresarial.

OBJETIVOS

Objetivo general

- Elaborar un plan de continuidad de negocio en los servidores de bases de datos de la empresa ACME.

Objetivos Específicos

- Definir la situación actual de los servidores de base de datos de la empresa ACME.
- Identificar los activos críticos para la continuidad de los servidores de base de datos de la empresa ACME.
- Determinar los riesgos asociados a los activos en los servidores de bases de datos.
- Preparar las estrategias de respuesta y recuperación necesarias dentro del plan de continuidad en los servidores de base de datos de la empresa ACME.

CAPITULO I: Marco teórico

El presente capítulo contiene la base teórica para el sustento y entendimiento necesario en el desarrollo de esta investigación.

Primeramente, se introducen los conceptos de riesgo y continuidad de negocio que son de importancia para el desarrollo tanto de la investigación como para el plan de continuidad en los servidores de bases de datos.

Más adelante se contemplan conceptos de tipo de estrategias. Además, se abordan los roles que puede manejar la organización según la (CCSS, 2007).

Finalmente, se consideran las normas y modelos necesarios para el desarrollo e implantación de un plan de continuidad de TI.

1.1. Riesgo

Para contextualizar el término de riesgo, (Fiorito, 2006) lo define como situaciones que involucran incertidumbre, en el sentido de que el rango de posibles resultados para una determinada acción es en cierta medida significativo.

Además, es importante agregar que el riesgo hace referencia a la probabilidad de que una determinada amenaza logre materializarse en un evento, localizado en el tiempo que supere la capacidad de atención de una organización con sus recursos habituales. (Soldano, 2009).

1.1.1. Riesgos TI

Las tecnologías de información y comunicación dentro de una organización no se encuentran ajenas a diferentes situaciones asociadas, como lo son los riesgos de TI.

Los riesgos TI pueden ocasionar periodos de inactividad de operaciones dentro de una organización, provocando desde la pérdida de productividad, la exposición de información de clientes por perdida hasta la inadecuada gestión de registros (Zumba, 2015).

1.1.2. Análisis de riesgos

Dentro de la norma internacional ISO 31010 (2009), se define el análisis de riesgos como un proceso estructurado que logra identificar cómo pueden ser afectados los objetivos de una organización por la materialización de un riesgo, igualmente permite generar una visión del riesgo en término de consecuencias y de su respectiva probabilidad con el objetivo y, generar los criterios necesarios para la toma de decisiones proactivas que logren prevenirlos o mitigarlos.

El análisis de riesgo es el proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una organización, de igual forma es una herramienta de gestión que permite tomar decisiones. Las decisiones pueden tomarse antes de desplegar un servicio o con éste funcionando. (PAE, 2012)

La importancia del análisis de riesgos dentro del desarrollo de un plan de continuidad, está comprendida por la identificación real del riesgo que puede afectar las operaciones dentro de una organización y con esto, lograr desarrollar estrategias dirigidas a contrarrestar dichos riesgos. (Martínez, 2018)

1.2. Continuidad de Negocio

Con el propósito de contextualizar el término de continuidad del negocio, se hace referencia a lo indicado dentro del estándar internacional ISO 22301 (2012), donde enmarca que, la continuidad del negocio es la capacidad de continuar entregando un producto o brindando un servicio dentro de niveles previamente definidos, después de un evento alterador que interrumpa la continuidad de sus operaciones.

Por lo tanto, tomando en consideración la definición anterior, garantizar la continuidad de las operaciones y servicios de un negocio, requiere mantener en un estado óptimo los niveles de servicios, considerando aplicaciones, accesos a red, servidores e infraestructura.

Dada la importancia del papel que desempeña TI dentro de una organización de acuerdo con la definición, contar con un plan de continuidad permite a los colaboradores del área o departamento que gestiona TI, contar con estrategias que permitan garantizar ante cualquier interrupción, la continuidad de las operaciones del negocio que son soportadas por TI. (Martínez, 2018)

1.2.1. Plan de continuidad

Un plan de continuidad se compone de procedimientos debidamente documentados que permiten guiar a la organización a reanudar y restablecer los niveles de operación luego de sufrir una interrupción de sus procesos (Martínez, 2018).

Dentro de sus objetivos, un plan de continuidad del negocio se enfoca en sostener las funciones del negocio durante y después de una interrupción a los procesos críticos de la organización, identifica las amenazas potenciales y los impactos a las operaciones que esas amenazas podrían causar si se llegaran a materializar Filippi (2012).

Filippi (2012) también mencionan que el éxito de un plan de continuidad de negocio depende de la correcta identificación de roles, asignación de responsabilidades y entrenamiento dentro de los colaboradores de la organización.

Además, un proceso de planeación para el desarrollo de un plan de continuidad de negocio según (Cerullo, 2004), debe alcanzar los siguientes objetivos:

- Identificar los mayores riesgos de interrupción del negocio.
- Desarrollo de un plan para reducir el impacto de riesgos identificados.
- Probar la efectividad del plan de continuidad.
- Capacitar a los colaboradores en la ejecución del plan de continuidad.

Es importante detallar que, dentro de una organización, un plan de continuidad es un componente clave para garantizar las operaciones críticas del negocio, por tal importancia, según (Martínez, 2018) un plan de continuidad debe ser respaldado por normas que garanticen las estrategias adecuadas a aplicar dentro del plan.

1.2.2. Importancia del plan de continuidad de negocio

Un Plan de continuidad de Negocio debe ser considerado parte integral de la estrategia del negocio. Un buen plan revisa los procesos críticos de la operación en las empresas, los clasifica, prioriza y determina cuales son los más sensibles y cuales no pueden dejar de operar para que el negocio continúe su funcionamiento. Si las empresas no cuidan ni manejan correctamente su información, en el momento en que padezcan una eventualidad no podrán atender asuntos prioritarios como: a quien le deben pagar, quien les debe, a quien le venden, a quién le deben otorgar un descuento, quién es meritorio de un crédito, entre otras variables vitales del negocio, (Mieles, 2020).

El hecho de no poder acceder a estos datos puede ocasionar importantes pérdidas al negocio.

1.2.3. Objetivo de un plan de continuidad de negocio

Brindar la capacidad a la organización de continuar con los procesos de negocio con normalidad o al menos a un nivel mínimo aceptable en caso de producirse una interrupción o eventos como desastres naturales, manifestaciones sociales, fallas tecnológicas o fallas humanas que afecten o interrumpan los procesos de negocio disminuyendo el impacto ante cualquier incidente, (Yomayuza, 2018).

1.2.4. Beneficios del plan de continuidad de negocios

Un plan de continuidad de negocio trae consigo muchos beneficios para cualquier organización sin importar su tamaño o actividad económica, aunque muchas veces las organizaciones lo ven como un gasto este debería considerarse como una inversión para la organización ya que no se debe ver desde el punto de cuánto cuesta sino cuánto podría llegar a perder la organización en cualquier incidente de estos.

- Mejora y ayuda a mantener una buena imagen de la organización para con sus empleados y sus clientes.
- Eficiencia organizacional, ya que ayuda a establecer, implementar y mejorar los procesos de la organización, ya que brinda un enfoque organizado para las acciones de respuesta y mejora.
- Mantiene la continuidad de negocio y la prestación de productos y servicios brindando así un soporte o una confiabilidad tanto para el negocio como para sus clientes.
- Identificación de los activos y recursos más relevantes o importantes para garantizar la prestación de sus servicios.
- Evaluación e identificación de los riesgos a los que está expuesta la organización sus recursos y sus activos.
- Identificación de los servicios más críticos de la organización.

- Brinda una rápida acción de respuesta ante cualquier incidente que se presente en la organización y que afecte el correcto desarrollo de sus procesos.
- Evita la perdida de dinero y costos innecesarios a causa de las afectaciones de los servicios críticos.

1.3. Información requerida

Para la creación de un plan de continuidad, Livingstone (2010) recomienda que este debe comprender las siguientes secciones:

- Descripción funcional: Definición de las funciones del proceso.
- Dependencias: Procesos requeridos para el funcionamiento de un proceso crítico.
- Contactos de recuperación: Contactos de líderes del equipo encargado del plan de recuperación.
- Procesos de recuperación: Proceso paso a paso necesarios para alcanzar la recuperación del proceso.

1.4. Tipo de estrategias

Dentro de un plan de continuidad según (Huércano, 2020), especifican dentro del libro *ITIL Service Design* que se debe combinar estrategias proactivas y reactivas con el objetivo de gestionar ya sea una posible interrupción o su materialización.

Las estrategias proactivas tienen dos objetivos principales:

- Reducir las consecuencias de una interrupción.
- Impedir la materialización de una interrupción.

Igualmente, las estrategias reactivas tienen como objetivo reanudar el servicio lo más pronto posible.

1.5. Organización y administración del plan de continuidad de TI

Para ejercer el correcto manejo del plan de continuidad de TI, es requerido definir los roles que poseerá el equipo a cargo de la administración, coordinación, ejecución y desarrollo (CCSS, 2007).

A continuación, se presentan los posibles roles que puede manejar la organización:

1.5.1. Coordinador del plan

Es el responsable de supervisar y coordinar todas las actividades de recuperación establecidas dentro del plan de continuidad de TI.

Igualmente, es responsable de acumular y administrar toda la información generada una vez iniciado el plan de continuidad.

1.5.2. Líder de equipo

Debe ser una persona con liderazgo y con capacidad de tomar decisiones durante un periodo de recuperación. Deberán realizar las siguientes tareas:

- Participar en las sesiones de trabajo programadas.
- Aportar en el proceso de análisis y diseño de los procedimientos de recuperación.
- Liderar la recuperación del proceso de negocios a su cargo.
- Identificar e implantar mejoras al plan de continuidad.
- Mantenimiento de la información del estado de recuperación.
- Coordinar con otros equipos de recuperación.

1.5.3. Miembros de equipo

Los miembros del equipo son los encargados de ejecutar las acciones de recuperación de los sistemas de TI.

1.5.4. Equipos para la continuidad

Para la gestión de un plan de continuidad de TI, es necesario la conformación de equipos que logren brindar su soporte. Como parte de la organización dentro de un plan de continuidad de TI, se pueden definir los cuatro equipos con un respectivo alcance y responsabilidades (CCSS, 2007).

Equipo de tecnología de información

Equipo encargado de supervisar y coordinar todas las acciones internas de recuperación y monitorea el avance de las acciones realizadas por los equipos de operaciones, comunicaciones y aplicaciones respectivamente (CCSS, 2007).

Dentro de las responsabilidades del equipo de tecnología de información se encuentran:

- Analizar los reportes de daños.
- Reportar el estado de la recuperación y cualquier otro problema que se presente.
- Servir de punto focal para las consultas planteadas por el personal de recuperación.
- Habilitar el sitio alterno para la recuperación de las aplicaciones.

Equipo de comunicación

El equipo de comunicación se encarga de todas las acciones de recuperación de las comunicaciones y debe brindar informes al líder del área de tecnología de información.

Dentro de las responsabilidades del equipo de comunicaciones se encuentran:

- Desarrollar y documentar la configuración de las comunicaciones.
- Ordenar e instalar el hardware necesario para establecer la comunicación entre las oficinas.
- Coordinar con entes externos para restaurar el servicio de comunicaciones.
- Comprobar que las comunicaciones se hayan establecido correctamente.

Equipo de operación

El equipo de operación debe asegurar el avance de la restauración de las operaciones de las plataformas críticas y debe brindar informes al líder del área de tecnología de información.

Dentro de las responsabilidades del equipo de operación se encuentran:

- Asegurar la disponibilidad de los respaldos.
- Restaurar archivos y sistemas operativos.
- Ordenar e instalar el hardware requerido para el procesamiento normal de las operaciones.

Equipo de aplicaciones

El equipo de aplicaciones supervisa la restauración de las aplicaciones que residen dentro de los distintos ambientes existentes. Además, debe coordinar y brindar informes al líder del área de tecnología de información.

Dentro de las responsabilidades del equipo de aplicaciones se encuentran:

- Coordinar la recuperación de las aplicaciones.
- Reconstruir el ambiente de operación de las aplicaciones que residen en los servidores.
- Desarrollar un plan de trabajo detallado para el traslado de operaciones del sitio principal al sitio alterno.

1.5.5. Habilidades requeridas por el personal

Dentro del manual para elaborar un plan de continuidad creado por la (CCSS, 2007), en conjunto con los procesos que maneja el departamento de informática de la empresa ACME, se recomienda establecer un conjunto de actividades específicas que debe contar cada posición dentro de los equipos para la continuidad (Véase Tabla 1).

Tabla 1: Habilidades requeridas por el personal.

Nombre	Habilidades generales	Habilidades especificas
Coordinador del plan de continuidad de TI	• Capacidades de trabajo en equipo y coordinación con los miembros de los demás equipos	• Conocimiento de la plataforma tecnológica • Conocimiento técnico en la infraestructura de comunicaciones • Conocimientos del portafolio de sistemas de la organización
Líder del equipo de comunicación		
Líder del equipo de operaciones		
Líder del equipo de sistemas		
Miembros de los equipos de recuperación	• Capacidad de trabajo en equipo	• Conocimiento técnico de la plataforma, sistemas y comunicaciones

Fuente: CCSS (2007)

1.6. Normas, guías y manuales

En este punto se presentan de forma resumida, una serie de guías, metodologías y normas que complementan el marco de conocimiento considerado para la investigación que soporta este trabajo monográfico.

1.6.1. Metodología para realizar el análisis y gestión de riesgos

Magerit es una metodología elaborada y promovida por el CSAE (Consejo Superior de Administración Electrónica) del gobierno de España, que implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información (PAE, 2012).

`

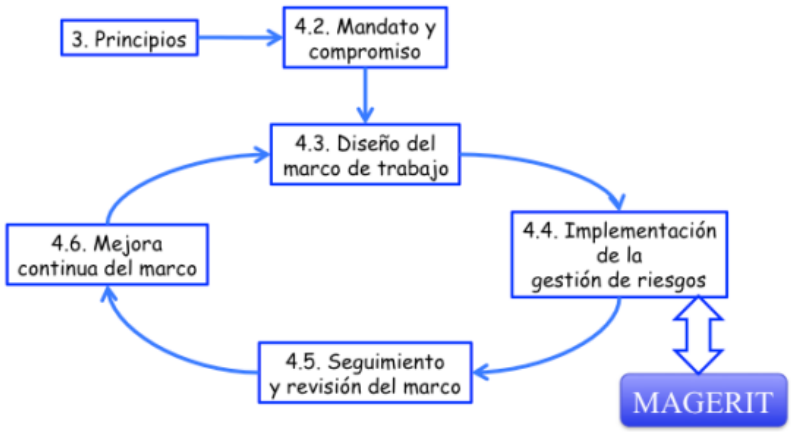


Ilustración 1: Marco de trabajo para la gestión de riesgo.

Fuente: Magerit 3.0 Libro I: Método

Objetivo de Magerit.

El objetivo principal de Magerit es concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos, así como ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC) (PAE, 2012).

A lo anterior mencionado también se le debe agregar que preparar a la organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

Método de Análisis de Riesgo

El análisis de riesgos es una aproximación metódica para determinar el riesgo siguiendo los pasos que se detallan a continuación:

Caracterización de los activos

Esta actividad busca identificar los activos relevantes dentro del sistema a analizar, caracterizándolos por el tipo de activo, identificando las relaciones entre los diferentes activos, determinando en qué dimensiones de seguridad son importantes y valorando esta importancia.

Subtareas:

- Identificación de los activos: Identificar los activos que componen el sistema, determinando sus características, atributos y clasificación.
- Dependencias entre activos: Identificar y valorar las dependencias entre activos, es decir la medida en que un activo de orden superior se puede ver perjudicado por una amenaza materializada sobre un activo de orden inferior.
- Valoración de los activos: Identificar en qué dimensión es valioso el activo.

Caracterización de las amenazas

Esta actividad busca identificar las amenazas relevantes sobre el sistema a analizar, caracterizándolas por las estimaciones de ocurrencia (probabilidad) y daño causado (degradación).

Subtareas:

- Identificación de las amenazas: Identificar las amenazas relevantes sobre cada activo.
- Valoración de las amenazas: Estimar la frecuencia de ocurrencia de cada amenaza sobre cada activo.

1.6.2. Norma ISO 22301

La norma ISO 22301:2012 es la primera norma internacional para la gestión de la continuidad de negocio y se ha desarrollado para ayudar a las empresas a minimizar el riesgo del tipo de interrupciones. (ISOTools Excellence, 2015).

La norma ISO 22301:2012 especifica mediante sus cláusulas claves los requisitos necesarios para ejercer la correcta planificación y operación que requiere la empresa para la gestión de la continuidad de negocio.

De entre todas las cláusulas que presenta la norma, se distinguen dos que son de interés para el presente trabajo. En la sexta clausura la norma presenta la planeación, la cual especifica que la organización debe asegurarse que los objetivos están establecidos para funciones relevantes y niveles en la organización.

Dentro de la octava clausura se encuentra la operación, se especifica las actividades que se debe realizar para aplicar correctamente dicha norma dentro de una organización.

Planeamiento operacional y control.

La organización debe planificar, implementar y controlar los procesos necesarios para cumplir con requerimientos e implementar las acciones necesarias, debe asegurar que los cambios planeados son controlados y que cambios no intencionados son revisados y acciones apropiadas tomadas.

Análisis de impacto del negocio y evaluación del riesgo

La organización debe establecer, implementar y mantener un proceso documentado y formal para el análisis del impacto del negocio y evaluación del riesgo, que permita:

- Definir criterios adecuados para los análisis.
- Establecer un contexto adecuado para su desarrollo.
- Definir los resultados esperados.

Estrategia de continuidad del negocio

La empresa debe determinar una estrategia de continuidad de negocio apropiado para:

- La protección de actividades priorizadas.
- La estabilización, reanudando y recuperando actividades priorizadas en las dependencias y apoyar los recursos.
- La mitigación y la gestión de impactos.

Establecer e implementar procedimientos de continuidad de negocio

La empresa debe establecer, implantar y mantener procedimientos de continuidad de negocio para gestionar un incidente y continuar sus actividades en base a los objetivos de recuperación que se identifica en el análisis de impacto de negocio.

La empresa debe documentar todos los procedimientos para asegurar la continuidad de las actividades y la gestión de un incidente perturbador. Los procedimientos deben:

- Establecer un protocolo de comunicaciones internas y externas apropiado.
- Ser específico con respecto a las medidas inmediatas que han de ser tomadas durante la interrupción.
- Responder a las amenazas imprevistas y cambiantes en condiciones internas y externas.
- Se centran en el impacto de los eventos que pueden interrumpir las operaciones.

1.6.3. Modelo PDCA

El modelo PDCA viene de las siglas Planificar, Hacer, Verificar y Actuar, en inglés “Plan, Do, Check, Act”. También es conocido como Ciclo de mejora continua o Círculo de Deming. Esta metodología describe los cuatro pasos esenciales que se deben llevar a cabo de forma sistemática para lograr la mejora continua. (Bernal, 2017). (Véase Ilustración 2).

Ilustración 2: Modelo PDCA (PHVA por sus siglas en español)

Fuente: (Gonzalez, 2018)

En la normativa ISO 22301 se referencia el modelo PDCA para el mejoramiento continuo de los Sistemas de Gestión de Continuidad de Negocio. (Véase Ilustración 3).

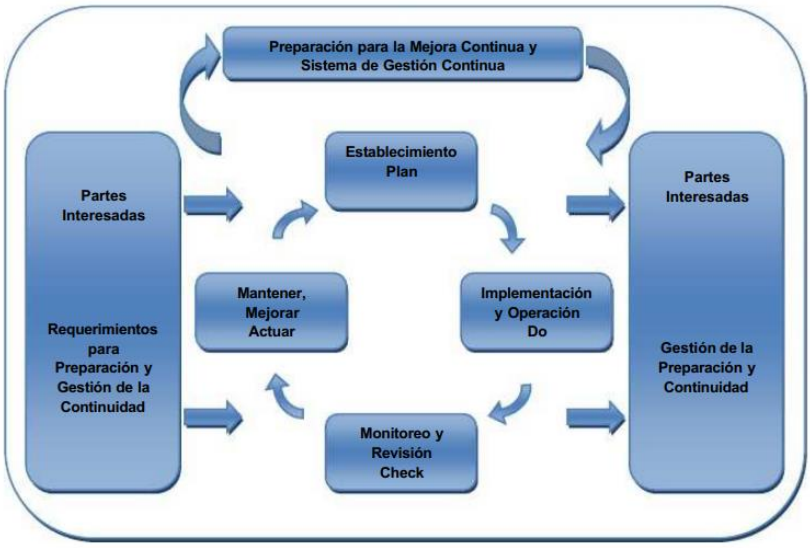


Ilustración 3: Ciclo PDCA Aplicado al Proceso de Continuidad del Negocio

Fuente: ISO 22301:2012

Los objetivos que contemplan los componentes del PDCA se detallan dentro de la ISO:

- Planear: Se identifican los problemas específicos que se pueden enfrentar en la ejecución de un proyecto.
- Hacer: Una vez se ha encontrado la solución a un problema inicia la etapa de implementación en la práctica.
- Verificar: Se miden y evalúan los resultados y se comparan con la expectativa planteada.
- Actuar: Se efectúan acciones de mejora cuando se detectan oportunidades.

1.6.4. Manual para elaborar un plan de continuidad de la gestión en tecnologías de información y comunicación

La dirección de tecnologías de información y comunicación de la CCSS en el año 2007, creo un manual para la elaboración de los planes de continuidad de la gestión en TIC.

Según la (CCSS, 2007), el enfoque que debe mantener un plan de continuidad debe ser la recuperación de las operaciones de los procesos de una organización, dentro de un tiempo determinado y buscando equilibrio entre costo y viabilidad.

Etapas para elaborar un plan de continuidad de TI

El manual CCSS detalla las etapas mínimas que se requieren para elaborar satisfactoriamente un plan de continuidad de TI (Véase ilustración 4).

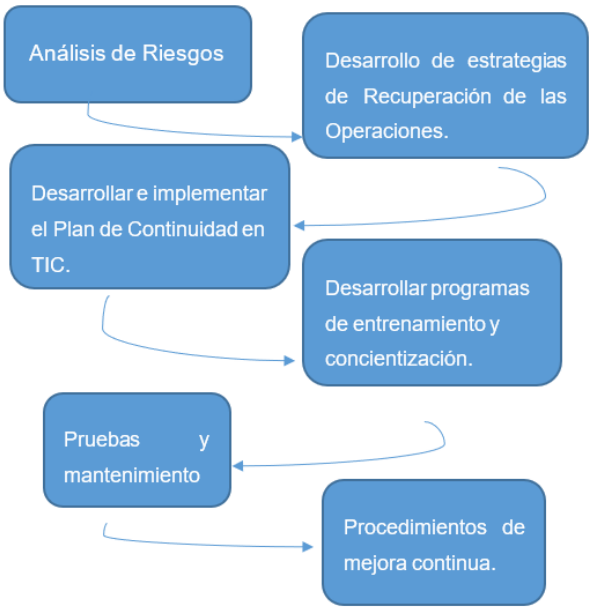


Ilustración 4: Etapas mínimas para elaborar un plan de continuidad de TI

Fuente: Elaboración propia

Análisis de Riesgos

Busca determinar los eventos y situaciones externas que pueden afectar adversamente a la organización y su infraestructura, tanto por una interrupción como por un desastre, evalúa el daño que dichos eventos pueden causar, y los controles requeridos para prevenir o minimizar los efectos de pérdida potencial. (CCSS, 2007)

Esta etapa está orientada a:

- Entender las pérdidas potenciales.
- Determinar la exposición de la Organización a pérdidas potenciales.
- Identificar controles para prevenir o mitigar los efectos de pérdidas potenciales.

- Evaluar, seleccionar y utilizar apropiadamente herramientas y metodologías para análisis de riesgos.
- Evaluar la efectividad de los controles.
- Evaluar y controlar los riesgos.
- Administrar los registros vitales para el negocio.

Desarrollo de Estrategias de Recuperación de las Operaciones

En esta etapa se deberán establecer diversas estrategias orientadas a la recuperación de la plataforma tecnológica de acuerdo con los objetivos de tiempo de recuperación establecidos por el negocio. (CCSS, 2007)

Como parte de la etapa se deberá realizar lo siguiente:

- Identificar los requerimientos estratégicos para la recuperación de la plataforma de TI.
- Valorar la oportunidad de estrategias alternativas contra los resultados del Análisis del Impacto del Negocio.
- Preparar un análisis costo/beneficio de las estrategias de recuperación.
- Seleccionar posibles sitios alternos de operación y respaldo de datos.
- Entender los requerimientos contractuales para los servicios del negocio.

Desarrollar e implementar el Plan de Continuidad

En esta etapa se debe diseñar, desarrollar e implementar el plan de continuidad que proveerá de la información necesaria para recuperar las operaciones de TI dentro del marco de tiempo establecido por el negocio. (CCSS, 2007)

Para lograr este objetivo se deberá:

- Determinar los requerimientos del Plan.
- Determinar la estructura del Plan.
- Diseñar el Plan.
- Definir y documentar los procedimientos de recuperación.
- Desarrollar los requerimientos de documentos a utilizar durante y después del desastre.
- Implementar el Plan.
- Establecer pruebas y procedimientos de control, distribución, capacitación y mejora continua del Plan.

Desarrollar programas de entrenamiento y concientización

En esta etapa, el objetivo principal será desarrollar un programa orientado a crear y mantener conciencia, además de mejorar las habilidades requeridas para desarrollar e implementar los planes de recuperación. (CCSS, 2007)

Para lograr esto deberá:

- Definir los objetivos de entrenamiento y concientización.
- Desarrollar y ejecutar programas variados de entrenamiento.
- Desarrollar programas de concientización.
- Identificar otras oportunidades de educación.

Pruebas y mantenimiento

Esta etapa se orienta a probar con antelación y coordinar ejercicios, documentando y evaluando los resultados de ellos. Desarrollar procesos para mantener vigentes las capacidades para lograr una adecuada recuperación de las operaciones de TI. (CCSS, 2007)

Para el logro de los objetivos se deberá:

- Establecer y ejercitar el plan de continuidad.
- Desarrollar escenarios y realizar para las pruebas.
- Preparar reportes y procedimientos de control.
- Obtener retroalimentación de los resultados obtenidos dentro de las pruebas.

Procedimientos de mejora continua.

La mejora continua del plan de continuidad de TI es un proceso clave, por ello dentro de esta etapa se recomienda considerar los siguientes elementos:

- Administración del cambio dentro de la organización.
- Capacitación del personal.
- Ensayos del plan de continuidad de TI.
- Revisión constante.

CAPITULO II: Metodología

Se especifica el tipo de investigación y la metodología utilizada para el progreso de la investigación.

2.1. Alcance de la investigación

El alcance metodológico abordado es de carácter analítico descriptivo, el cual se ha tomado debido a que se requiere establecer una descripción del problema presentado y el estado actual de la gestión de la continuidad de negocio en los servidores de base de datos.

2.2. Enfoque de la investigación

El enfoque de la investigación abordado es el enfoque cualitativo, debido a que se busca comprender, profundizar y explorar la situación actual de los servidores de bases de datos.

2.3. Diseño de investigación

El diseño de esta investigación está basado en el diseño investigación-acción, debido a que ejerce la toma de decisiones en base a los datos recopilados durante la investigación. (Hernández, 2014)

Los principios que sigue una investigación con un diseño investigación-acción cooperativa son los siguientes:

- Los resultados obtenidos deben generar un impacto positivo.
- Confianza y cooperación entre los involucrados
- Debe existir empoderamiento de los involucrados
- El contexto de la investigación es fundamental.

2.4. Fuente de información

Para lograr lo propuesto en los objetivos de este plan, se emplearon técnicas orientadas a obtener información relevante, estos fueron recolectados a través de las siguientes técnicas:

- Entrevista: Es una forma específica de interacción social que tiene por objeto recolectar datos para una indagación. El investigador formula preguntas a las personas capaces de aportar datos de interés, estableciendo un diálogo peculiar, asimétrico, donde una de las partes busca recoger informaciones y la otra es la fuente de esas informaciones (Rivero, 2008).

- Observación: Método de recopilación de información primaria acerca del objeto estudiado mediante la directa percepción y registro de todos los factores concernientes al objeto estudiado, significativo desde el punto de vista de los objetivos de la investigación (Rivero, 2008).
- Inspección**:** La inspección consiste en examinar registros, documentos, o activos tangibles.

2.5. Procedimiento metodológico

El presente marco metodológico empleado para dar soporte al desarrollo del proyecto está dividido en dos fases: Planear y Hacer. Las cuales se definen dentro de la norma ISO 22301, esto referenciando al modelo PDCA (PHVA en español).

A pesar que PDCA cuenta con cuatro fases, por la naturaleza del presente trabajo y el alcance que se quiere abarcar, solo se contemplan las primeras dos, que pueden ser comprendidas fácilmente mediante la siguiente ilustración.

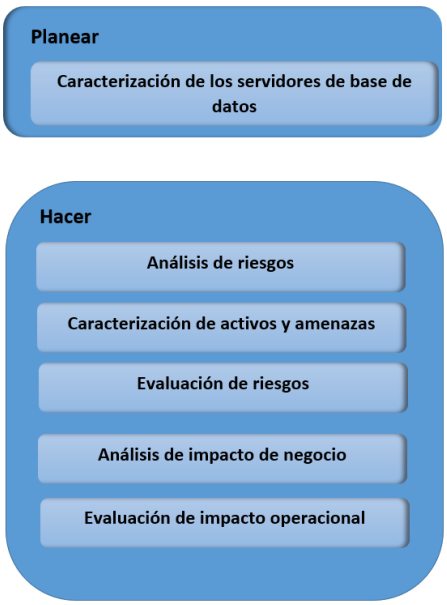


Ilustración 5: Procedimiento metodológico.

Fuente: Elaboración propia

2.5.1. Etapa I: Planear

Para este primer paso, se requiere tener entendimiento de los elementos que conforman los servidores de base de datos para así abordarlos de forma concisa.

La actividad que corresponde a esta etapa se detalla a continuación:

Caracterización de los servidores de base de datos

Para la caracterización, se describe y documentan los elementos que apoyan al correcto funcionamiento de los servidores de base de datos (Activos, elementos de monitoreo, elementos de control, personal autorizado).

2.5.2. Etapa II: Hacer

Teniendo lista la fase de planeación, se procede con la segunda etapa: Hacer. Para ello se consideran las siguientes actividades que permiten desarrollar el plan de continuidad en los servidores de base de datos.

Análisis de riesgo

Para la ejecución correcta de este paso resulta necesario especificar un conjunto de actividades que permitan abordar los riesgos. Dentro del análisis, se ha de caracterizar los activos, las amenazas a los que están expuestos y la valoración respecto a su nivel de probabilidad e impacto.

a. Caracterización de activos.

Parte de la necesidad del buen entendimiento de los elementos que conforman los servidores de base de base de datos, así como de sus relaciones, por ello se desprende tres tareas tal cual se aprecia en la tabla 2.

Tabla 2: Caracterización de los activos

Caracterización	Descripción
Identificación	Clasifica los activos y los engloba por cada tipo.
Dependencias	Presenta la jerarquía existente entre los activos.
Valoración	Dimensiona el valor de los activos, según el perjuicio que genera su carencia.

Fuente: Elaboración propia

b. Caracterización de amenazas.

Esta actividad permite describir las amenazas que pueden afectar a cada activo. Para lograr esto se ejecutan se deben realizar las dos tareas que se presenta en la tabla 3:

Tabla 3: Caracterización de las amenazas

Caracterización	Descripción
Identificación	Identifica las amenazas más relevantes por cada activo.
Valoración	Verifica en que dimensión afectan las amenazas a cada activo.

Fuente: Elaboración propia

Evaluación del riesgo

La evaluación de los riesgos brinda la información necesaria para determinar cuáles riesgos requieren una atención específica dentro del plan de continuidad.

Se evalúa el nivel de probabilidad y el nivel de impacto que alcanzan los riesgos dentro de las operaciones ligadas a los servidores de bases de datos, tomando en consideración la opinión y conocimiento de los colaboradores del área de base de datos.

Con respecto a la evaluación de la probabilidad (Véase Ilustración 42), se considera la clasificación especificada por la (CCSS, 2007) para el análisis del nivel de probabilidad.

En el caso de la evaluación del impacto igualmente se considera la clasificación especificada por la (CCSS, 2007) para el análisis del nivel del impacto (Véase ilustración 43).

Con el objetivo de alcanzar el éxito en esta actividad, se realiza un análisis de cuestionario, donde se analizan los datos recopilados de los colaboradores del área de base en el departamento de informática de la empresa ACME, datos necesarios para determinar el nivel de probabilidad de ocurrencia e impacto.

Además, se desarrolla una matriz de calor para representar la criticidad de los riesgos según la probabilidad de ocurrencia e impacto (Véase ilustración 6) y tomando en consideración rangos de clasificación (Véase ilustración 7).

Probabilidad.	Impacto.				
	10	30	50	70	100
	7	21	35	49	70
	5	15	25	35	50
	3	9	15	21	30
	1	3	5	7	10

Ilustración 6: Matriz de calor

Fuente: CCSS (2007)

Riesgo.	Rango Inferior.	Rango Superior.
Muy alto.	70	100
Alto.	35	69
Medio.	16	34
Bajo.	6	15
Muy Bajo.	1	5

Ilustración 7: Matriz de rango de riesgos

Fuente: CCSS (2007)

Evaluación del impacto del Negocio

Un análisis de impacto en el negocio (BIA) predice las consecuencias de la interrupción de una función y proceso del negocio y recopila la información necesaria para desarrollar estrategias de recuperación. Los posibles escenarios de pérdida deben identificarse durante una evaluación de riesgos. Las operaciones también pueden verse interrumpidas por el fracaso de un proveedor de bienes o servicios o por el retraso en las entregas. Hay muchos escenarios posibles que deben ser considerados.

Identificar y evaluar el impacto de los desastres en las empresas proporciona la base para la inversión en estrategias de recuperación, así como la inversión en estrategias de prevención y mitigación.

El BIA debe identificar los impactos operativos y financieros resultantes de la interrupción de las funciones y procesos comerciales. Los impactos a considerar incluyen:

Tabla 4: Categorías de impacto.

Categorías de riego
Pérdida de ventas e ingresos
Ventas o ingresos retrasados
Aumento de los gastos (por ejemplo, mano de obra extra, subcontratación, agilización de costos, etc.)
Multas reglamentarias
Penalizaciones contractuales o pérdida de bonificaciones contractuales
Insatisfacción o deserción del cliente

Fuente: Elaboración Propia

Tiempo y duración de la interrupción.

El momento en que se interrumpe una función o proceso comercial puede tener una influencia significativa en la pérdida sufrida. Un sistema web con problemas en días esenciales para una empresa puede llegar a perjudicar de una manera muy significativa. Un corte de energía que dure unos minutos sería un inconveniente menor para la mayoría de las empresas, pero uno que dure horas podría resultar en pérdidas comerciales significativas. Una interrupción de la producción de corta duración puede superarse mediante el envío de productos terminados desde un almacén, pero la interrupción de un producto con alta demanda podría tener un impacto significativo.

CAPITULO III: Análisis de resultados

En este capítulo se detalla los resultados obtenidos una vez aplicado el procedimiento metodológico.

3.1. Etapa I: Planear

3.1.1. Caracterización de los servidores de base de datos

Para elaborar el plan de gestión de la continuidad en los servidores de bases de datos del departamento de informática de la empresa ACME, se hizo necesario recopilar información para conocer la situación actual de los sistemas de base de datos, estimulando la implementación y operación de controles que permitan manejar los riesgos de seguridad asociados a las bases de datos de la empresa.

A continuación, se definen cada uno de los aspectos que comprenden esta actividad de control:

Equipos de trabajo

Área de bases de datos y sistemas operativos

El área de base de datos y sistemas operativos se encarga de administrar y monitorear cada uno de los diferentes servidores de bases de datos.

Tabla 5: Roles y responsabilidades del equipo de base de datos.

Nombre	Roles	Responsabilidades
xxxxxxx	**Líder de base de datos y sistemas operativos**	Coordinar y liderar todas las actividades para asegurar el buen funcionamiento de cada uno de los servidores que se encuentran en los centros de datos de la empresa ACME.
xxxxxxx	**Líder inmediato de bases de datos y sistemas operativos**	Coordinar y liderar todas las actividades para asegurar el buen funcionamiento de cada uno de los servidores que se encuentran en los centros de datos de la empresa ACME.
xxxxxxx	**Líder de bases de datos y sistemas operativos**	Velar por el buen funcionamiento de servidores que han sido asignados, realizando una revisión diaria y asistiendo cada operación que se realice en ellos.

Fuente: Elaboración propia

Área de comunicaciones

El área de comunicaciones es la encargada de administrar y monitorear la infraestructura de las redes de comunicaciones tanto del centro de datos principal como la del centro de datos alterno. Además, la comunicación entre las diferentes rentas que existen en el país.

Tabla 6: Roles y responsabilidades del equipo de comunicación

Nombre	Roles	Responsabilidades
Xxxxxxx	**Líder de comunicaciones**	Es la persona responsable coordinar y validar la integridad y disponibilidad de los activos que componen la plataforma de comunicación, estos son: switches, routers, unidades de telefonía, enlaces de datos y cableado de datos.
Xxxxxxx	**Administrador de comunicaciones**	Validar la integridad y disponibilidad de los activos que componen la plataforma de comunicación, estos son: switches, routers, unidades de telefonía, enlaces de datos y cableado de datos.

Fuente: Elaboración propia

Área de Desarrollo

Es la encargada del desarrollo y mejora continua de cada sitio y aplicación de la empresa.

Tabla 7: Roles y responsabilidades del equipo de desarrollo.

Nombre	Roles	Responsabilidades
xxxxxxx	**Líder de desarrollo**	Coordinar y liderar todas las actividades para el desarrollo y funcionamiento de cada sitio web y aplicación de la empresa.
xxxxxxx	**Desarrollador de sistemas**	Desarrollo y mejora de sitios y aplicaciones de la empresa, en coordinación con el Líder de desarrollo.

Fuente: Elaboración propia

Infraestructura tecnológica de la empresa ACME

En cuanto a la infraestructura, es robusta, la plataforma es un ambiente virtual gestionado por aplicaciones VMWare todos los servidores (productivos, desarrollo y control de calidad), facilita la administración y gestión de todas las aplicaciones críticas, con escalabilidad de recursos, a continuación, en la ilustración 8, se detalla en general la parte lógica y ubicación de servidores.

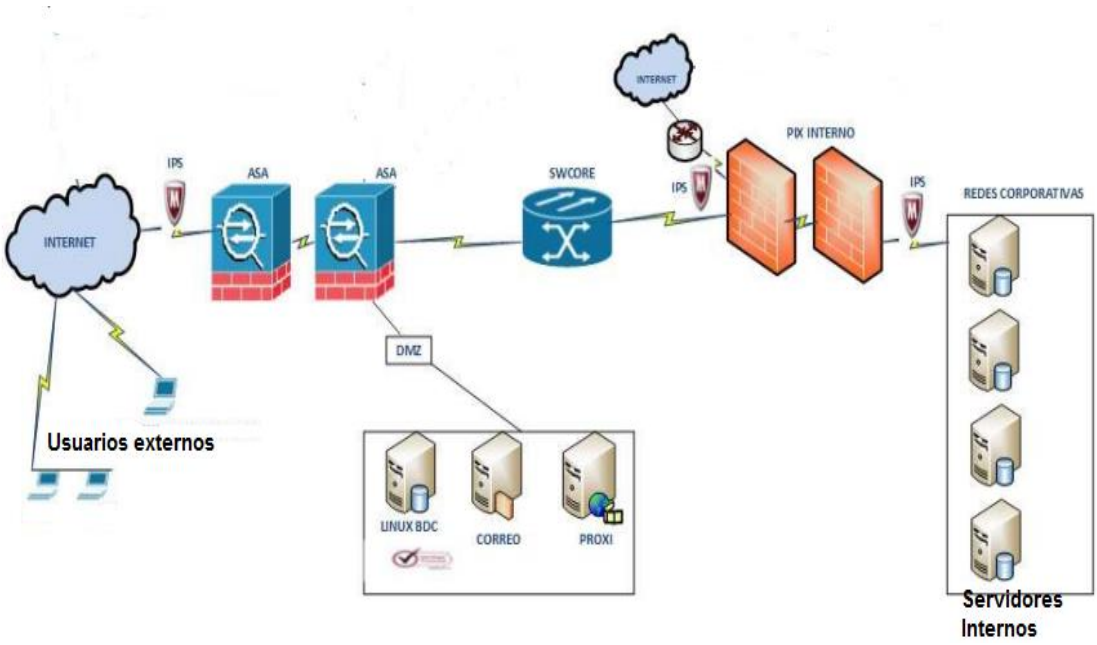


Ilustración 8: Infraestructura tecnológica.

Fuente: Elaboración propia

Distribución de los servidores de bases de datos

Las bases de datos en el departamento de informática están organizadas en dos grupos, bases de datos productivas las cuales están de cara a las transacciones que realizan los usuarios finales y de prueba que se utilizan para el desarrollo y mantenimiento de los sistemas informáticos de la empresa ACME.

La mayoría de los servidores productivos cuentan con un servidor réplica, con el objetivo de no afectar el rendimiento en los sistemas productivos y al mismo tiempo poder consultar los datos casi en tiempo real.

Motores de bases de datos existentes

La empresa ACME ha venido en constante actualización con sus gestores de base de datos, como primera instancia sus bases de datos productivas solo se gestionaban en ADABAS, hoy en día el departamento de informática cuenta con diversos motores de bases de datos, presentados en la tabla 8.

La mayor parte de las bases de datos productivas y de prueba están alojadas en el motor de base de datos MariaDB con sistema operativo SUSE Linux Enterprise Server esto equivale a un 55%, SQL Server con sistemas operativos Windows Server en un 35%, y un 10% en ADABAS.

Tabla 8: Motores de base de datos.

Motor	Versiones instaladas
Microsoft SQL Server	Microsoft SQL Server 2008 R2 (RTM) con sistema operativo Windows server 2008 R2.
	Microsoft SQL Server 2016 (RTM) Enterprise Edition con Sistema operative Windows Server 2012 Standard.
	Microsoft SQL Server 2016 (SP1) Standard Edition (64-bit) con Sistema Operativo Windows Server 2012 R2 Datacenter
MariaDB	MariaDB 10.2.15 con el sistema operativo SUSE Linux Enterprise Server 15
ADABAS	Actualmente solo existe la versión de Adabas 6.3 SP2 con sistema operativo SUSE Linux versión 3.0.101

Fuente: elaboración propia

Firewall

Las configuraciones del firewall se realizan a nivel de servidor, se activan únicamente a servidores productivos y sus réplicas.

Se configura un archivo de acceso con el puerto, protocolo y la dirección IP del terminal que quiere acceder a la base de datos.

Acceso a los servidores

Hay muchos servidores de bases de datos los cuales son distribuidos en varios DBA, estos son encargados de custodiar las claves de sus servidores asignados, no existe una política de caducidad de contraseña, el cambio lo realiza el DBA cuando el jefe de base de datos lo autoriza, el tiempo de cambio se realiza en un periodo de 7 meses.

Acceso a bases de datos

El acceso de usuarios a bases de datos se coordina a través de correo electrónico, cada jefe de oficina revisa el correo y lo aprueba. En muchas ocasiones se conceden permisos temporales para uno o dos días, no se les da seguimiento y esos permisos quedan permanentes.

Monitoreo de TI automático

Dentro del área de base de datos, se gestiona un sistema de monitoreo **Nagios**, el cual ayuda a monitorear el comportamiento de dispositivos de red, servidores, aires de climatización y unidades de precisión, con el objetivo de enviar correos de alertas a los administradores de base de datos y de esta manera verificar de inmediato la causa del problema para darle solución.

Nagios es un sistema de monitorización de redes ampliamente utilizado, de código abierto, que vigila los equipos (hardware) y servicios (software) que se especifiquen, alertando cuando el comportamiento de los mismos no sea el deseado.

Proceso de monitoreo manual

El proceso de monitoreo manual es parte esencial en la administración de los servidores de bases de datos, cada administrador tiene el deber de velar por el buen funcionamiento de sus servidores. A nivel de servidor se revisa el estado de CPU, Memoria, Lectura y escritura en disco y el estado de particiones principales donde se alojan las bases de datos.

Conexión con centro de datos alterno

Actualmente la empresa ACME cuenta con un centro de datos principal ubicado en el departamento de informática y un centro de datos alterno ubicado en las afueras de Managua. Ambos están interconectados de tal forma que si surge un problema en el centro de datos principal los servidores de base de datos productivos se pueden migrar al centro de datos alterno.

Cabe señalar que el proceso de migración de servidores de bases de datos no es automático, este proceso es realizado manualmente por el jefe del área de bases de datos. Aún sigue siendo un problema ya que no existe un sistema de conmutación por error que garantice la migración automática de los servicios al centro de datos alterno y de esta manera disminuir el tiempo de inactividad.

El enlace de datos que existe entre los dos centros de datos es de 5G, esta pasa por un canal de fibra óptica.

Actualmente la estructura de red que conecta al centro de datos principal con el centro de datos alterno está diseñada de la siguiente manera.

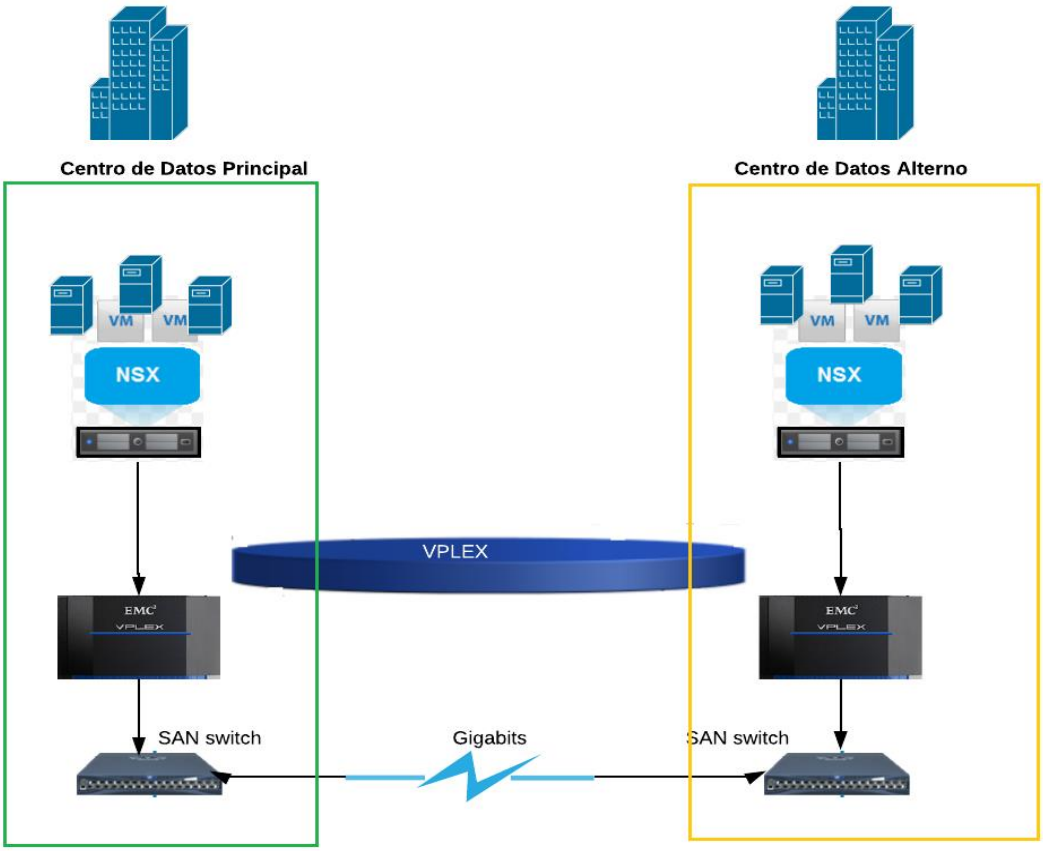


Ilustración 9: Conexión entre los centros de datos

Fuente: elaboración propia

Proceso de respaldo o copias de seguridad

Los respaldos están programados para que se generen automáticos, se realizan diario por las noches y se transfieren por FTP automáticamente al servidor de respaldos.

Actualmente los respaldos son trasladados a discos y estos son llevados a resguardo a un sitio externo de la empresa ACME.

A continuación, se detallan los pasos para el proceso de respaldo que se realizan en la empresa.

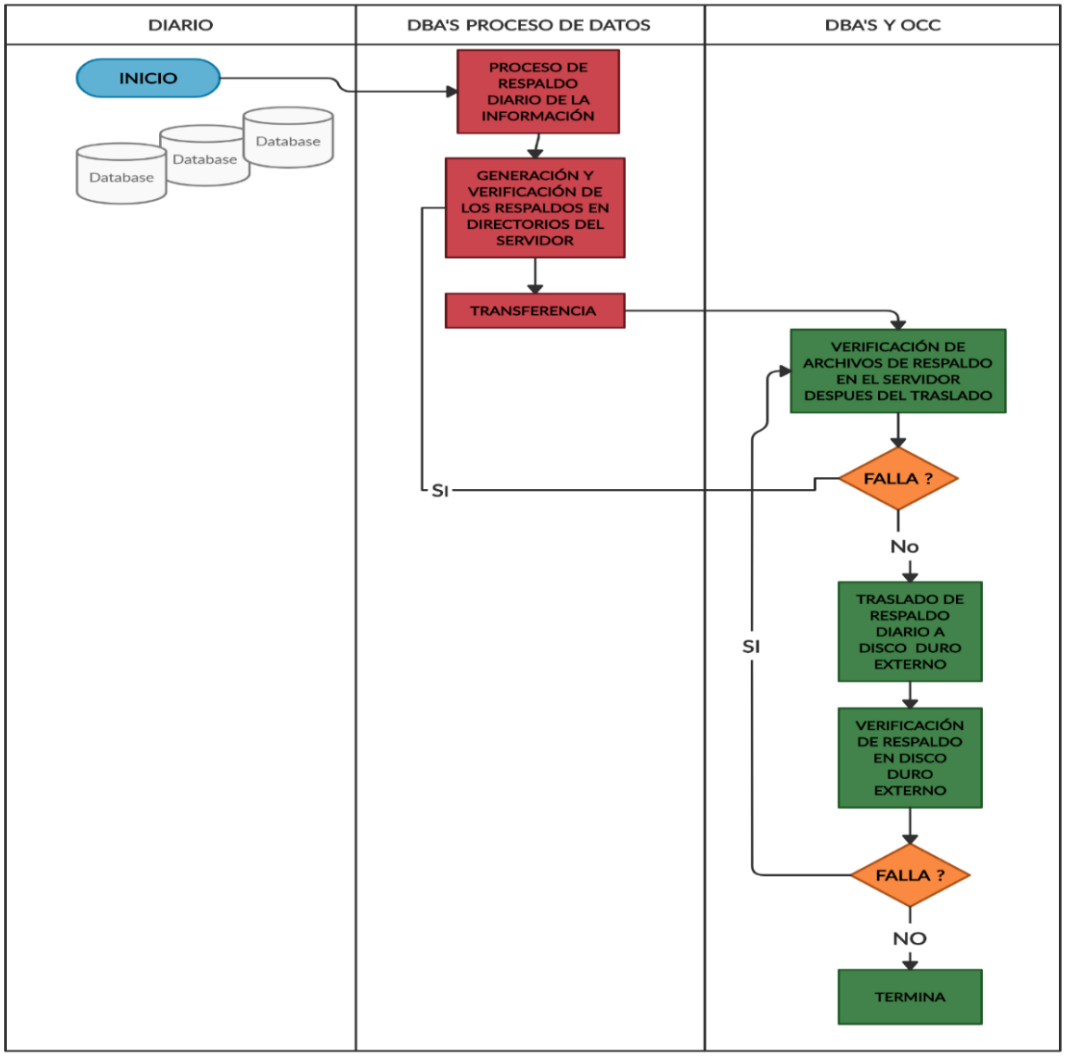


Ilustración 10: Diagrama proceso de respaldo.

Fuente: Elaboración propia

Suministro eléctrico

Todo componente eléctrico y un servidor no podía ser menos, necesita un suministro constante de electricidad para funcionar. Fallos en este suministro, aunque sean por periodos muy cortos de tiempo tendrá consecuencias catastróficas para los sistemas informáticos de la empresa.

El departamento de informática cuenta con una alternativa de respaldo eléctrico el cual está estructurado de la siguiente manera:

- UPS: Son baterías especiales que se conectan entre los servidores y el generador eléctrico. Garantizan un suministro constante y estable por un tiempo, dependiendo este de la capacidad de las mismas. En este caso en el departamento de informática de la Empresa ACME el tiempo que suministra estas tecnologías cuando la red eléctrica falla es aproximadamente de 20 minutos.
- Generadores eléctricos: Funcionan generalmente con diésel y se conectan entre los UPS y la red de suministro eléctrico (comercial). Solo entran en funcionamiento cuando el suministro se corta por más de un determinado tiempo. Pueden suministrar electricidad por un tiempo indefinido siempre que tengan carburante en el tanque.
- Líneas de suministros: En centros de datos grandes, se suelen tener al menos 2 conexiones diferentes e independientes a la red de suministro eléctrico. En este caso la empresa ACME cuenta con una sola línea.

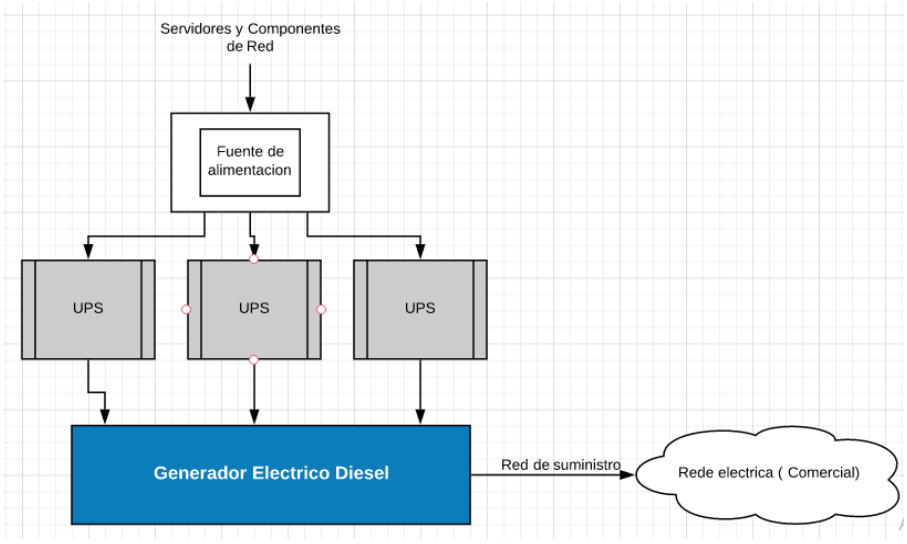


Ilustración 11: Conectividad en el suministro eléctrico.

Fuente: Elaboración propia

Replicación de bases de datos

La empresa ACME cuenta con muchos sistemas en línea y locales, además existen diversas bases de datos que son utilizadas por estos.

El departamento de informática en común acuerdo con la dirección superior de la empresa está impulsando un proyecto para migrar la mayoría de las bases de datos alojas en ADABAS a los sistemas de gestión de base de datos MariaDB y Microsoft SQL Server, con el fin de adoptar tecnología actualizada y gestionar la información de una mejor manera.

La mayoría de las bases de datos productivas poseen una base de datos de réplica la cual es utilizada por los desarrolladores para realizar las pruebas necesarias.

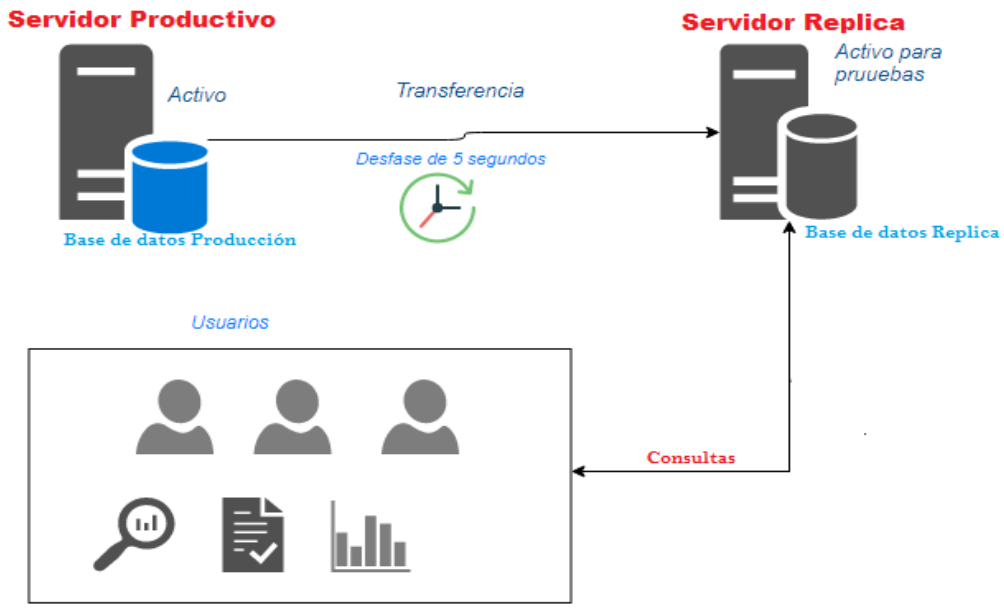


Ilustración 12: Replicación de bases de datos productivas

Fuente: elaboración propia

Todas las bases de datos de la empresa son de suma importancia. Pero existen dos bases de datos que es el pilar de la empresa, a esta base y es indispensable que esté funcionando las 24 horas del día y los 7 días de la semana, ya que es donde más movimientos transaccionales se generan.

La base de datos ACMEPROD tiene una base de datos replica. Esta alternativa no es una solución de Alta disponibilidad si ocurre una falla en el servidor principal, es únicamente para realizar consultas de pruebas y de esta forma no afectar el rendimiento del servidor productivo.

3.2. Etapa II: Hacer

3.2.1. Fase de Análisis de Riesgos o Diagnóstico

Para el desarrollo de esta actividad se emplea la metodología de análisis y evaluación de riesgos MARGERIT, que permite alcanzar los resultados esperados dentro de cada actividad.

Posteriormente, se emplea un cuestionario a los miembros del departamento de informática de la empresa ACME específicamente al Área de base de datos y sistemas operativos ya que son los que están de cara a la administración de los servidores de base de datos.

3.2.1.1. Caracterización de activos

Esta actividad consta de tres subtareas:

- Identificación de los activos de los servidores de bases de datos.
- Dependencia entre los activos.
- Valoración de los activos.

Identificación de los activos

Esta primera subtarea es de suma importancia debido a que la identificación de activos es la base que permite realizar las siguientes subtareas.

Tabla 9: Identificación de los activos de la base de datos.

Tipo del activo	Nombre del activo	Descripción
Datos	[backup] Copias de seguridad de base de datos	Copia de seguridad de estructura y datos.
	[conf] Copias de seguridad de datos de configuración	Copia de seguridad de archivos de configuración del sistema.
	[acl] Datos de control de acceso	Datos de control de acceso a las diferentes bases de datos.
	[log] Registro de actividad	Es el archivo de registro donde se guardan todos los eventos tanto del sistema como de las bases de datos.
Claves criptográficas	[disk] Cifrado de soportes de información	Permite hacer el cifrado del disco donde se guardan las copias de seguridad.
	[server] Cifrado de copias de seguridad	Permite hacer el cifrado de la copia de seguridad.
Aplicaciones informáticas (Software)	[sbms] Sistema de gestión de bases de datos	Es un conjunto de programas que nos permiten gestionar bases de datos.
	[os] sistema operativo	Es un conjunto de programas de un sistema informático, que administra los recursos físicos.
	[hypervisor] Gestor de máquinas virtuales	Aplicación capaz de permitir que varios sistemas operativos convivan de manera simultánea
	[backup] Sistema de backup	Sistema que permite guardar datos en un soporte de almacenamiento adecuado
	[av] Antivirus	software que se utiliza para evitar, buscar, detectar y eliminar virus de una computadora.
	[fw] Firewall	Software que nos permite gestionar y filtrar la totalidad de tráfico entrante.
Equipamiento informático (hardware)	[sbd] Servidores de Base de datos	Servidores físicos de base de datos
	[backup] Equipamiento de respaldo	Disco duro que almacena la información de respaldo de las bases de datos
	[switch] Conmutadores	Dispositivo de comunicación
	[routers] Encaminadores	Dispositivo de comunicación
	[firewall] Cortafuegos	Hardware que nos permite gestionar y filtrar la totalidad de tráfico entrante

Tipo del activo	Nombre del activo	Descripción
Redes de comunicaciones	[LAN] Red local	Red de computadoras que abarca un área específica
	[MAN] Red metropolitana	Red de computadoras que abarca toda el área de la empresa.
Soportes de información	[disk] Discos	Discos duros externos que almacenan información.
	[san] Almacenamiento en red	Almacenamiento en red compartida.
Equipamiento auxiliar	[ups] Sistema de alimentación ininterrumpida	Dispositivo de baterías encargado de almacenar energía.
	[gen] Generadores de energía	Permiten generar electricidad como sustituto de la electricidad de la red eléctrica.
	[ac] Equipos de climatización	Equipo que gestiona de forma integral la temperatura.
	[safe] Caja fuerte	Caja de seguridad que guarda elementos de suma importancia.
Instalaciones	[dcp] Centro de datos principal	Centro de procesamiento de la información.
	[dca] Centro de datos alterno	Centro de procesamiento de la información secundario.
Personal	Líder de apoyo tecnológico	Personal de máxima autoridad en área de base de datos.
	Líder inmediato de Base de Datos y S. O.	Personal de área de base de datos.
	Administradores de Base de Datos y S. O.	Personal de área de base de datos.
	Jefe de comunicaciones	Personal de área de base de datos.
	Personal de monitoreo	Personal de área de base de datos.

Fuente: Elaboración propia.

Dependencia entre los activos

El siguiente diagrama representa la dependencia existente entre los activos para la fácil comprensión de que activo de orden superior es perjudicado por la interrupción de un activo de orden inferior.

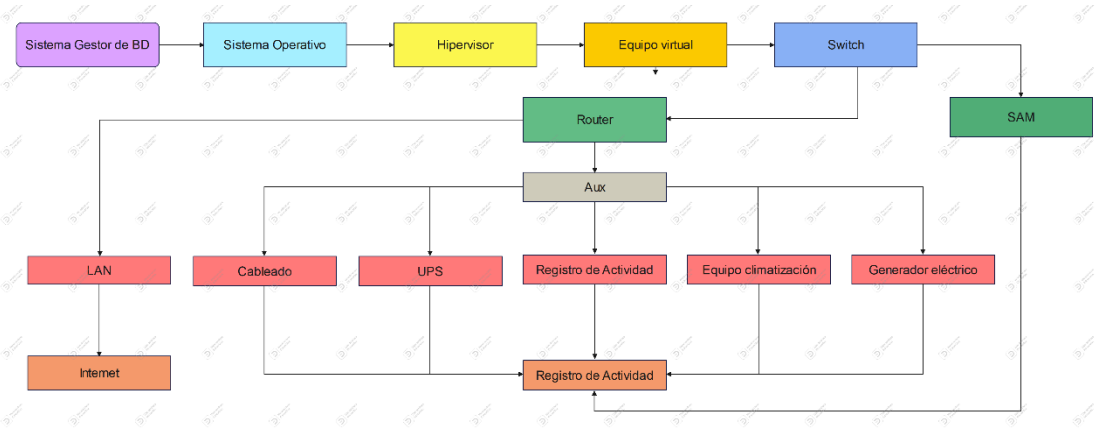


Ilustración 13: Dependencia de los activos.

Fuente: Elaboración propia.

Se estableció estas dependencias de activos mediante entrevista realizada al personal del área del área de base de datos.

El sistema de gestión de base de datos al ser indispensable para el correcto funcionamiento de las operaciones, se estableció su posición en la parte superior del diagrama.

Un nivel por debajo se encuentra el Sistema Operativo que es donde se encuentra el sistema gestor de base de datos, en la misma capa se encuentra el antivirus.

El equipo virtual está a un nivel por debajo debido a que es en este que se almacena el hipervisor y las máquinas virtuales. En los activos inferiores se ubica el router y switches.

Por debajo de todo el diagrama se tienen los equipos auxiliares.

Valoración de los activos

Para el análisis de riesgos se utilizará un dimensionamiento para valorar las consecuencias de la materialización de una amenaza. La Valoración que recibe un proceso en una cierta dimensión es la medida del perjuicio para la organización si el proceso se ve perjudicado en dicha dimensión.

- Disponibilidad [D]: Propiedad o característica de los activos consistentes en que los usuarios o procesos autorizados tienen acceso a los mismos cuando lo requieren.
- Integridad [I]: Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.
- Confidencialidad [C]: Propiedad o característica consistente en que la información no se pone a disposición, ni se revela a usuarios o procesos no autorizados.

Tabla 10: Valoración de los activos.

Tipo del activo	Activos	Valoración			Valoración total
		D	I	C	
Datos	[backup] Copias de seguridad de base de datos	8	5	7	20
	[conf] Copias de seguridad de datos de configuración	0	5	0	5
	[acl] Datos de control de acceso	10	8	10	28
	[log] Registro de actividad	8	5	0	13
Claves criptográficas	[disk] Cifrado de soportes de información	0	0	10	10
	[server] Cifrado de copias de seguridad	0	0	10	10
Aplicaciones informáticas (Software)	[sbms] Sistema de gestión de bases de datos	10	8	0	18
	[os] sistema operativo	10	0	5	15
	[hypervisor] Gestor de máquinas virtuales	10	0	5	15
	[backup] Sistema de backup	8	8	10	26
	[av] Antivirus	5	5	10	20
	[fw] Firewall	0	0	10	10

Tipo del activo	Activos	Valoración			Valoración total
		D	I	C	
Equipamiento informático (hardware)	[sbd] Servidores de Base de datos	10	0	0	10
	[backup] Equipamiento de respaldo	8	8	5	21
	[switch] Conmutadores	8	8	0	16
	[routers] Encaminadores	8	8	0	16
	[firewall] Cortafuegos	8	8	0	16
Redes de comunicaciones	[LAN] Red local	10	5	10	25
	[MAN] Red metropolitana	10	5	10	25
Soportes de información	[disk] Discos	8	8	8	24
	[san] Almacenamiento en red	8	8	8	24
Equipamiento auxiliar	[ups] Sistema de alimentación ininterrumpida	10	8	0	18
	[gen] Generadores de energía	10	8	0	18
	[ac] Equipos de climatización	10	8	0	18
	[safe] Caja fuerte	10	10	0	20
Instalaciones	[dcp] Centro de datos principal	10	10	10	30
	[dca] Centro de datos alterno	9	8	10	27
Personal	Jefe de apoyo tecnológico	8	5	0	13
	Jefe inmediato de Base de Datos y S. O.	8	5	0	13
	Administrador de Base de Datos y S. O.	8	5	0	13
	Jefe de comunicaciones	8	5	0	13
	Personal de monitoreo	8	5	0	13

Fuente: Elaboración propia

3.2.1.2. Caracterización de las amenazas

Según Magerit, las amenazas están clasificadas en cuatro grupos.

- [N] Desastres Naturales.
- [I] De origen Industrial.
- [E] Errores y fallos no intencionados.
- [A] Ataque intencionado.

Esta actividad consta de una subtarea:

Identificación de las amenazas

El objetivo de esta tarea consiste en identificar las amenazas más relevantes sobre cada activo (Ver tabla 11).

Tabla 11: Identificación de las amenazas.

Tipo de activo	Activos	Amenazas
Datos	[backup] Copias de seguridad de base de datos	[E.2] Errores de administrador [E.18] Destrucción de la información [A.11] Acceso no autorizado
	[conf] Copias de seguridad de datos de configuración	[E.2] Errores de administrador [E.18] Destrucción de la información [A.11] Acceso no autorizado
	[acl] Datos de control de acceso	[A.5] Abuso de privilegio de acceso
	[log] Registro de actividad	[A.15] Modificación deliberada de la información [E.2] Errores de administrador [A.11] Acceso no autorizado
Claves criptográficas	[disk] Cifrado de soportes de información	[E.2] Errores de administrador
	[server] Cifrado de copias de seguridad	[E.2] Errores de administrador
Aplicaciones informáticas (Software)	[sbms] Sistema de gestión de bases de datos	[I.5] Averías de origen lógico [E20] Vulnerabilidad de los programas [E.21] Errores de mantenimiento / actualización de programas (Software)
	[os] sistema operativo	[I.5] Averías de origen lógico [E.2] Errores de administrador [E20] Vulnerabilidad de los programas [E.21] Errores de mantenimiento / actualización de programas (Software) [A.6] Abuso de privilegio de acceso
	[hypervisor] Gestor de máquinas virtuales	[I.5] Averías de origen lógico [E.2] Errores de administrador

Tipo de activo	Activos	Amenazas
Aplicaciones informáticas (Software)	[hypervisor] Gestor de máquinas virtuales	[E20] Vulnerabilidad de los programas [E.21] Errores de mantenimiento / actualización de programas (Software) [A.6] Abuso de privilegio de acceso
	[backup] Sistema de backup	[I.5] Averías de origen lógico [E.2] Errores de administrador [E.21] Errores de mantenimiento / actualización de programas (Software) [A.6] Abuso de privilegio de acceso
	[av] Antivirus	[E.8] Difusión de software dañino [E20] Vulnerabilidad de los programas [E.21] Errores de mantenimiento / actualización de programas (Software)
	[fw] Firewall	[E.2] Errores de administrador [E20] Vulnerabilidad de los programas [E.21] Errores de mantenimiento / actualización de programas (Software)
Equipamiento informático (hardware)	[sbd] Servidores de Base de datos	[N.1] Fuego [N.2] Daños por agua [I.5] Avería de origen físico [I.6] Corte de suministro eléctrico [E.23] Errores de mantenimiento / actualización de equipos hardware [E.24] Caída de sistemas por agotamiento de recursos
	[backup] Equipamiento de respaldo	[N.1] Fuego [N.2] Daños por agua [I.5] Avería de origen físico [I.6] Corte de suministro eléctrico [E.23] Errores de mantenimiento / actualización de equipos hardware

Tipo de activo	Activos	Amenazas
Equipamiento informático (hardware)	[switch] Conmutadores	[N.1] Fuego [N.2] Daños por agua [I.5] Avería de origen físico [I.6] Corte de suministro eléctrico [E.23] Errores de mantenimiento / actualización de equipos hardware
	[routers] Encaminadores	[N.1] Fuego [N.2] Daños por agua [I.5] Avería de origen físico [I.6] Corte de suministro eléctrico [E.23] Errores de mantenimiento / actualización de equipos hardware
	[firewall] Cortafuegos	[N.1] Fuego [N.2] Daños por agua [I.5] Avería de origen físico [I.6] Corte de suministro eléctrico [E.23] Errores de mantenimiento / actualización de equipos hardware
Soportes de información	[disk] Discos	[N.1] Fuego [N.2] Daños por agua [I.5] Avería de origen físico lógico [E.18] Destrucción de información [E.19] Fuga de información [E.25] Pérdida de discos [A.25] Robo
	[san] Almacenamiento en red	[N.1] Fuego [N.2] Daños por agua [I.5] Avería de origen físico lógico

Tipo de activo	Activos	Amenazas
Equipamiento auxiliar	[ups] Sistema de alimentación ininterrumpida	[N.1] Fuego [N.2] Daños por agua [I.5] Avería de origen físico [I.7] Condiciones inadecuadas de temperatura o humedad
	[gen] Generadores de energía	[N.1] Fuego [N.2] Daños por agua [I.5] Avería de origen físico [I.7] Condiciones inadecuadas de temperatura o humedad
	[ac] Equipos de climatización	[N.1] Fuego [N.2] Daños por agua [I.5] Avería de origen físico [I.7] Condiciones inadecuadas de temperatura o humedad
	[safe] Caja fuerte	[I.5] Avería de origen físico
Instalaciones	[dcp] Centro de datos principal	[N.1] Fuego [N.2] Daños por agua [I.*] Desastres industriales [A.11] Acceso no autorizado
	[dca] Centro de datos alterno	[N.1] Fuego [N.2] Daños por agua [I.*] Desastres industriales [A.11] Acceso no autorizado

Tipo de activo	Activos	Amenazas
Personal	Jefe de apoyo tecnológico	[E.7] Deficiencias en la organización [E.28] Indisponibilidad del personal
	Jefe inmediato de Base de Datos y Sistemas Operativos	[E.28] Indisponibilidad del personal [A.29] Extorsión
	Administradores de Base de Datos y Sistemas Operativos	[E.28] Indisponibilidad del personal [A.29] Extorsión
	Jefe de comunicaciones	[E.28] Indisponibilidad del personal [A.29] Extorsión
	Personal de monitoreo	[E.28] Indisponibilidad del personal

Fuente: Elaboración propia.

3.2.1.3. Evaluación de riesgos

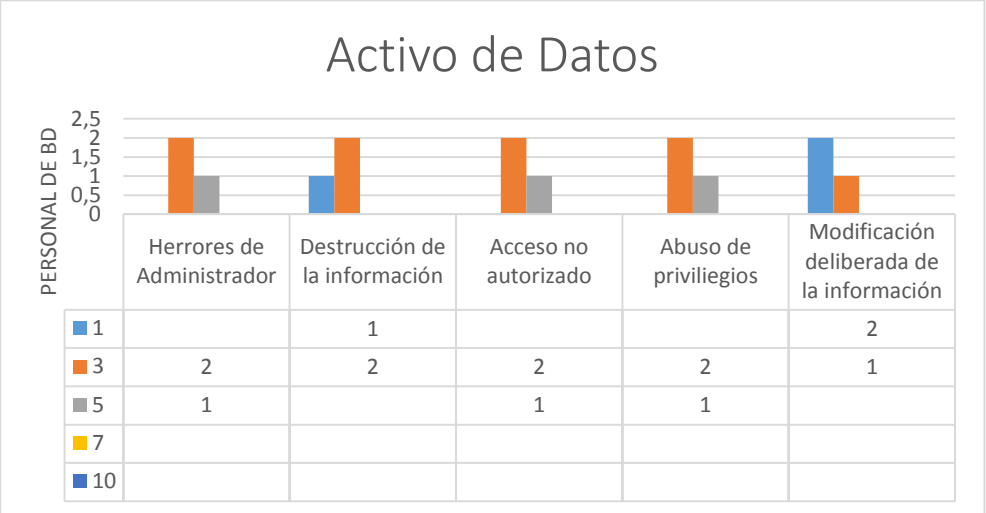
La evaluación de riesgos relacionados con los servidores de base de datos se realiza a través de un cuestionario elaborado en Google Forms y enviado a 3 miembros del área de base de datos y sistemas operativos. Quienes basándose en su experiencia de los años que llevan trabajando en esa área, brindaron una valoración objetiva.

En el cuestionario se evalúa el nivel de probabilidad de ocurrencia y el nivel de impacto que alcanza cada una de las amenazas que fueron identificadas con la implementación de la guía Magerit, tomando como referencia una escala (Véase ilustración 47 e ilustración 48) que facilita realizar el cálculo de nivel de riesgo.

En el cuestionario enviado a los 3 miembros y contestado por los tres, se puede apreciar (véase ilustración 49 e ilustración 50), donde se brindada cada una de la clasificación de activos y las amenazas asociadas a cada activo.

Con respecto al nivel de probabilidad de ocurrencia, según las valoraciones realizadas por el personal del área de base de datos y sistemas operativos obtenidos por categoría de activo y sus amenazas, se muestra en los gráficos siguientes.

Grafico 1: Niveles de Probabilidad de ocurrencia, para activos de Datos

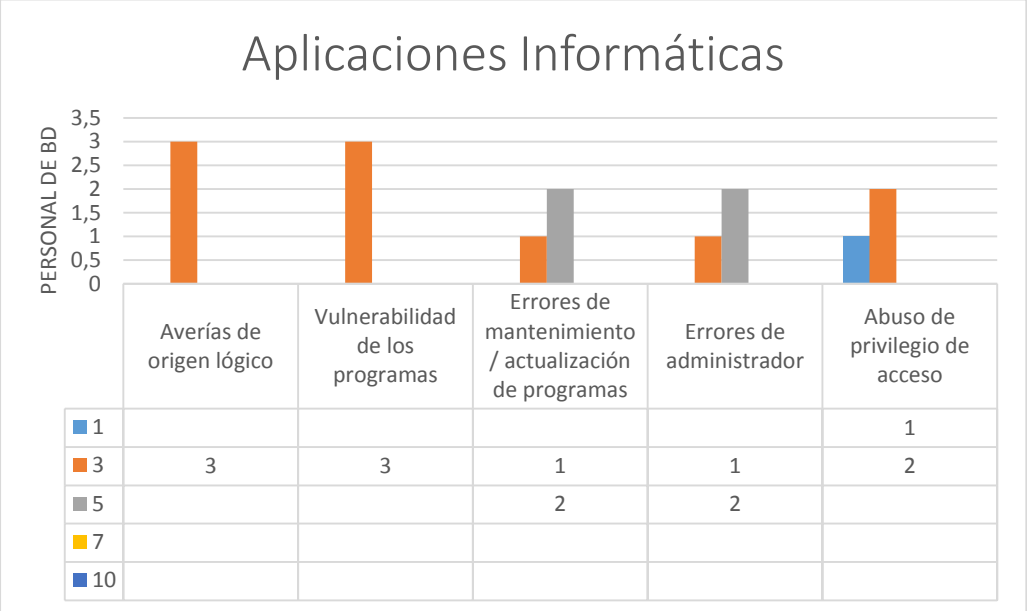


Fuente: Elaboración propia

Grafico 2: Niveles de Probabilidad de ocurrencia, activo Clave Criptográficas

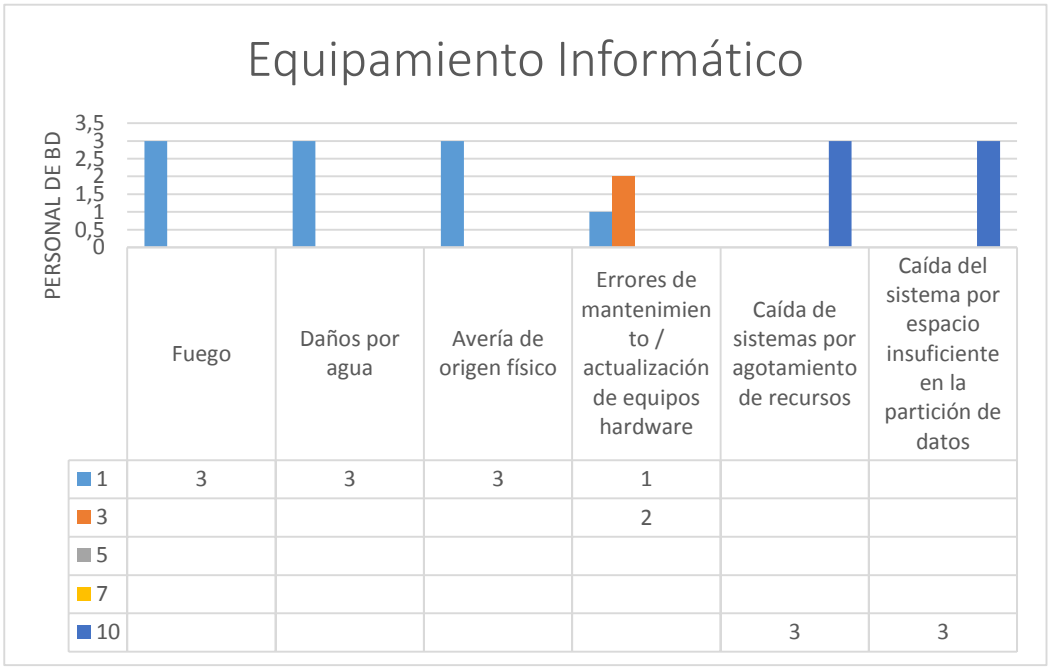
Fuente: Elaboración propia

Grafico 3: Niveles de Probabilidad de ocurrencia, para activos de Software



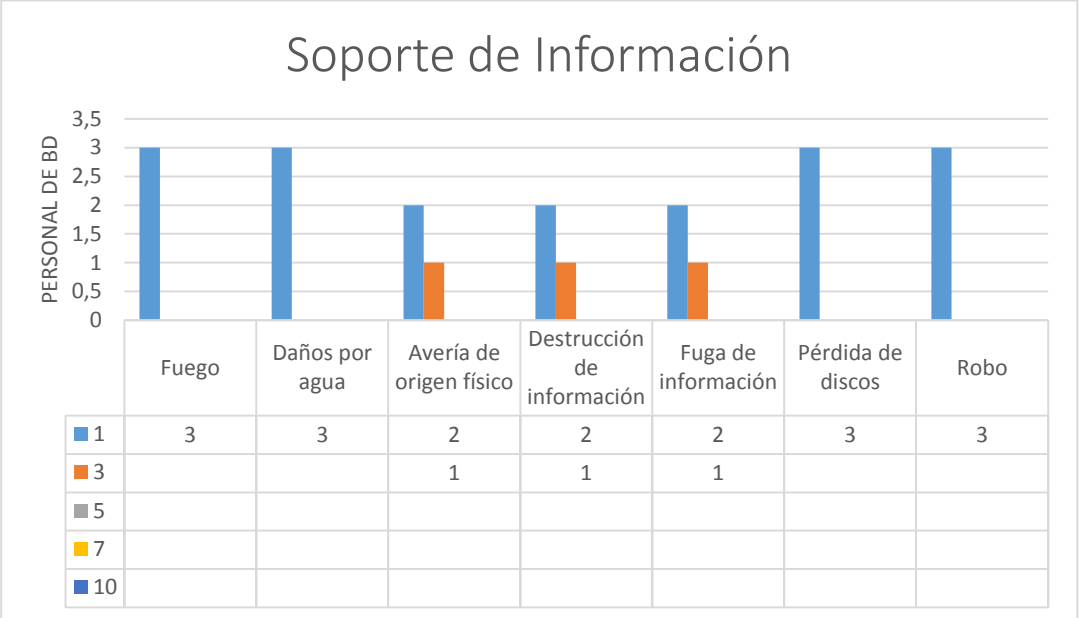
Fuente: Elaboración propia

Grafico 4: Niveles de Probabilidad de ocurrencia, para activos Hardware



Fuente: Elaboración Propia

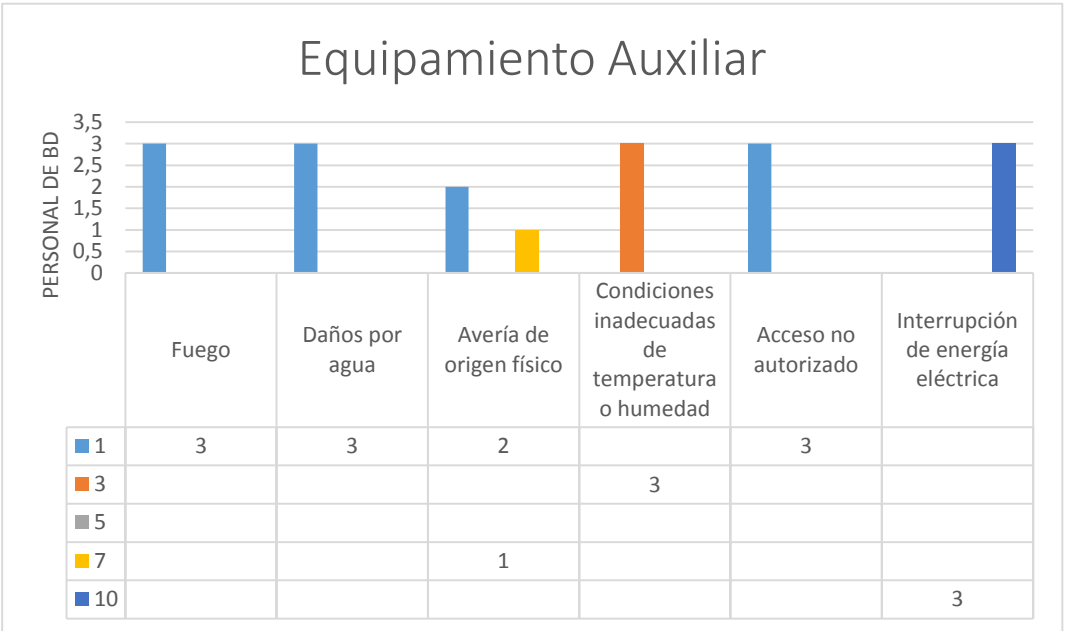
Grafico 5: Niveles de Probabilidad de ocurrencia, activos soporte de Información



	Fuego	Daños por agua	Avería de origen físico	Destrucción de información	Fuga de información	Pérdida de discos	Robo
1	3	3	2	2	2	3	3
3			1	1	1		
5							
7							
10							

Fuente: Elaboración Propia

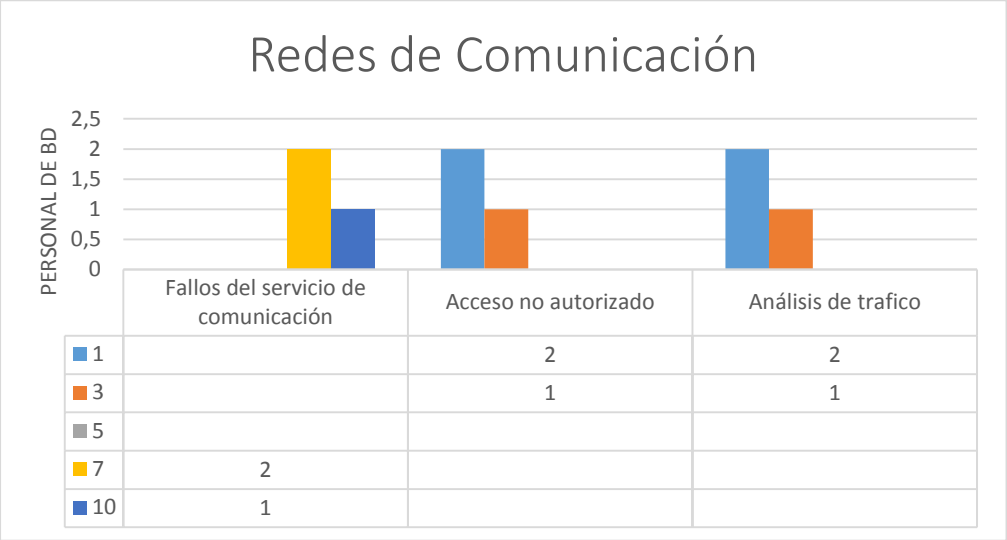
Grafico 6: Niveles de Probabilidad de ocurrencia, activo Equipamiento Auxiliar



	Fuego	Daños por agua	Avería de origen físico	Condiciones inadecuadas de temperatura o humedad	Acceso no autorizado	Interrupción de energía eléctrica
1	3	3	2		3	
3				3		
5						
7			1			
10						3

Fuente: Elaboración Propia

Grafico 7: Niveles de Probabilidad de ocurrencia, activo Redes de Comunicación

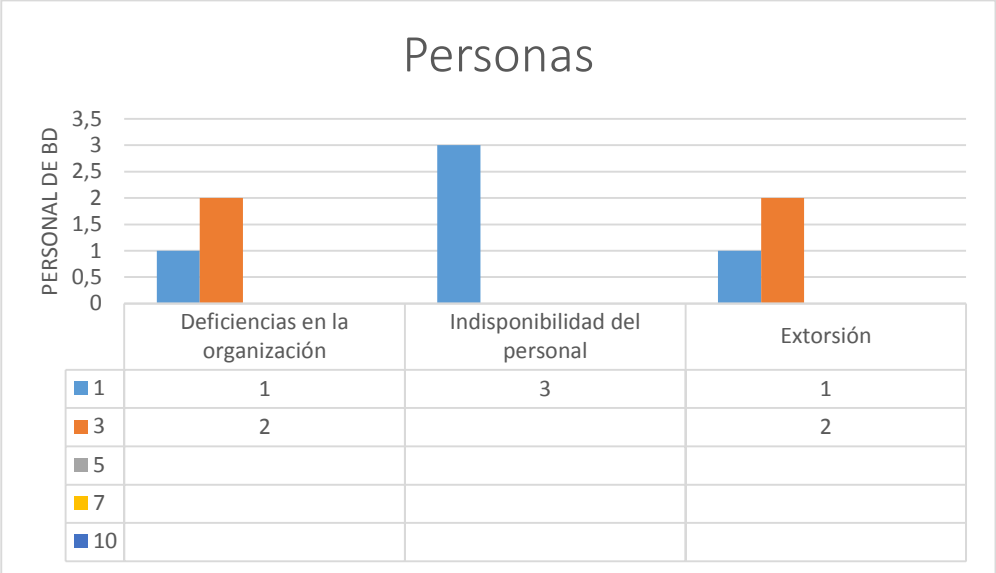


Fuente: Elaboración Propia

Grafico 8: Niveles de Probabilidad de ocurrencia, para activo Instalaciones

Fuente: Elaboración Propia

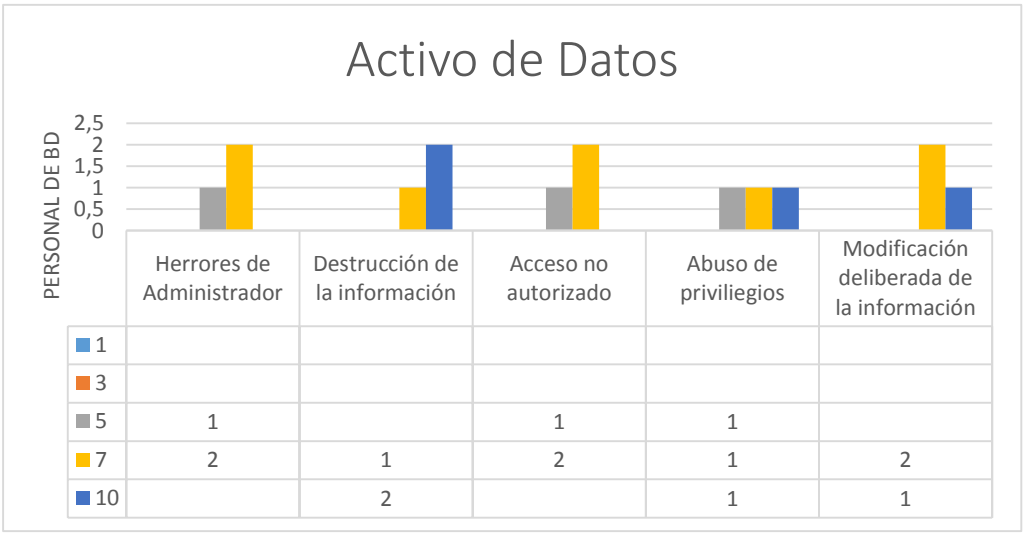
Grafico 9: Niveles de Probabilidad de ocurrencia, para activos de Personas



Fuente: Elaboración Propia

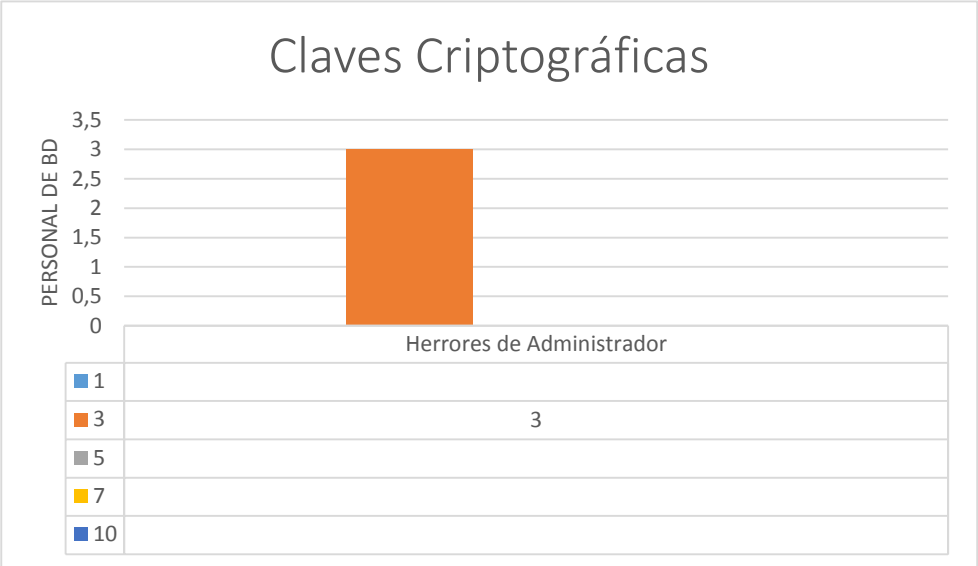
En el caso del nivel de impacto, considerando los resultados emitidos por el personal del área de base de datos y sistemas operativos, se promedian los valores obtenidos por categoría de activo y sus amenazas, se muestran en los gráficos siguientes.

Grafico 10: Niveles de Impacto, activo de datos



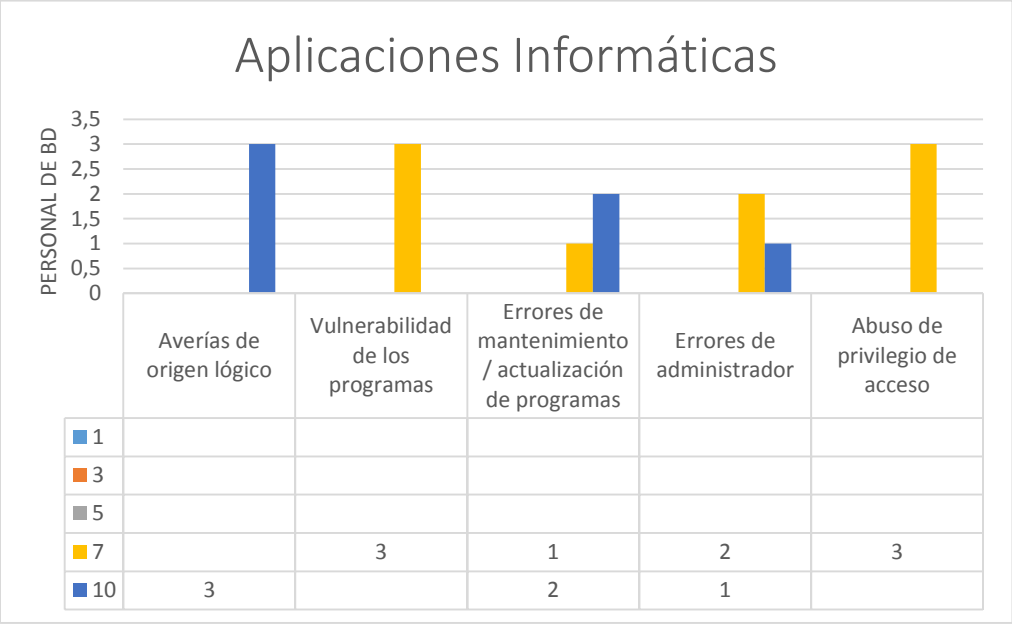
Fuente: Elaboración Propia

Grafico 11: Niveles de Impacto, activo de claves criptográficas



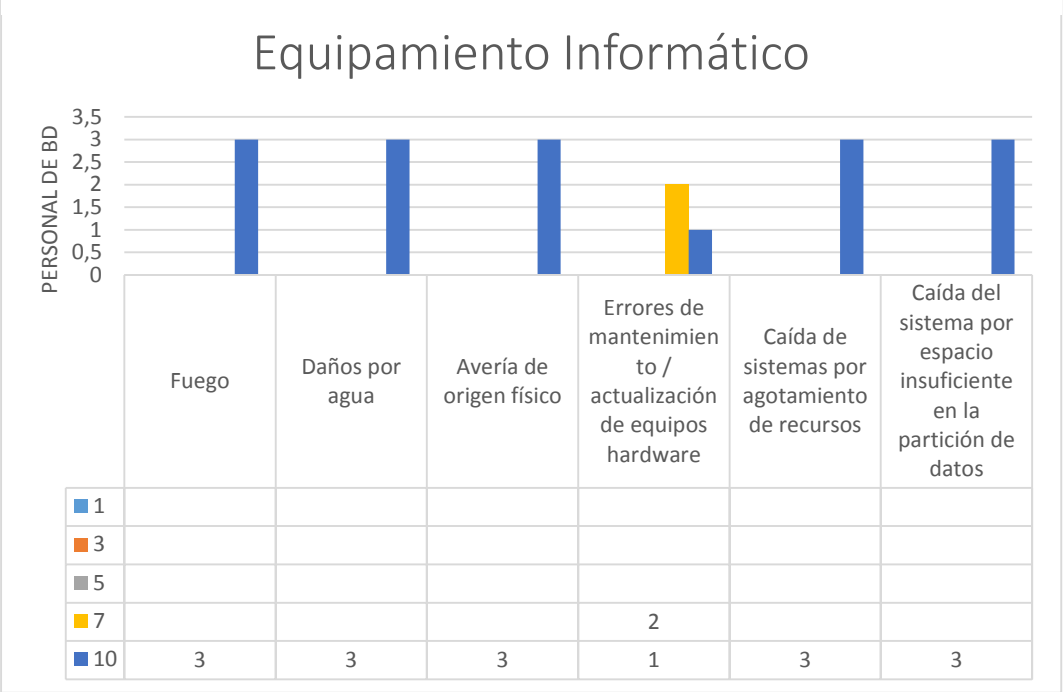
Fuente: Elaboración Propia

Grafico 12: Niveles de Impacto, activo de Software



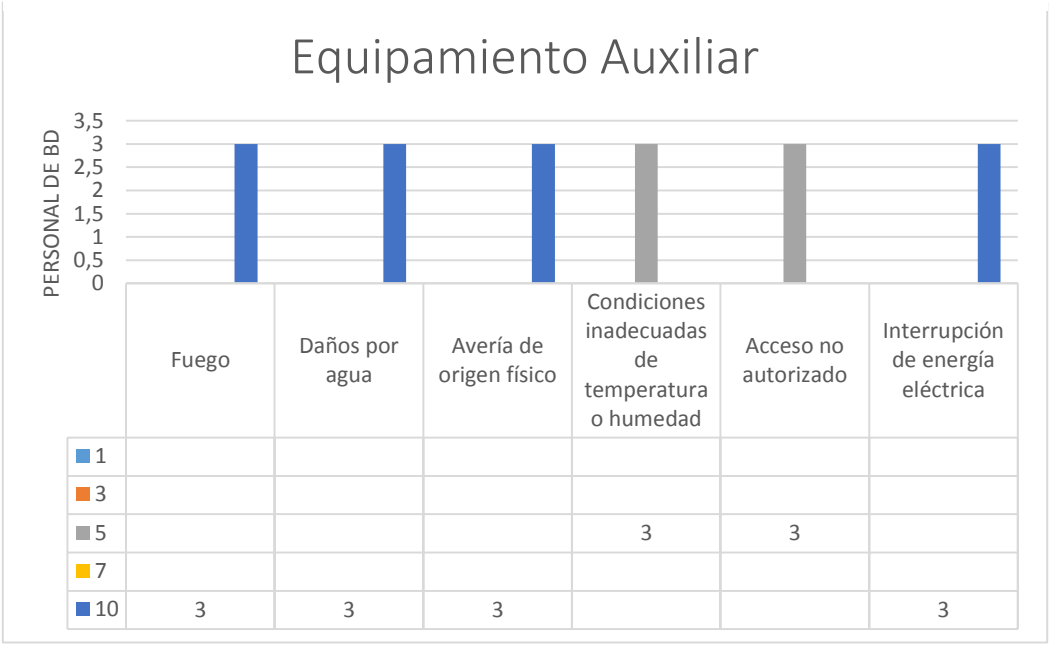
Fuente: Elaboración Propia

Grafico 13: Niveles de Impacto, activo de Hardware:



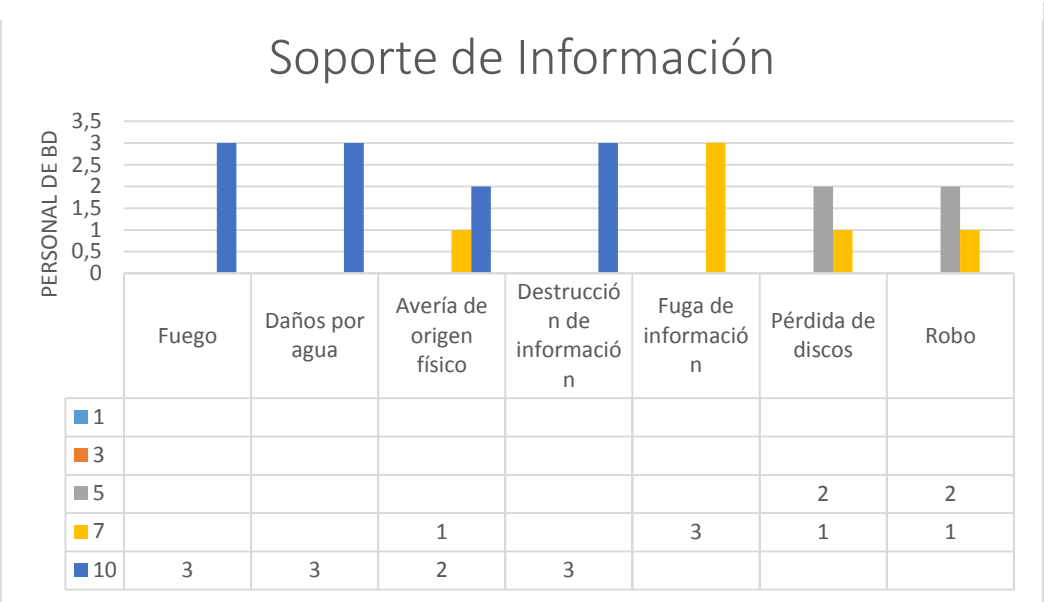
Fuente: Elaboración Propia

Grafico 14: Niveles de Impacto, activo Equipamiento Auxiliar



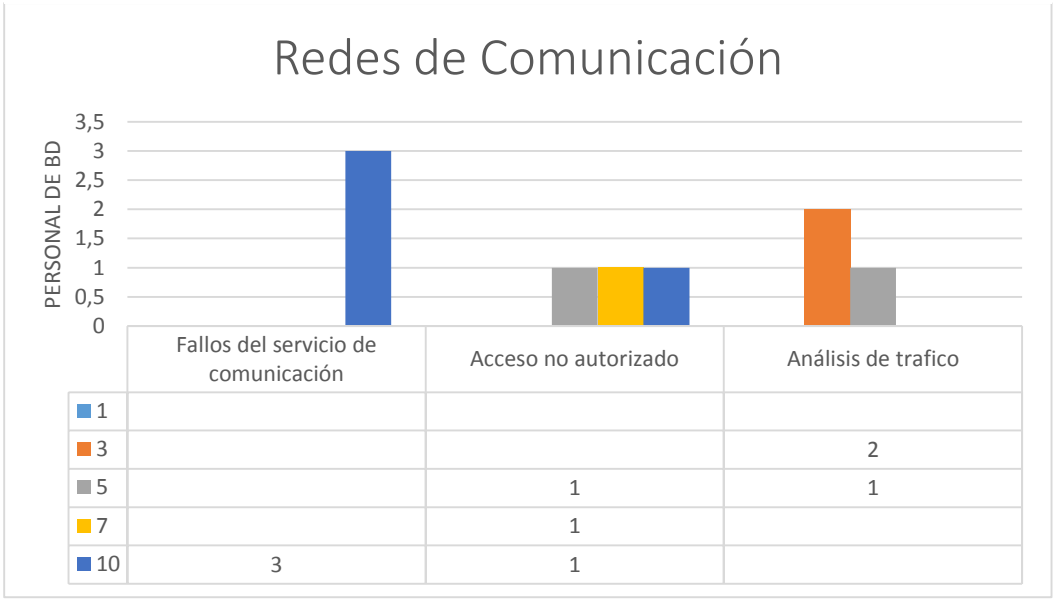
Fuente: Elaboración Propia

Grafico 15: Niveles de Impacto, activo de Soporte de Información



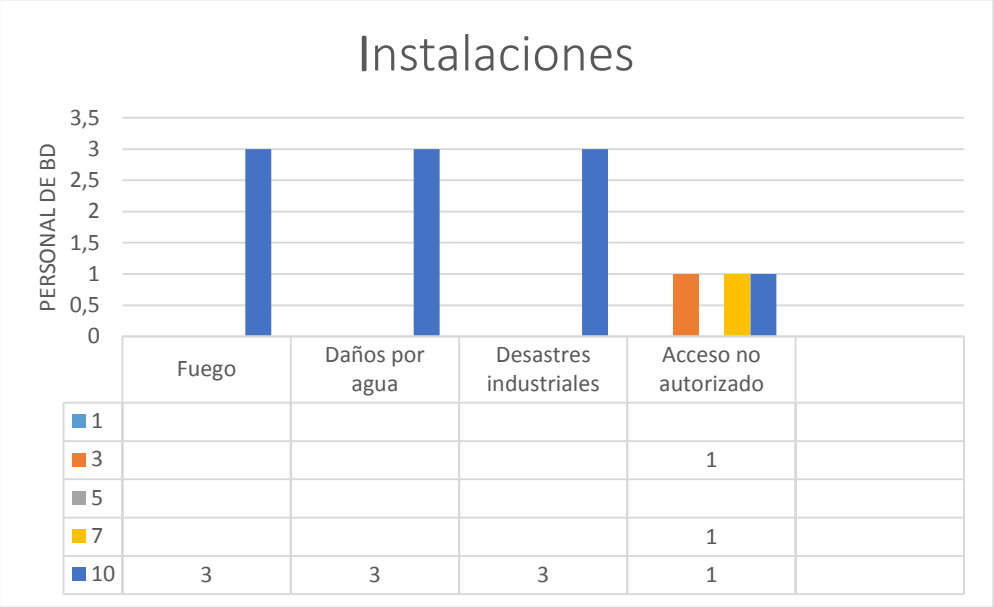
Fuente: Elaboración Propia

Grafico 16: Niveles de Impacto, activo de Redes de Comunicación



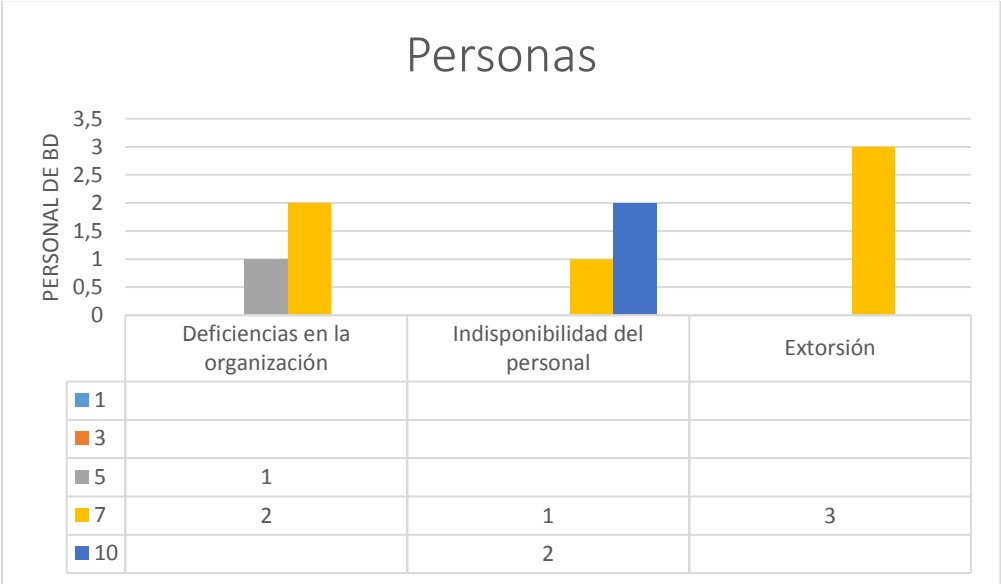
Fuente: Elaboración Propia

Grafico 17: Nivel de impacto, activo de Instalaciones



Fuente: Elaboración Propia

Grafico 18: Nivel de impacto, activo persona



Fuente: Elaboración Propia

Considerando los valores presentados anteriormente, se realiza una tabla donde se multiplica el promedio del nivel de probabilidad de ocurrencia con el promedio del nivel del impacto (véase tabla 12), con el fin de determinar el nivel de riesgo que alcanza cada amenaza.

Tabla 12: Probabilidad e impacto

Tipo de activo	Amenazas	Probabilidad	Impacto	Nivel
Datos	[E.2] Errores de administrador	3	6	18
	[E.18] Destrucción de la información	2	9	18
	[A.11] Acceso no autorizado	3	6	18
	[A.5] Abuso de privilegio de acceso	3	7	21
	[A.15] Modificación deliberada de la información	1	8	8
Claves criptográficas	[E.2] Errores de administrador	2	3	6
Aplicaciones informáticas (Software)	[I.5] Averías de origen lógico	5	10	50
	[E20] Vulnerabilidad de los programas	4	7	28
	[E.21] Errores de mantenimiento / actualización de programas (Software)	3	9	27
	[E.2] Errores de administrador	4	8	32
	[A.6] Abuso de privilegio de acceso	2	7	14
Equipamiento informático (hardware)	[N.1] Fuego	1	10	10
	[N.2] Daños por agua	1	10	10
	[I.5] Avería de origen físico	1	10	10
	[E.23] Errores de mantenimiento / actualización de equipos hardware	1	7	7
	[E.24] Caída de sistemas por agotamiento de recursos	7	10	70
	Caída del sistema por espacio insuficiente en la partición de datos	8	10	80

Tipo de activo	Amenazas	Probabilidad	Impacto	Nivel
Soportes de información	[N.1] Fuego	1	10	10
	[N.2] Daños por agua	1	10	10
	[I.5] Avería de origen físico lógico	1	9	9
	[E.18] Destrucción de información	1	10	10
	[E.19] Fuga de información	1	7	7
	[E.25] Pérdida de discos	1	5	5
	[A.25] Robo	1	5	5
Equipamiento auxiliar	[N.1] Fuego	1	10	10
	[N.2] Daños por agua	1	10	10
	[I.5] Avería de origen físico	5	10	50
	[I.7]Condiciones inadecuadas de temperatura o humedad	3	5	15
	[A.11] Acceso no autorizado	1	5	5
	[H.11] Interrupción de energía eléctrica	8	10	80
Redes de comunicación	Fallos del servicio de comunicación (Enlace de datos)	8	10	80
	Acceso no autorizado	1	7	7
	Análisis de trafico	1	3	3

Tipo de activo	Amenazas	Probabilidad	Impacto	Nivel
Instalaciones	[N.1] Fuego	1	10	10
	[N.2] Daños por agua	1	10	10
	[I.*] Desastres industriales	1	10	10
	[A.11] Acceso no autorizado	1	6	6
Personal	[E.7] Deficiencias en la organización	2	6	12
	[E.28] Indisponibilidad del personal	3	9	27
	[A.29] Extorsión	2	7	14

Fuente: Elaboración propia

Se logra evidenciar por medio del cuestionario aplicado al personal del área de base de datos, que los riesgos asociados con Caída de sistemas por agotamiento de recursos, Caída del sistema por espacio insuficiente en la partición de datos, Avería de origen físico, Interrupción de energía eléctrica y Fallos del servicio de comunicación (caída del enlace de datos). Tomando como referencia estos resultados y los intervalos establecidos en al procedimiento metodológico (ilustración 7). Las estrategias de continuidad se enfocan en contrarrestar estas categorías de riesgos, dado el nivel de riesgo alto y muy alto que alcanzan.

3.2.1.4. Análisis del impacto del negocio

Identificación de los procesos del negocio

En esta etapa se describen todos los procesos aplicados por la Institución que apoyan al logro de la misión, visión y metas propuestas.

Tipo de Proceso	Tipo de servicio	Nombre	Prioridad
Operacionales y Financiera	Sistema de Base de Datos	SOFACMEPROD	Alta
Directivo	Sistema de Base de Datos	SITACMEPROD	Alta
Administrativo	Sistema de Base de Datos	GENACMEPROD	Alta
		SORACMEPROD	
Cliente	Sistema de Base de Datos	VETACMEPROD	Alta
		ACMEPROD	

Ilustración 14: Procesos del Negocio

Fuente: Elaboración propia

. **Procesos Críticos**

En función del nivel de relación y relevancia directa con la continuidad del negocio y desde un enfoque de análisis detallado posterior de los recursos que soportan los procesos, se llega a la conclusión que todos los sistemas de base de datos son esenciales, pero tienen cierto nivel de prioridad los expuestos a continuación:

Tipo de Proceso	Tipo de servicio	Nombre	Prioridad
Cliente	Sistema de Base de Datos	ACMEPROD	Alta
		VETACMEPROD	

Ilustración 15: Procesos Críticos

Fuente: Elaboración propia

Establecimiento de los tiempos de recuperación (Definiciones)

Como parte del proceso de construcción del PCN, se identificó aquellos tiempos críticos que la empresa puede tolerar en un proceso que se encuentre detenido, entre los principales tiempos tenemos:

- Maximun Tolerable Downtime (MTD): Representa el período máximo de tiempo que puede tolerar la organización sin entrar en un colapso financiero y operacional
- Recovery Time Objective (RTO): Indica el tiempo disponible para recuperar sistemas y/o recursos que han sufrido una alteración
- Recovery Point Objective(RPO): Se refiere a la magnitud de la pérdida de datos, medida en términos de un período de tiempo que un proceso de negocios puede tolerar
- Work Recovery Time (WRT): Es el tiempo disponible para recuperar datos perdidos una vez que los sistemas están reparados dentro del MTD

Para el caso de la Empresa ACME se tomará en cuenta principalmente los tiempos RPO y RTO, además se debe recordar que estos tiempos fueron definidos por los responsables de los procesos, y servirán como marco de referencia para dos temas puntuales:

RPO.- Tiempo usado para identificar si la frecuencia actual en la que se obtienen los backups y PITs de las bases de datos y demás servicios son los adecuados.

RTO.- Sirve de condicionante para el tiempo que deberá durar la ejecución de la alternativa de solución seleccionada ante la ocurrencia de un evento alterador.

Tiempos críticos por Servicio

Una vez identificado el sistema de base de datos más crítico de la empresa, se establecen los tiempos de recuperación que son una serie de componentes correspondientes al tiempo disponible para recuperarse de una alteración o falla del sistema. Los tiempos de recuperación se describen a continuación.

Proceso	Máquina Virtual	Tiempo critico
BASE DE DATOS	ACMEPROD	20 MINUTOS
BASE DE DATOS	SITACMEPROD	30 MINUTOS
BASE DE DATOS	GENACMEPROD	30 MINUTOS
BASE DE DATOS	SORACMEPROD	30 MINUTOS
BASE DE DATOS	VETACMEPROD	20 MINUTOS
BASE DE DATOS	SOFACMEPROD	30 MINUTOS

Ilustración 16: Tiempos críticos

Fuente: Elaboración propia

En la tabla anterior, el servicio de bases de datos ACMEPROD y VETACMEPROD nos viene a decir que posee una criticidad alta, proyectándose en las fechas límites para la empresa, donde el nivel de transacciones es más alto. Se determina un RTO de 20 minutos como tiempo de recuperación para restablecer el servicio.

Se deben contar con alternativas y mecanismos que le brinden disponibilidad apenas se detecte una falla en el servicio de base de datos y así evitar un largo tiempo de inactividad de las operaciones del negocio.

CAPITULO IV: Fase de Diseño del Plan de Continuidad

A continuación, se presenta la solución generada a partir de la investigación realizada en este trabajo final.

Nosotros entenderemos el plan de continuidad de negocio como plan de continuidad de los servidores de bases de datos, omitiendo la parte del enfoque global para una organización y centrándonos única y exclusivamente a un componente que corresponde a un plan de continuidad de TI.

Consiste en un plan de acción donde se especifican las acciones a seguir para recuperar las funciones operativas de forma parcial o total y, restaurarlas a su ambiente de trabajo normal en un tiempo determinado, ante una eventualidad o interrupción no deseada que impacte a los sistemas de base de datos.

“Plan de continuidad de Negocio en los servidores de bases de datos para el departamento de informática de la empresa ACME”

Elaborado por:

Luis Manuel Menocal

Y

Moisés Enrique Zeledón

2022

TITULO	Plan de continuidad de negocio en los servidores de bases de datos	**CODIGO**	ACME-DC01
DISTRUBUIDA A	DEPARTAMENTO DE INFORMATICA	**VERSION**	Enero 2022
FECHA DE EMISION	Marzo 2022	**PAGINA**	76-
AUTORES	Luis Manuel Menocal Moisés Enrique Zeledón		

CONTROL DE VERSIONES

VERSIÓN	OBSERVACIONES
1.0	Documento original

LISTA DE DISTRIBUCIÓN

Este documento es de uso interno de la empresa ACME, los cambios de este documento son controlados y registrados en la tabla de control de revisiones.

1. Propósito

Este documento describe cómo debe ser realizada la gestión de continuidad por la empresa ACME mediante un Plan de Continuidad, instaurando una estrategia que permita minimizar el riesgo existente ante peligros que afecten a los servidores de base de datos, y en caso de que se presente un evento disruptivo restablecer las operaciones en el tiempo mínimo posible

2. Alcance

Esta propuesta aplica a la empresa ACME, Departamento de informática, especialmente al área de base de datos, se limita al ámbito de acción con estrategias a los procesos principales y riesgos de los servidores de base de datos identificados en el análisis de riesgos respectivamente.

Este plan está redactado en base a los resultados del Análisis y evaluación de riesgos en los servidores de base de datos.

3. Equipos

El personal que compone el equipo de trabajo responsable de gestionar y ejecutar el plan de continuidad de negocio en los servidores de base de datos del departamento de informática de la empresa ACME, se encuentra conformado según la siguiente ilustración.

Ilustración 17 Organigrama del Equipo de Trabajo

A continuación, en las tablas 13, 14 y 15 se detallan cada una de las funciones de los equipos de trabajo y los integrantes de cada equipo.

Tabla 13: Equipos director, responsables del Plan

EQUIPO	FUNCIONES	INTEGRANTES
Equipo director	Dirigir las actividades durante la contingencia y recuperación: • Análisis de la situación. • Activación o no del plan de continuidad. • Coordinar las actividades de contingencia con los diferentes integrantes del equipo responsable del plan de continuidad. • Seguir el estado de las estrategias aplicadas, confirmar el cierre del plan y retorno a la normalidad.	• Director del departamento de informática. • Subdirector del departamento de informática.

Tabla 14: Equipos de Recuperación, responsables del Plan

EQUIPO	FUNCIONES	INTEGRANTES
Equipo de recuperación	Proveer la logística necesaria para las actividades de recuperación de los servidores de base de datos: • Coordinar las actividades relacionadas con la recuperación de los servicios, en este caso los sistemas de base de datos. • Evaluar la disponibilidad de los servidores. • Inspeccionar los activos que componen el sistema de comunicaciones principalmente el centro de datos y el sitio alterno ubicado fuera de Managua. • Transporte de máquinas virtuales a centro de datos alterno. • Coordinar las actividades relacionadas con revisión o monitoreo de configuraciones de routers, switches y enlaces. • Contacto con los proveedores.	• Líder del área de Apoyo tecnológico • Líder de Base de Datos y sistemas operativos • Administrador de base de datos y sistemas operativos

Tabla 15: Equipos de Pruebas, responsables del Plan

EQUIPO	FUNCIONES	INTEGRANTES
Equipo de pruebas	Realizaran las pruebas de verificación de operaciones de los servidores de base de datos y sitios web relacionados: • Certificar el buen funcionamiento de los servidores de bases de datos previo al cierre del plan. • Certificar el buen funcionamiento de los sitios web que tienen conexión con el servidor de base de datos. • Cada perfil debe tener su plan de pruebas de verificación el cual debe entregar al equipo de recuperación.	• Líder de Apoyo tecnológico • Líder de Base de Datos y sistemas operativos • Administrador de base de datos y sistemas operativos • Líder de comunicaciones • Líder de desarrollo

Fuente: Elaboración propia

4. Datos informativos

A continuación, se coloca la información de contactos de miembros de equipos, proveedores, centro de dato alterno y líderes de áreas.

4.1. Datos de los Miembros de los Equipos

Tabla 16: Datos de contactos del Equipo Director

MIEMBRO DE EQUIPO DIRECTOR			DATOS DE CONTACTO			
Rol	**Nombre**	**Clasificación**	**Celular**	**Extensión**	**Correo**	**Dirección**
Director del departamento de informática	xxxxxx	Interno	86364916	0000	xxxxxx	Managua
Sub Director del departamento de informática	xxxxxx	Interno	86364916	0000	xxxxxx	Managua

Fuente: Elaboración propia

Tabla 17: Datos de Contacto del Equipo de Recuperación

MIEMBRO DE EQUIPO DE RECUPERACION			DATOS DE CONTACTO			
Rol	**Nombre**	**Clasificación**	**Celular**	**Extensión**	**Correo**	**Dirección**
Líder de Apoyo tecnológico	xxxxxx	Interno	86364920	0000	xxxxxx	Managua
Líder de unidad de base de datos	xxxxxx	Interno	86364917	0000	xxxxxx	Managua
Líder de comunicaciones	xxxxxx	Interno	86364918	0000	xxxxxx	Managua
Administrador de base de datos y sistemas operativos	xxxxxx	Interno	86364922	0000	xxxxxx	Managua

Fuente: Elaboración propia

Tabla 18: Datos de Contacto del Equipo de Pruebas

MIEMBRO DE EQUIPO DEPRUEBAS			DATOS DE CONTACTO			
Rol	**Nombre**	**Clasificación**	**Celular**	**Extensión**	**Correo**	**Dirección**
Líder de Apoyo tecnológico	xxxxxx	Interno	86364920	0000	xxxxxx	Managua
Líder de unidad de base de datos	xxxxxx	Interno	86364917	0000	xxxxxx	Managua
Líder de comunicaciones	xxxxxx	Interno	86364918	0000	xxxxxx	Managua
Administrador de base de datos y sistemas operativos	xxxxxx	Interno	86364922	0000	xxxxxx	Managua
Líder de Desarrollo	xxxxxx	Interno	86364922	0000	xxxxxx	Managua

Fuente: Elaboración propia

Tabla 19: Datos de Contacto del Proveedores

DATOS DE PROVEEDORES			DATOS DE CONTACTO			
Compañía	**Servicio**	**Clasificación**	**Nombre**	**Celular**	**Correo**	**Dirección**
Claro	Internet	Externo	xxxxxx	86364916	xxxxxx	Managua
Ideay	Internet	Externo	xxxxxx	86364920	xxxxxx	Managua
Telssa	Mantenimiento de UPS y aires de climatización	Externo	xxxxxx	22780255	xxxxxx	Managua

Fuente: Elaboración propia

Tabla 20: Datos de Contacto del Centro de Datos Alterno

Centro	Centro de datos Alterno		
Cuidad	En las afueras de Managua		
Nombre	Xxxxxx	**Rol**	Supervisor de Centro de Datos Alterno
Extensión	0000		
Teléfono	22780255		

Fuente: Elaboración propia

5. Ejecución y conclusión del plan de continuidad

Dentro de la gestión del plan de continuidad de los servidores de bases de datos, un punto clave de definir son los responsables tanto de iniciar el plan de continuidad como de cerrarlo.

5.1. Responsable de iniciar el plan de continuidad

El plan de continuidad debe de iniciarse cada vez que exista una eventualidad que impacte en la operación y el ambiente normal de los servidores de bases de datos de la empresa ACME.

El plan de continuidad puede ser iniciado por:

- Director del Departamento de Informática
- Sub Director del Departamento de Informática

En caso de estar ausentes, la función será realizada por:

- Líder de Apoyo Tecnológico

5.2. Responsables de cerrar el plan de continuidad

El plan de continuidad puede ser cerrado una vez que se cumpla con las actividades de retorno a la operación normal.

El plan de continuidad debe ser cerrado en conjunto por:

- Director del Departamento de Informática
- Sub Director del Departamento de Informática
- Líder de Apoyo Tecnológico

5.3. Comunicación

Se utilizarán las siguientes vías de comunicación entre el equipo de gestión de continuidad en los servidores de base de datos para el Departamento de Informática.

1. Teléfono Móvil: Se dispone de un Smartphone dedicado para emergencias que se presenten tanto en el Centro de Datos principal como en el centro de Datos alterno. Este consta de llamadas ilimitadas y mensajería a cada uno de los Lideres responsables del Plan de continuidad.

   El teléfono celular se encuentra ubicado en la gaveta número 3 del casillero que se encuentra en la entrada al centro de datos.

2. Extensión con salida externa: Se dispone de una extensión de telefonía IP con salida a teléfonos externos. El número de extensión con salida externa es la 3456.

3. Correo electrónico: Se dispone de correo electrónico para dejar documentado el incidente.

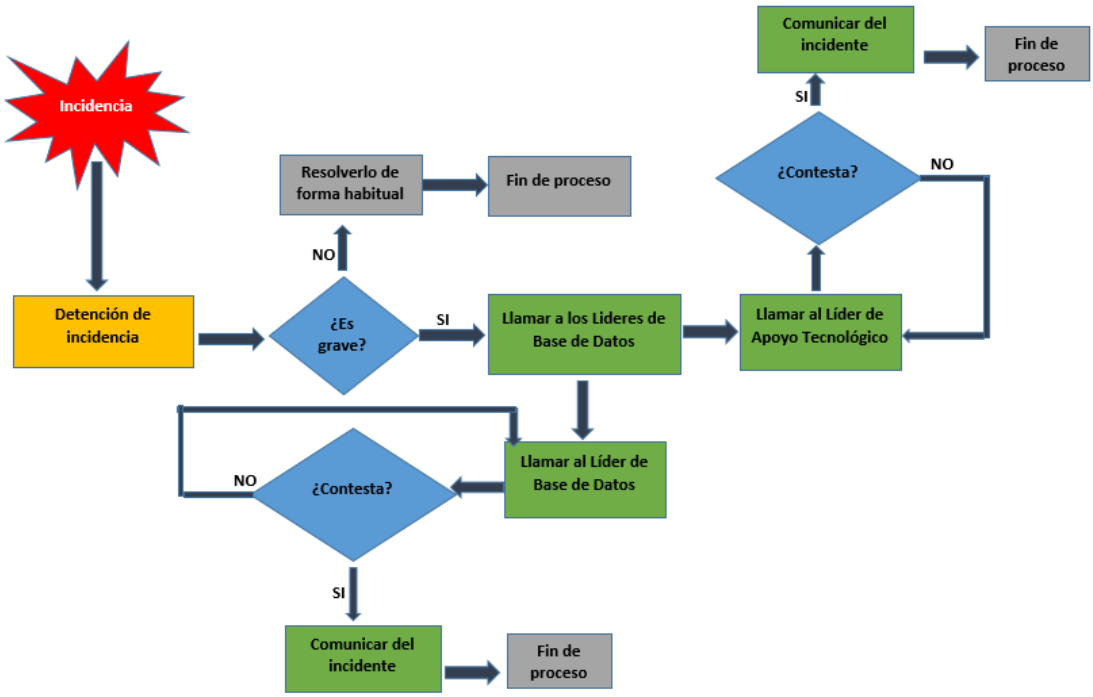


Ilustración 18: Proceso de Comunicación

Fuente: Elaboración propia

6. Activación de plan de continuidad

La activación del plan de continuidad en los servidores de base de datos conlleva una serie de actividades secuenciales que son necesarias para aplicar las estrategias según el incidente presentado.

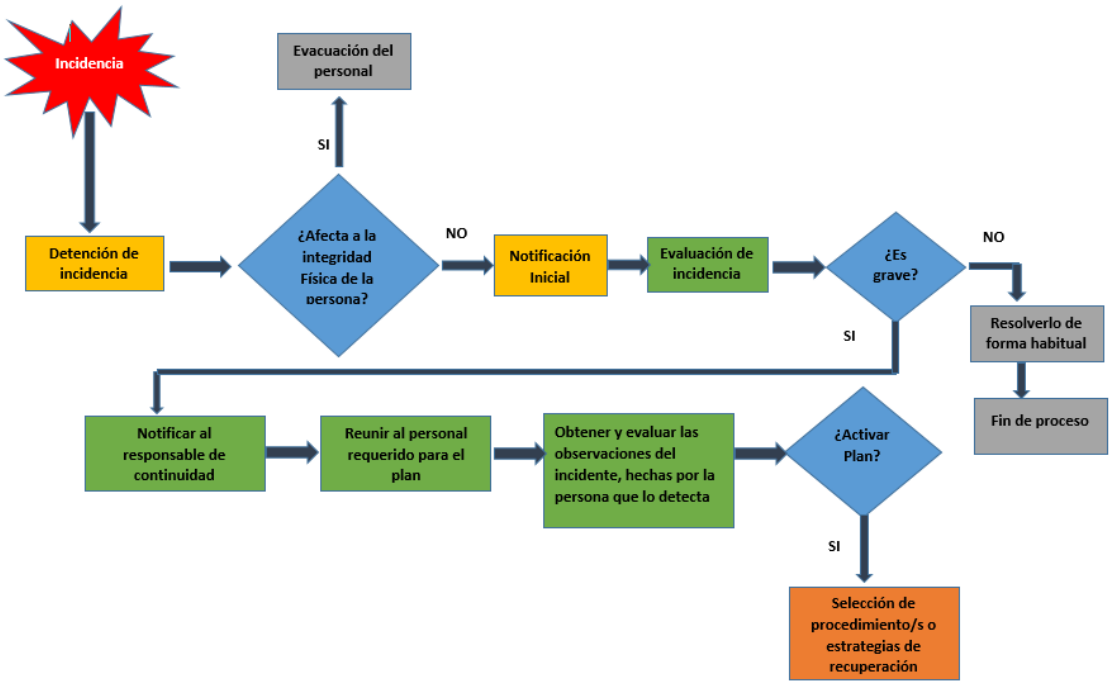


Ilustración 19: Proceso de activación del Plan

Fuente: Elaboración propia

A continuación, en la tabla 21 se detallan cada una de las actividades y responsables al momento de presentarse un incidente en los servidores de base de datos.

Tabla 21: Actividades de activación del Plan

FASE	EVENTO	ACTIVIDAD	RESPONSABLE
Alerta	Notificación Inicial	Al momento que se presente una interrupción del servicio de base de datos, el administrador de base de datos que lo identifica debe notificar inmediatamente al personal señalado en la sección responsables de iniciar el plan de continuidad en los servidores de bases de datos (Véase Plantilla de Notificación Inicial).	Usuario que conoce en primera instancia de la incidencia
Alerta	Evaluación de Incidentes	Una vez que se reciba la notificación inicial, y que el responsable notifique la autorización de la aplicación del plan de continuidad en los servidores de bases de datos, el coordinador del plan notifica y reúne a todo el personal requerido para su ejecución en caso de ser necesario.	Líder de Apoyo Tecnológico
Alerta	Evaluación de Incidentes	El equipo del plan de continuidad revisa las observaciones hechas por el personal que detecta el incidente o falla en los sistemas de base de datos, y realiza una inspección del incidente.	Equipo de recuperación
Activación del Plan	Activación	Una vez que se identifica el incidente y sus consecuencias en la operación, se confirma con el responsable de iniciar el plan con las actividades necesarias para mantener las operaciones críticas y recuperar los sistemas de bases de datos de la empresa.	Equipo de recuperación

FASE	EVENTO	ACTIVIDAD	RESPONSABLE
Vuelta a la Normalidad	Análisis	El equipo Director se reunirá para realizar una valoración de los daños y llenaran el registro de evaluación colocando adicionalmente si el servicio de base de datos está operativo o no. Además, en que Centro de Datos se encuentra funcionando. Se realizará una valoración de los servicios activados, tiempos empleados para su activación, servicios no activados y todas aquellas observaciones que se encontraron en los procesos.	Equipo Director

Fuente: Elaboración propia

7. Estrategias de continuidad

Dentro del plan de continuidad se detalla un conjunto de estrategias dirigidas a anticipar y/o responder a incidentes que afecten los activos críticos que conforman y complementan el buen funcionamiento de los servidores de base de datos.

Se brindará el detalle de cómo se actuará ante cada posible escenario de paralización de los Servicios de Bases de Datos.

7.1. Estrategias Proactivas

Las estrategias que se plantean a continuación buscan impedir la materialización de un riego y/o reducir las consecuencias de una interrupción a través de inspecciones preventivas aplicadas por los responsables de velar por el buen funcionamiento de los servidores de base de datos y cada uno de sus activos dependientes.

Tabla 22: Estrategias Proactivas

	CÓDIGO DE PLANTILLA	RESPONSABLE	PLANTILLA
INSPECCIÓN DIARIA DE LOS SERVIDORES DE BASE DE DATOS	ACME_PO01	Administradores de base de datos y sistemas operativos.	Véase tabla 25
INSPECCIÓN DIARIA DE COPIAS DE SEGURIDAD EN SERVIDOR DE RESPALDO	ACME_PO02	Administradores de base de datos y sistemas operativos.	Véase tabla 26
REVISIÓN DIARIA DE LAS INSTALACIONES DEL CENTRO DE DATOS.	ACME_PO03	Administrador de base de datos y sistemas operativo asignada a los respaldos	Véase tabla 27
INSPECCIÓN MENSUAL DE ACTUALIZACIONES	ACME_PO04	Administradores de base de datos y sistemas operativos.	Véase tabla 28

	CÓDIGO DE PLANTILLA	RESPONSABLE	PLANTILLA
PRUEBAS DE INTEGRIDAD DE COPIAS DE SEGURIDAD	ACME_PO05	Administradores de base de datos y sistemas operativos.	Véase tabla 29
PRUEBAS DE FUNCIONALIDAD DE EQUIPAMIENTO AUXILIAR	ACME_PO06	Líder de Apoyo tecnológico, Líder de comunicaciones y Administradores de base de datos.	Véase tabla 30

Fuente: Elaboración propia

7.2. Estrategias reactivas

Las estrategias que se plantean a continuación tienen como objetivo ayudar a reanudar los servicios de base de datos u operaciones de los activos relacionados, en caso de sufrir una interrupción generada por la materialización de un riesgo.

Tabla 23: Estrategias Reactivas

	CÓDIGO DE PLANTILLA	RESPONSABLE	PLANTILLA
PARTICIÓN PRINCIPAL DONDE SE ALOJAN LAS BASE DE DATOS SIN ESPACIO	ACME_PR01	Administradores de base de datos y sistemas operativos.	Véase tabla 31
SATURACIÓN DE RECURSOS DEL SERVIDOR	ACME_PR02	Administradores de base de datos y sistemas operativos.	Véase tabla 32

	CÓDIGO DE PLANTILLA	RESPONSABLE	PLANTILLA
CORTE DE SUMINISTRO ELÉCTRICO	ACME_PR03	Administradores de base de datos y sistemas operativos.	Véase tabla 33
AVERIA FISICA EN EL SISTEMA DE CLIMATIZACION	ACME_PR04	Administradores de base de datos y sistemas operativos.	Véase tabla 34

Fuente: Elaboración propia

8. Cierre del plan

En esta sección se muestran los elementos que deben verificarse una vez se haya cumplido con cada uno de los aspectos que detalla la estrategia aplicada y que el servicio de base de datos haya sido restaurado (véase tabla 24).

Dependiendo del incidente presentado, puede requerirse una inspección minuciosa por parte del personal del área de base de datos.

Tabla 24: Estrategias de Cierre

	CÓDIGO DE PLANTILLA	RESPONSABLE	PLANTILLA
INSPECCION DE INSTALACIONES DEL CENTRO DE DATOS	ACME_PC01	Administradores de base de datos y sistemas operativos.	Véase tabla 35
SITIOS WEB Y ACCESO A INFORMACION	ACME_PC02	Administradores de base de datos y sistemas operativos.	Véase tabla 36

Fuente: Elaboración propia

9. Platillas

A continuación, se presentan las plantillas a utilizar en la gestión del plan de continuidad de los Servidores de Base de Datos. Las Plantillas contemplan cada una de las actividades tanto para las estrategias proactivas que ayudaran a minimizar el riesgo de ocurrencia de una amenaza, como las proactivas que servirán en repuesta a un evento que se presente y perjudique la operatividad de los Servicios de Base de Datos.

9.1. Plantillas para estrategias proactivas

Los siguientes activos o elementos deben de ser revisados diariamente por el Administrador de base de datos y sistemas operativos responsable de velar por el bienestar de sus servidores asignados.

9.1.1. PLANTILLAS DIARIAS

Las siguientes plantillas que se presentan son de suma importancia que se lleven a cabo todos los días.

Tabla 25: Inspección diaria de Servidores

<table>
<tr><td colspan="3">PLAN DE CONTINUIDAD DE SERVIDORES DE BASE DE DATOS
DEPARTAMENTO DE INFORMATICA
INSPECCION DIARIA DE SERVIDORES DE BASE DE DATOS</td></tr>
<tr><td colspan="2">Responsable: Responsable de cada servidor</td><td>CODIGO: ACME_PO01</td></tr>
<tr><td colspan="2">Los siguientes elementos deben de ser revisados diariamente.
Marque con un en ✓ cada elemento inspeccionado, en caso de encontrar una anomalía detallarlo en la sección de observaciones. Enviar un reporte al correo reportesd@acme.com.</td><td></td></tr>
<tr><td colspan="2">PROTOCOLO DE RESTAURACION</td><td>Marque</td></tr>
<tr><td colspan="2">1. CONEXIÓN A SERVIDORES</td><td></td></tr>
<tr><td>Para conexión de servidores Linux:
Acceder al servidor a través del protocolo ssh:
a. Abrir la aplicación putty
b. Digitamos la ip del servidor y el puerto 22
c. Ingresamos el usuario: root y contraseña: *******</td><td>Para conexión de servidores Windows:
Realizar la conexión a través de escritorio remoto:
a. Pulsa la tecla "Windows" + "R"
b. Escribir "mstsc"
c. Se abrirá la ventana de escritorio remoto, ingresar ip y credenciales.</td><td></td></tr>
<tr><td colspan="2">2. INSPECCION DE PARTICIONES PRINCIPALES</td><td></td></tr>
<tr><td colspan="2">Realizar una inspección detallada del espacio utilizado.</td><td></td></tr>
<tr><td>Para servidores Linux
Particiones principales a revisar:
/var
/sti
/dba
Para verificar el estado actual:</td><td>Para servidores Windows
Particiones principales a revisar:
C:
D:
Verificar el espacio disponible.</td><td></td></tr>
</table>

<table>
<tr><th colspan="2">PROTOCOLO DE RESTAURACION</th><th>Marque</th></tr>
<tr><td colspan="2">3. VERIFICACION QUE SE HAYA HECHO EL RESPALDO DE LAS BASES DE DATOS Y ARCHIVOS DE CONFIGURACIÓN</td><td></td></tr>
<tr><td colspan="2">Revisar que se haya realizado el respaldo de las bases de datos que están alojadas en el servidor, además revisar el respaldo de los archivos de configuración.</td><td></td></tr>
<tr><td>Para servidores Linux

Entrar a la ruta de respaldos:
cd /dba/Respaldos/RESPAL_Fecha_del_dia

verificar el peso de cada archivo de respaldo:
ls –lh
du –hcs * |more</td><td>Para servidores Windows

D:/RespaldosSQL/

Verificar que se hayan eliminado los respaldos más antiguos y que ya se hayan trasladado al servidor de respaldo.</td><td></td></tr>
<tr><td colspan="2">4. VERIFICACIÓN DE LA REPLICACIÓN DE LAS BASES DE DATOS</td><td></td></tr>
<tr><td colspan="2">Hacer una inspección del servicio de replicación de bases de datos. De esta manera confirmar el traslado y respaldo de información en el servidor replica.</td><td></td></tr>
<tr><td>Para conexión de servidores Linux

Para verificar el estado de la replicación
Ejecutamos el siguiente comando en el servidor maestro desde mysql:

show master status;
Para verificar el estado de la replicación en el servidor esclavo ejecutamos el siguiente comando:

show slave status \G;

verificamos el parámetro de segundos de retraso.

Si hay retraso procedemos a revisar las conexiones a la base de datos y verificar si no hay tablas bloqueadas.</td><td>Para servidores Windows

Para la verificación de la replicación:

Iniciar el Management Studio y desplegar el servidor .

– Entrar a Replicación.
– Publicaciones Locales.
– Click derecho al nombre del servidor replica.
– Iniciamos el monitor de replicación.
– Y verificamos que el estado este en ejecución.</td><td></td></tr>
</table>

Show processlist; Si hay bloqueo eliminamos las sesiones que lo están ocasionando, pero omitiendo las del root. *Kill -9 id_de_sesion*		
5. VERIFICACION DEL TAMAÑO DE LOS LOG		
Para servidores Linux Se deben de verificar los logs de mysql, esto se almacenan en la siguiente ruta: *Cd /var/log/mysql* *Para listarlos:* *du -hcs * |more* *Verificamos el tamaño de los archivos siguientes:* *mysql-queries.log* *mysql-slow.log* *mysqld.log* Si los archivos son muy grandes y pasan los 10G procedemos a vaciar los logs. *mysqladmin flush-logs* Este comando corta los archivos logs y crea nuevos archivos. Seguidamente pasamos los archivos viejos al servidor de respaldo y los borramos del servidor de base de datos. *Scp archivos 10.10.220.23:/Respaldos/BD/Fecha_del_dia*	**Para servidores Windows** Para los servidores Windows se debe de revisar el estado de los logs en la ruta: *C:\LogsSQL* Verificamos el tamaño y si son muy grandes procedemos a ejecutar el depurador de logs en la ruta. *C:\LogsSQL* Para ejecutar seleccionamos el archivo *depurarLogs.bat* y click derecho ejecutar.	

Además, revisamos el estado de los Binary Logs de replicación: *Entramos a mysql y listamos los logs de replicación con el comando:* *show Binary logs;* Si existen más de tres archivos de Binary Logs, procedemos a depurarlos. *PURGE BINARY LOGS BEFORE '2008-02-01 21:00:00'* Borra los Logs antes a la fecha.		

Tabla 26 Revisión diaria de Copias de Seguridad

PLAN DE CONTINUIDAD DE SERVIDORES DE BASE DE DATOS **DEPARTAMENTO DE INFORMATICA** **INSPECCIONES DIARIA DE COPIAS DE SEGURIDAD EN SERVIDOR DE RESPALDO**	
Responsable: Responsable de cada Servidor	CODIGO: ACME_PO02
Los siguientes elementos deben de ser inspeccionados diariamente. Marque con un ✓ en cada elemento inspeccionado, en caso de encontrar una anomalía detallarlo en la sección de observaciones. Enviar un reporte al correo reportesd@acme.com. Esta actividad asegurara que se cuente con una copia de seguridad en caso de llegar a necesitarla.	
ACIONES	
Elementos a inspeccionar	**Marque**
1. Realizar conexión al servidor de respaldo.	

Atreves de una conexión ssh.	
2. Verificar el espacio disponible en la partición de respaldo de los servidores productivos. /Respaldos	
3. Verificar que cada respaldo de las bases de datos y archivos de configuración se hayan trasladado correctamente y que se encuentren completos. a. Si no están completos, reportar al administrador encargado del servidor, para que verifique el respaldo y lo traslade al servidor de respaldo. b. Si el respaldo está completo continuar con la siguiente actividad.	
4. Trasladar y verificar los respaldos de base de datos productivas al disco externo que luego este será enviado a resguardo.	

Tabla 27 Inspección diaria de instalaciones

PLAN DE CONTINUIDAD DE SERVIDORES DE BASE DE DATOS **DEPARTAMENTO DE INFORMATICA** **REVISIÓN DIARIA DE LAS INSTALACIONES DEL CENTRO DE DATOS**	
Responsable: DBA que está haciendo el turno ese día.	CODIGO: ACME_PO03
La siguiente actividad debe ser realizada diario. Marque con un ✓ en cada elemento inspeccionado, en caso de encontrar una anomalía detallarlo en la sección de observaciones. Enviar un reporte al correo reportesd@acme.com. Esta actividad garantizara que las instalaciones y equipos informáticos estén siempre supervisados evitando posibles fallas por falta de inspección en equipos e infraestructura.	
ACIONES	
Elementos a inspeccionar	**Marque**
1. Inspección de funcionalidad de equipos de protección como: UPS, unidades de refrigeración, alarmas contra incendio y cámaras de seguridad .	
2. Inspección del estado de dispositivos de comunicaciones como: Switches, routers y cableado)	
3. Inspección de humedad en el centro de datos, mover en puntos críticos el piso falso para revisar si existe basura o humedad que pueda perjudicar.	
4. Inspección de integridad física de los servidores.	

9.1.2. PLANTILLAS MENSUALES

Las siguientes plantillas que se presentan son de suma importancia que se lleven a cabo mensualmente.

Tabla 28 Inspección Mensual de Actualizaciones

PLAN DE CONTINUIDAD DE SERVIDORES DE BASE DE DATOS **DEPARTAMENTO DE INFORMATICA** **INSPECCION MENSUALES DE ACTUALIZACIONES**	
Responsable: Responsable de cada servidor	CODIGO: ACME_PO04
Los siguientes elementos deben de ser revisados de manera mensual. Marque con un ✓ en cada elemento inspeccionado, en caso de encontrar una anomalía detallarlo en la sección de observaciones. Enviar un reporte al correo reportesd@acme.com.	
ACIONES	
Elementos a inspeccionar	**Marque**
1. Realizar conexión a los servidores: Para los servidores Linux a través de ssh y para servidores Windows conexión de escritorio remoto.	
2. Realizar una inspección detallada de las actualizaciones de versiones del sistema operativo y paquetes del servidor de base de datos.	
3. Revisar la configuración del firewall que se encuentre configurada correctamente con las ip de los usuarios y servidores que tienen acceso a las base de datos.	

4. Verificar que el antivirus en los servidores Windows este en la última actualización de firma.	
5. Hacer una inspección de los diferentes accesos a las bases de datos, actualizando el reporte de acceso.	

Tabla 29 Pruebas de Integridad de Copias de Seguridad

PLAN DE CONTINUIDAD DE SERVIDORES DE BASE DE DATOS **DEPARTAMENTO DE INFORMATICA** **PRUEBAS DE INTEGRIDAD DE COPIAS DE SEGURIDAD**	
Responsable: DBA responsable de las pruebas de copias de seguridad	CODIGO: ACME_PO05
La siguiente actividad debe ser realizada Mensualmente. Marque con un ✓ en cada elemento inspeccionado, en caso de encontrar una anomalía detallarlo en la sección de observaciones. Enviar un reporte al correo reportesd@acme.com. Esta actividad garantizara que la información respaldada de las diferentes bases de datos productivas cumpla con los requerimientos de integridad y disponibilidad al momento de necesitarlos por alguna falla en los servidores de base de datos.	
ACIONES	
Elementos a inspeccionar	**Marque**
1. Realizar conexión al servidor de respaldo.	
2. Traslado de respaldos de bases de datos a los ambientes de comprobación de integridad.	
3. Realizar la restauración de los respaldos en cada ambiente correspondiente, este puede ser en Windows o Linux.	

4. Realizar las pruebas de integridad de los datos restaurados.	
5. Trasladar y etiquetar la unidad de almacenamiento donde se guardara el respaldo verificado.	
6. Enviar el reporte de resultados al Líder de Apoyo tecnológico con la plantilla de pruebas de respaldos.	

Tabla 30 Pruebas de Funcionalidad de Equipamiento Auxiliar

PLAN DE CONTINUIDAD DE SERVIDORES DE BASE DE DATOS **DEPARTAMENTO DE INFORMATICA** **PRUEBAS DE FUNCIONALIDAD DE EQUIPAMIENTO AUXILIAR**	
Responsable: Líder de Apoyo tecnológico, Líder de comunicaciones y Administradores de base de datos.	CODIGO: ACME_PO06
La siguiente actividad debe ser realizada Mensualmente. Marque con un en ✓ cada elemento inspeccionado, en caso de encontrar una anomalía detallarlo en la sección de observaciones. Enviar un reporte al correo reportesd@acme.com. Con la realización de estas pruebas se pondrán a prueba el Sistema de UPS, el generador eléctrico, el sistema de refrigeración.	
ACIONES	
Elementos a inspeccionar	**Marque**
UPS y Generador de Energía	
1. Realizar corte de energía comercial.	
2. Las UPS después del corte, deberían entrar a funcionar.	
3. Si la energía comercial no ha regresado, el generador de energía debe entrar en un lapso de 15 minutos.	

Sistema de refrigeración	
4. El sistema de refrigeración está compuesto por dos unidades ambas sincronizadas, es decir que si una falla la otra que está suspendida debe de arrancar. Como prueba se debe de apagar la que está funcionando.	
5. Se debe de esperar un periodo de 10 segundos para que la unidad entre en funcionamiento.	
Nota: Estas pruebas de funcionalidad se tienen que realizar en periodos no laborables, para ser más específicos en ventanas de mantenimiento.	

9.2. Plantillas para estrategias reactivas

A continuación, se presentan las plantillas con las estrategias reactivas que conforman el plan de continuidad.

Tabla 31 Partición principal de base de datos sin espacio

PLAN DE CONTINUIDAD DE SERVIDORES DE BASE DE DATOS **DEPARTAMENTO DE INFORMATICA** **ESTRATEGIA REACTIVA** **PARTICION PRINCIPAL DONDE SE ALOJAN LAS BASE DE DATOS SIN ESPACIO**	
Nombre del colaborador : **Fecha:**	ACME_PR01
Escenario: Estrategia reactiva en caso de caída del servicio de base de datos por espacio insuficiente en la partición principal donde se alojan las bases de datos.	
PROTOCOLO DE RESTAURACIÓN	**Marque**
Conexión a servidor	
1. Acceder al servidor por medio de una conexión ssh. d. Abrir la aplicación *putty*	

e. Digitamos la *ip* del servidor y el puerto *22*

f. Ingresamos el *usuario: root* y c*ontraseña: ********

Dentro del servidor de base de datos

1. Una vez realizada la conexión exitosa al servidor
   a. Entramos a la partición con: *cd /var*
   b. Ejecutamos el siguiente comando para buscar los archivos más grabes.

      find /usr -type f -printf "%s %pn" | sort -rn | head -n 10

   c. Si el resultado nos muestra que el problema está en los log de mysql.

Depuración de log de mysql

1. Entramos a la ruta de los log.

   cd /var/log/mysql

   a. Listamos los archivos con la última fecha:

      ls -lht

      *du -hcs * | more*

2. Si el archivo de log es el problema procedemos a limpiarlo.
   a. Con el comando:

      mysqladmin -uroot -p flush-logs

      Se cerrará el archivo existente y se creará uno nuevo.

3. Pasamos los archivos log viejos al servidor de respaldo:

   Scp archivo 10.10.75.50:/Respaldos/BDPROD1/Fecha_del_dia

   Contraseña del servidor de respaldo: *Clave: **********

   a. Borramos los archivos log

Servicio de Mysql

1. Una vez depurado los archivos log
2. Procedemos a ver el estado del servicio de base de datos
   a. Para ver el estado: *service mysql status*
   b. Si el servicio está detenido procedemos a subirlo con el siguiente comando:

      service mysql start

   c. *Confirmamos de nuevo el estado del servicio*

service mysql status
Servicio de replicación
1. Ingresamos a Mysql *Mysql –u root –p* *Clave: ********** 2. Revisamos el estado de la replicación. *SHOW MASTER STATUS;* 3. Si la replicación esta correcta procedemos hacer un monitoreo continuo del servicio de base de datos, tanto manual como automático con la herramienta Nagios.

Tabla 32 Saturación de recursos de servidor

PLAN DE CONTINUIDAD DE SERVIDORES DE BASE DE DATOS **DEPARTAMENTO DE INFORMATICA** **ESTRATEGIA REACTIVA** **SATURACION DE RECUROS DEL SERVIDOR**	
Nombre del colaborador : **Fecha:**	ACME_PR02
Escenario: Estrategia reactiva en caso de caída del servicio de base de datos por saturación de recursos del servidor como: CPU, memoria y wr.	
PROTOCOLO DE RESTAURACIÓN	**Marque**
Conexión a servidor	
2. Acceder al servidor por medio de una conexión ssh. a. Abrir la aplicación *putty* b. Digitamos la *ip* del servidor y el puerto *22* c. Ingresamos el *usuario: root* y c*ontraseña: ********	
Dentro del servidor de base de datos	

2. Una vez conectados listamos los procesos en ejecución

   Comando: top

   Nos lista todos los procesos

   a. Procedemos a localizar todos los procesos que están saturando el servidor y los procesos tienen sesiones colgadas.

      ps –fu usuario

      Lista las sesiones que tiene ese usuario

      Con el comando: kill -9 id matamos la sesión

   b. Si el resultado nos muestra que el problema está en los log de mysql.

Conexiones Connx

4. Entramos a la ruta del servicio del connx.

   cd /sti/sag/connx

   Bajamos el servicio del connx:

   Sh connxserver stop

   a. Si hay sesiones colgadas de Connx las listamos y matamos

      Ps –fe |grep cnx

      Kill -9 id

Servicio de base de datos

3. Verificamos el estado de la base de datos

   a. Para ver el estado: *adaopr db=028 di=uq*

   b. Si el servicio esta caído porcedemos a asubirlo.

      adastart 028

   c. Confirmamos de nuevo el estado del servicio

      Adaopr db=028 di=uq

Servicio de Connx

4. Subimos el servicio del Connx

   Como usuario root: Cd /sti/sag/connx
   Sh connxserver start

5. isoVerificamos el estado.

   Sh connxserver status

Repartidor

1. Una vez arriba los servicios iniciamos el proceso de repartidor.

a. Ingresamos a la base de datos DAFPROD atreves del asistente Navicat o Mysql Management. b. Buscamos la tabla sesiones_contra c. Existe una columna de usuario y sesiones, a cada rango de usuarios se le puede dar una cantidad de sesiones. Se hace de esta manera para ir controlando el flujo de sesiones y no saturar los recursos. Estos valores son regulados por el director y subdirector del departamento de informática.

Tabla 33 Corte de suministro eléctrico

PLAN DE CONTINUIDAD DE SERVIDORES DE BASE DE DATOS **DEPARTAMENTO DE INFORMATICA** **ESTRATEGIA REACTIVA** **CORETE DE SUMINISTRO ELECTRICO**	
Nombre del colaborador : **Fecha:**	ACME_PR03
Escenario: Estrategia reactiva en caso de corte de suministro eléctrico en instalaciones donde se encuentra el Centro de Datos principal.	
PROTOCOLO DE RESTAURACIÓN	**Marque**
Ingreso a las instalaciones del Centro de Datos	
1. Ingresar rápidamente a las instalaciones del Centro de datos. 2. Asegurarse que las UPS entren en funcionamiento. a. Para asegurarse de que entren en funcionamiento, visualizar en el panel de control el estado. b. Tienen que estar en ON	
Funcionamiento del generador de energía	
1. Después de que las UPS, entran en funcionamiento. Hay que esperar 15 segundos para que el generador de energía arranque	

Si el arranque automático del generador falla?
1. Dirigirse rápidamente al cuarto donde se encuentra el generador, para proceder con el encendido manual. 2. Dirigirse al panel de color gris que se encuentra en la pared. a. Abrir el panel de control. b. Presionar el botón rojo. c. Bajar el interruptor número 1. d. Esperar que el generador encienda
Si el estado de combustible es bajo?
1. Verificar el estado del combustible 2. Si el estado es muy bajo llamar al personal encargado al número: 86364916
Regreso de energía a la normalidad
1. Una vez haya regresado la energía comercial, el generador se apagará automáticamente después de 5 minutos. 2. Si el generador no se apaga, realizar el proceso manualmente.
Verificación de regreso de energía comercial
1. Verificamos en los conectores de energía comercial.
Apagado manual del generador
1. Dirigirse rápidamente al cuarto donde se encuentra el generador, para proceder con el encendido manual. 2. Dirigirse al panel de color gris que se encuentra en la pared. a. Abrir el panel de control. b. Presionar el botón verde. c. Subir el interruptor número 1.

Tabla 34 Avería física en el sistema de climatización

PLAN DE CONTINUIDAD DE SERVIDORES DE BASE DE DATOS **DEPARTAMENTO DE INFORMATICA** **ESTRATEGIA REACTIVA** **AVERIA FISICA EN EL SISTEMA DE CLIMATIZACION**	
Nombre del colaborador : **Fecha:**	ACME_PR04
Escenario: Estrategia reactiva en caso de daño del sistema de climatización en el Centro de Datos, llegando a un nivel alto de temperatura y provocando que se apaguen los servidores.	
PROTOCOLO DE RESTAURACIÓN	**Marque**
Ingreso al centro de Datos	
1. Ingresar rápidamente al centro de Datos a. Verificar el estado de las unidades de refrigeración, que se encuentran en el panel frontal de cada unidad. Asegurarse que la unidad está en ON. b. Si no es el caso proceder a encender Manualmente la unidad de refrigeración.	
Si no hacen la sincronización automática	
1. En el panel de control presionar el botón: *Restart* 2. Si el reinicio no funciona y la temperatura es mayor de 40 grados. a. Presionar el botón de mecanismo de escape de aire para sacar todo el aire cliente. **3.** Si el método anterior no funciona, llamar de inmediato a los proveedores que se encargan del buen funcionamiento de las unidades. Se encuentra en la sección de **Datos de los Miembros de los Equipos.**	
Si las unidades de refrigeración no responden	
1. Acceder al VMware vCenter	

a. Entramos desde el navegador web a la dirección URL: https://vcenteracme.acme.com/
b. Seleccionamos la opción de html5
vSphere Client (HTML5)
c. Ingresamos el usuario y contraseña.
Usuario: dominio
Clave: dominio

Proceso de Migración de Máquinas virtual a Centro de Datos Alterno

1. Una vez dentro del VSphere Client
   a. Nos vamos a ***Menu*** y seleccionamos la opción ***Host and Clusters***
   b. Buscamos la máquina virtual con el nombre
   c. Seleccionamos la máquina virtual que queremos migrar.
   Click derecho
   Opcion Migrate
   d. Se abre la ventana de migración
   Seleccionamos la opción **Change both compute resurce and storage**
   Le damos Next
   Seleccionamos el **esx_02centroAlterno**
   Seleccionamos la red
   Le damos Next
   Seleccionamos **Schedule vMotion with high priority (recommended)**

Encendido de servidor o máquina virtual

1. Una vez trasladada la máquina virtual al host del centro de datos Alterno.
   a. Seleccionamos la máquina virtual
   Click derecho
   Nos vamos a la opción de Power ON
   Y esperamos que inicie el sistema operativo.
2. Después procedemos a subir los servicios de base de datos.

Reinicio de servicios

1. Procedemos a ver el estado del servicio de base de datos
   a. Para ver el estado: `service mysql status`
   b. Si el servicio está detenido procedemos a subirlo con el siguiente comando:
   `service mysql start`

c. *Confirmamos de nuevo el estado del servicio*

```
service mysql status
```

Servicio de replicación

1. Ingresamos a Mysql

```
Mysql –u root –p
Clave: *********
```

2. Revisamos el estado de la replicación.

```
SHOW MASTER STATUS;
```

3. Si la replicación no está funcionando procedemos a reiniciar el servicio.

```
STOP SLAVE;
```

4. Le pasmos el archivo binario de la última replicación

```
RESET SLAVE;
CHANGE MASTER TO MASTER_LOG_FILE='mysql-bin.000001’,
MASTER_LOG_POS=98;
```

5. Revisamos el estado de la replicación

```
SHOW MASTER STATUS;
```

6. Si no funciona procedemos a reiniciar el servidor, y posteriormente iniciar en el punto d reinicio del servidor.

Observaciones:

9.3. Plantillas de uso para cierre del plan

Los siguientes activos o elementos deben de ser revisados por los responsables del Plan de Continuidad, con la intención de asegurar que todo esté funcionando bien y de esta manera poder cerrar el plan.

Tabla 35 Inspección de Instalaciones del centro de datos

PLAN DE CONTINUIDAD DE SERVIDORES DE BASE DE DATOS **DEPARTAMENTO DE INFORMATICA** **INSPECCION DE INSTALACIONES DEL CENTRO DE DATOS**	
Responsable: Líder de Apoyo tecnológico, Líder de comunicaciones y Administradores de base de datos.	CODIGO: ACME_PC01
Los siguientes elementos deben de ser revisados por los responsables del plan de continuidad con la intención de cerrar el plan. Marque con un ✓ en cada elemento inspeccionado, en caso de encontrar una anomalía detallarlo en la sección de observaciones. Enviar un reporte al correo reportesd@acme.com.	
ACIONES	
Elementos a inspeccionar	**Marque**
1. Servidores en el centro de datos.	
2. Sistema de climatización del centro de datos.	
3. Sistemas de baterías UPS que alimentan los servidores del centro de datos.	
4. Sistema contra incendios del centro de datos.	
5. Generador de energía.	
Observaciones:	

Tabla 36 Sitios Web y acceso a Información

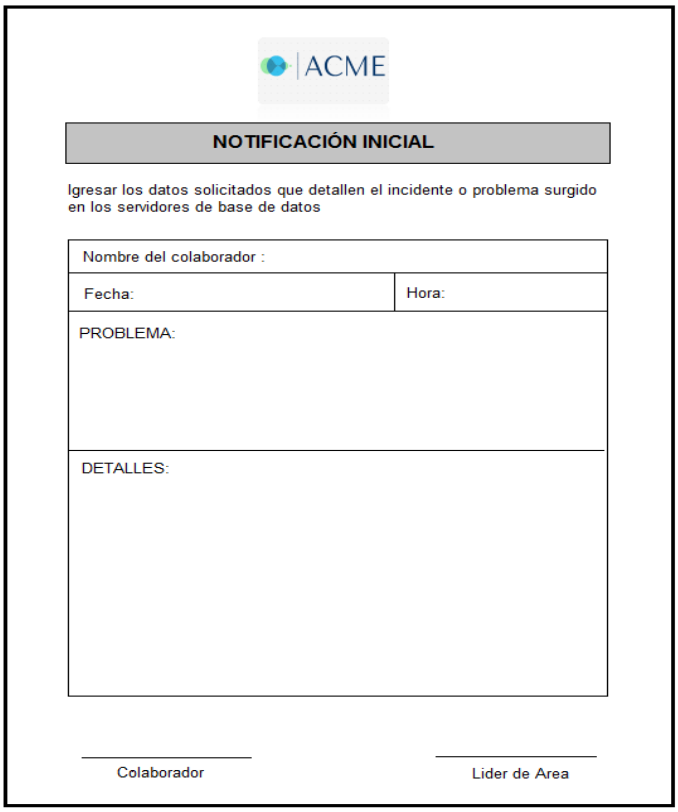
PLAN DE CONTINUIDAD DE SERVIDORES DE BASE DE DATOS **DEPARTAMENTO DE INFORMATICA** **SITIOS WEB Y ACCESO A INFORMACION**	
Responsable: Líder de Apoyo tecnológico, Líder de comunicaciones, Líder de desarrollo y Administradores de base de datos .	CODIGO: ACME_PC02
Los siguientes elementos deben de ser revisados por los responsables del plan de continuidad con la intención de cerrar el plan. Marque con un ✓ en cada elemento inspeccionado, en caso de encontrar una anomalía detallarlo en la sección de observaciones. Enviar un reporte al correo reportesd@acme.com.	
ACIONES	
Elementos a inspeccionar	**Marque**
1. Verificación de repuesta del servidor. Haciendo ping o conectándose directamente al servidor.	
2. Realizar pruebas de conexión a bases de datos que se encuentran alojadas en dicho servidor, este proceso se hace en tanto con el personal de base de datos como con el de desarrollo.	
3. Realizar pruebas de conexión desde los sitios web, este proceso se debe de realizar con usuarios de pruebas destinados únicamente a este propósito.	
4. Realizar pruebas de consultas a diferentes tablas y monitorear el comportamiento del servidor.	
5. Verificar el estado de la replicación de cada uno de los servidores que fueron afectados.	
6. Verificar el estado del firewall que esté funcionando correctamente.	

9.4. Plantillas de gestión

A continuación, se presentan las diferentes plantillas de gestión que permiten documentar información respecto a la notificación inicial, pruebas de copias de seguridad, ventanas de mantenimiento de servidores.

9.4.1. Plantilla de Notificación inicial

Plantilla que se debe rellanar al momento que se detecta un problema o incidente en los servidores de bases de datos.



ACME

NOTIFICACIÓN INICIAL

Igresar los datos solicitados que detallen el incidente o problema surgido en los servidores de base de datos

Nombre del colaborador :	
Fecha:	Hora:
PROBLEMA:	
DETALLES:	

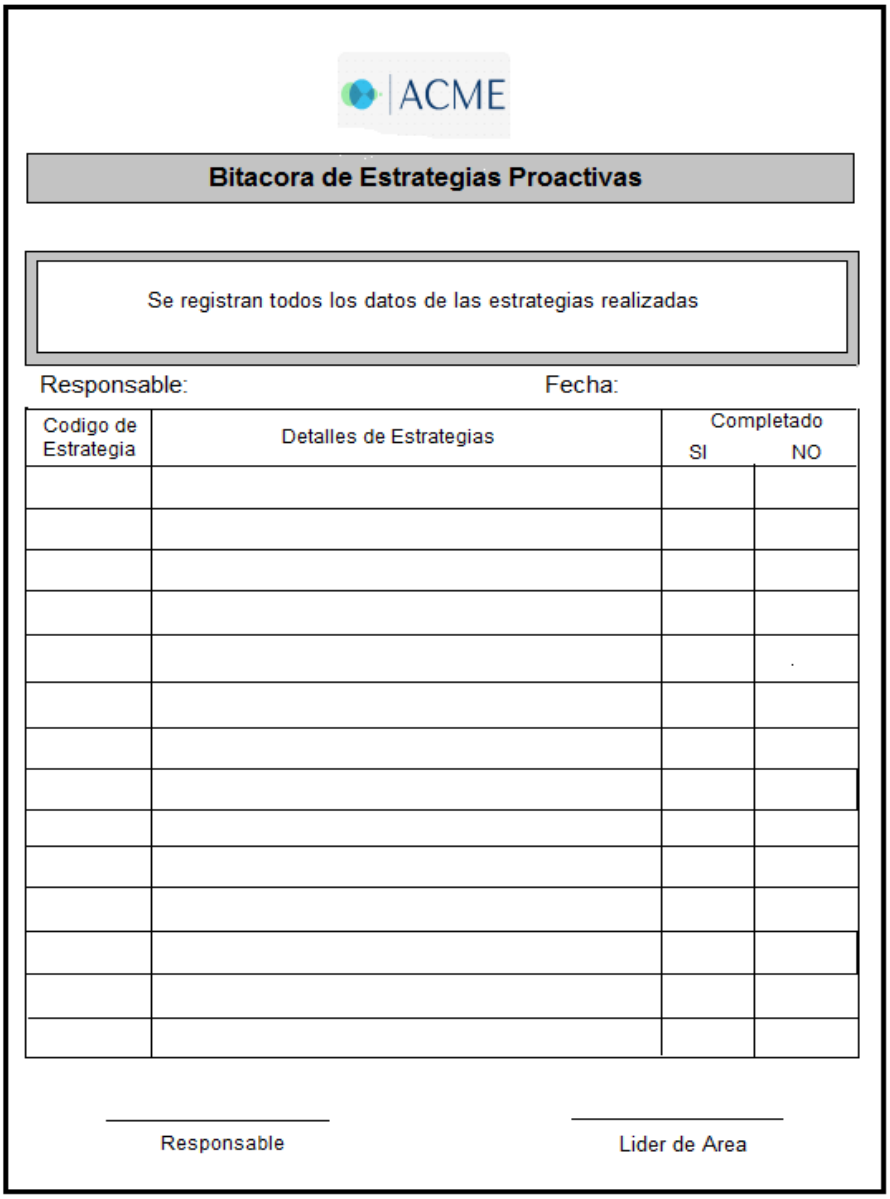
Colaborador

Lider de Area

Ilustración 20: Plantilla de Notificación Inicial

Fuente: Elaboración Propia

9.4.2. Plantillas de bitácoras para procedimientos proactivos



ACME

Bitacora de Estrategias Proactivas

Se registran todos los datos de las estrategias realizadas

Responsable: Fecha:

Codigo de Estrategia	Detalles de Estrategias	Completado SI	NO

Responsable

Lider de Area

Ilustración 21: Bitácora de estrategias proactivas

Fuente: Elaboración Propia

9.4.3. Plantilla de bitácora para procedimientos reactivos

ACME

Bitacora de Estratgias Reactivas

Se registran los datos de las estrategias realizadas

Responsable: Fecha:

Codigo de Estrategia	Detalles de Estrategias	Completado SI	NO

Responsable

Lider de Area

Ilustración 22: Bitácora de estrategias reactivas

Fuente: Elaboración Propia

9.4.4. Plantilla de bitácora para pruebas de copias de seguridad.

PRUEBAS DE COPIAS DE SEGURIDAD
EMPRESA ACME
DEPARTAMENTO DE INFORMÁTICA Y SISTEMAS

INFORMACION DE ACTIVIDAD				
FECHA Y HORA INICIAL		**FECHA Y HORA FINAL**		**DURACION**
Hora de inicio	Fecha de inicio	Hora de finalización	Fecha de finalización	Duración del proceso total de comprobación de la copia de seguridad
IFORMACION DE COPIA DE SEGURIDA O RESPALDO				
TIPO DE RESPALDO		**FECHA DEL RESPALDO**		**DETALLE**
Tipo de respaldo		Se detalla la fecha de creación del respaldo		Detalles de la copia de seguridad
INFORMACION DEL PROCESO				
ACTIVIDADES DE RESTAURACION				
Se detallan cada una de las actividades que se realizaran para llevar acabo del proceso de restauración del respaldo en el servidor de pruebas				
PRUEBAS A REALIZAR		**DEATALLES Y RESULTADOS**		
Se detallan todas las pruebas a realizar		Se detalla cada uno de los resultados de las pruebas realizadas		
DIAGRAMA DE ESTADO				

Ilustración 23: Bitácora para pruebas de copias de seguridad

Fuente: Elaboración Propia

9.4.5. Plantilla de bitácora para Notificación de ventanas de mantenimiento

INFORMACION SOBRE LA ACTIVIDAD EMPRESA ACME DEPARTAMENTO DE INFORMÀTICA Y SISTEMAS				
FECHA Y HORA INICIAL		**FECHA Y HORA FINAL**		**DURACION**
Hora de inicio	Fecha de inicio	Hora de finalización	Fecha de finalización	Duración del mantenimiento en horas
IFORMACION GENERAL DEL SERVIDOR				
NOMBRE		**DIRECCION IP**		**DETALLE**
Nombre del servidor		Dirección ip del servidor		Detalles del servidor
ACTIVIDADES A REALIZAR		**SERVICIOS AFECTADOS**		**BENEFICIOS ESPERADOS**
Se detallan cada una de las actividades que se realizaran		Se detallan los servicios que serán afectados al momento de realizar el mantenimiento		Se detallan los beneficios o que traerá consigo la realización del mantenimiento
NOTAS ADICIONALES				

Ilustración 24: Bitácora de notificación de ventanas de mantenimiento

Fuente: Elaboración Propia

CAPÍTULO V: CONCLUSIONES Y ECOMENDACIONES

5.1. Conclusiones

Resulta imprescindible para todas las organizaciones sin importar su naturaleza contar con un plan de continuidad, el cual permita amortiguar y minimizar los efectos de las amenazas que puedan afectar los activos críticos, así como la reducción de los tiempos de recuperación y restauración

Este estudio muestra una evaluación de la continuidad de negocio en los servidores de bases de datos del departamento de Informática de la empresa ACME.

Mediante el desarrollo del presente trabajo investigativo se resalta que la empresa ACME tiene la oportunidad de mejorar el control de aquellos activos críticos que son operados por su sistema de bases de datos.

A pesar de conocer los riesgos potenciales a los que están expuestos tales como fallas en los servicios, desastres naturales, siniestros, mala praxis e incluso epidemias, la empresa aun no implementa alternativas de solución de continuidad de negocio que mitiguen las amenazan más frecuentes que ponen en riesgo la operatividad.

Se ha concientizado a la empresa ACME sobre alternativas que amortigüen las problemáticas surgidas por su incapacidad de garantizar la continuidad operativa de los sistemas de información al momento de un altercado.

Mediante la aplicación de los controles, se le garantiza a la empresa ACME mantener un nivel aceptable de operación durante y después de caídas en los servicios ocasionadas por y no limitándose a desastres naturales o fallas de seguridad.

Definida la propuesta de mejora, el departamento de informática de la empresa ACME ahora puede tener control sobre aquellas amenazas que ponen en riesgo procesos fundamentales en los servidores de base de datos.

5.2. Recomendaciones

Es necesario que la empresa ACME cubra y rastree los procesos controlados por los servidores de bases de datos que con mayor o menor medida están en riesgo de sufrir interrupciones.

Se debe dar seguimiento a aquellos procesos críticos que fueron catalogados como más vulnerables en el análisis, para así conocer si el grado de aceptación definido en el control llega a alcanzarse.

Establecer y mantener procedimientos de control hacia los nuevos procesos y tareas que se anexen a los servicios de base de datos, para evitar vulnerabilidades ya contempladas.

Mantener una visión de largo plazo que permita modelar posibles escenarios negativos, para así desarrollar estrategias de contingencia.

Establecer y mantener procedimientos para identificar, analizar y actuar sobre los problemas que requieren soluciones inmediatas.

Capacitar al personal responsable de manipular los servidores de base de datos ante situaciones de contingencia y/o crisis para que puedan actuar de manera articulada, eficiente y oportuna.

CAPITULO VI: BIBLIOGRAFÍA

Bernal, J. J. (2017). *pdcahome.* Obtenido de https://www.pdcahome.com/5202/ciclo-pdca/

BSG Institute. (2019). Obtenido de https://bsginstitute.com/bs-campus/blog/Seguridad-de-la-Informacion-20

BSG Institute. (2019). *bsginstitute.com*. Obtenido de bsginstitute.com: https://bsginstitute.com/area/Continuidad-del-Negocio

CCSS. (Noviembre de 2007). *Manual para Elaborar un Plan de Continuidad de la Gestión en Tecnologías de Información y Comunicaciones.* San José.

Cerullo, V. a. (1 de 1 de 2004). Obtenido de https://www.tandfonline.com/doi/abs/10.1201/1078/44432.21.3.20040601/82480.11

datacentric. (s.f.). Obtenido de datacentric: http://www.datacentric.es/blog/bases-datos/importancia-bases-de-datos-2/

El portal de ISO 27000 en Español. (2013). Obtenido de http://www.iso27000.es/iso27002_17.html

Figuerola, N. (04 de 2014). Obtenido de https://articulospm.files.wordpress.com/2014/04/continuidad-del-negocio-y-recuperacic3b3n-de-desastres.pdf

Fiorito, F. (2006). *ucema.edu.ar.* Obtenido de https://ucema.edu.ar/~ffiorito/Handout_Simulacion_y_RISK_06.pdf

Fuentez, S. (28 de 01 de 2014). *eird.org.* Obtenido de eird.org: https://www.eird.org/pr14/formulario/presentaciones/138.pdf

Galileus. (08 de 07 de 2012). *businesscontinuity*. Obtenido de businesscontinuity: http://businesscontinuity-pe.blogspot.com/2012/07/antecedentes-historicos-de-la.html

Gerens Escuela de Postgrado. (2019). *gerens.pe*. Obtenido de gerens.pe: https://gerens.pe/blog/gestion-riesgo-que-por-que-como/

GMS Seguridad de la información. (13 de 02 de 2019). *GMS Seguridad*. Obtenido de https://gmsseguridad.com/continuidad.html

Gonzalez, J. (2018). *steemit*. Obtenido de https://steemit.com/spanish/@jorgegonzalez11/mejora-continua-en-nuestras-vidas-ciclo-pdca

Guzmán, A. (30 de 01 de 2015). *http://repository.unipiloto.edu.co.* Obtenido de http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2955/Trabajo%20de%20grado.pdf?sequence=1

Huércano, S. R. (2020). Obtenido de Obtenido de https://docs.supersalud.gov.co/PortalWeb/planeacion/AdministracionSIG/GSDE01.pdf

Ibercom. (25 de 09 de 2006). *ibercom.com.* Obtenido de ibercom.com: https://twonet.files.wordpress.com/2011/08/sistemas_informticos_redundantes.pdf

INC Web Hosting. (2019). *inc.cl*. Obtenido de inc.cl: https://www.inc.cl/blog/hosting/que-es-la-redundancia-y-cual-es-su-importancia

informaticaparatunegocio. (2019). Obtenido de https://www.informaticaparatunegocio.com/blog/redundancia-datos-seguridad-sistemas/

ISO/IEC 27002. (2013). https://www.iso.org/standard/54533.html.

ISOTools Excellence. (15 de Octubre de 2015). *pmg-ssi*. Obtenido de https://www.pmg-ssi.com/2015/10/iso-22301-2012-sistema-gestion-continuidad-negocio/

La suma de todos. (2012). Análisis y cuantificación del Riesgo. Madrid.

Ludy, G. R. (2013). Obtenido de http://polux.unipiloto.edu.co:8080/00000815.pdf

Martínez, C. N. (11 de 2018). Obtenido de https://repositoriotec.tec.ac.cr/handle/2238/11063

Mendoza, M. Á. (06 de 11 de 2014). *welivesecurity*. Obtenido de https://www.welivesecurity.com/la-es/2014/11/06/business-impact-analysis-bia/

microsoft. (23 de Abril de 2019). *microsoft.* Obtenido de https://docs.microsoft.com/es-mx/sql/database-engine/availability-groups/windows/always-on-availability-groups-sql-server?view=sql-server-ver15

Mieles, T. T. (14 de 02 de 2020). Obtenido de http://www.dspace.espol.edu.ec/bitstream/123456789/16711/2/Tesina%20BCP%20FINAL.pdf

National Institute of Standards and Technology. (Mayo de 2010). Contingency Planning Guide for Federal Information Systems. Estados Unidos. Obtenido de https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

PAE. (Octubre de 2012). *Portal de Administración Electrónica.* Obtenido de https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Pandini, W. (20 de 1 de 2019). *ostec.blog*. Obtenido de ostec.blog: https://ostec.blog/es/generico/iso-27002-buenas-practicas-gsi

Puricica, C. A. (03 de 05 de 2018). *veeam*. Obtenido de veeam: https://www.veeam.com/blog/es-lat/rto-rpo-definitions-values-common-practice.html

Quálitas. (06 de 2016). ESTRATEGIAS DE CONTINUIDAD DE NEGOCIO.

Quevedo, J. (2012). Obtenido de https://pdfs.semanticscholar.org/8580/6386da6194e7053ddb1f7948f6ca1f569098.pdf

Raffino, M. E. (19 de 04 de 2019). *consepto.de*. Obtenido de consepto.de: https://concepto.de/gestion-de-riesgos/

Rivero, D. S. (2008). *Introducción a la Metodología de la Investigación.* Editorial Shalom 2008.

Rouse, M. (21 de 12 de 2018). *techtarget*. Obtenido de https://searchsqlserver.techtarget.com/definition/database

scprogress. (2017). Obtenido de https://www.scprogress.com/NOTICIAS/CyberNoticia47-20170824.pdf

Secureit. (2020). *securyit*. Obtenido de https://www.secureit.es/procesos-y-gobierno-it/continuidad-de-negocio/

SGSI. (3 de 08 de 2017). Obtenido de https://www.pmg-ssi.com/2017/08/norma-iso-27002-politica-seguridad/

Soldano, A. (20 de 03 de 2009). Obtenido de http://www.rimd.org/advf/documentos/4921a2bfbe57f2.37678682.pdf

Soldano, A. (2009). *Conceptos sobre Riesgos.* Cordoba.

Tecon Soluciones Informáticas. (2019). *tecon.es*. Obtenido de tecon.es: https://www.tecon.es/la-seguridad-de-la-informacion/

uv. (s.f.). Obtenido de https://www.uv.mx/celulaode/seguridad-info/tema1.html

valoradata. (13 de 02 de 2020). *valoradata*. Obtenido de valoradata: https://www.valoradata.com/blog/impacto-desastres-naturales-organizaciones/

Yomayuza, M. (21 de 11 de 2018). *repository.unipiloto.edu.co.* Obtenido de repository.unipiloto.edu.co: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/4635/00004908.pdf?sequence=1&isAllowed=y

Zumba, F. A. (2015). Obtenido de http://dspace.ucuenca.edu.ec/handle/123456789/22342

Glosario de términos

Adabas: es una base de datos de lista invertida de alto rendimiento creada por la empresa alemana Software AG, en el año 1969.

Amenazas: son todas aquellas cosas que le pueden suceder a los activos que se salen de la normalidad.

Vulnerabilidad: debilidad en activos que pueden ser aprovechadas por amenazas para dañar a un activo (son los agujeros de seguridad).

Impacto: consecuencia de la materialización de una amenaza sobre un activo.

UBDSO: Unidad de Base de Datos y Sistemas Operativos.

Respaldo: es una copia de seguridad de la información.

Centro de datos: espacio donde se concentran los recursos necesarios para el procesamiento de información de una organización.

TIC: Tecnologías de la Información y Comunicación, es el hardware y software que automatizan la recolección, procesamiento, distribución, almacenamiento y consulta de datos.

Replicación: proceso de copiar y mantener actualizado los datos en varios modos de base de datos ya sean estos persistentes o no.

Saturación: ocupar un servicio hasta el límite de su capacidad.

Escalabilidad: capacidad de crecimiento de la computadora.

Firewall: conjunto de programas de protección y dispositivos especiales que ponen barreras al acceso exterior a una determinada red privada.

Hardware componente físico de la computadora.

Software: Componentes intangibles (programas) de las computadoras.

LAN: (Local área network) Red de computadoras interconectadas, distribuida en la superficie de una sola oficina o edificio

Log: Archivo que registra movimientos y actividades de un determinado programa. Utilizado como mecanismo de control y estadística.

CAPITULO VII: Anexos

7.1. Anexo 1: Monitoreo Automático (Nagios)

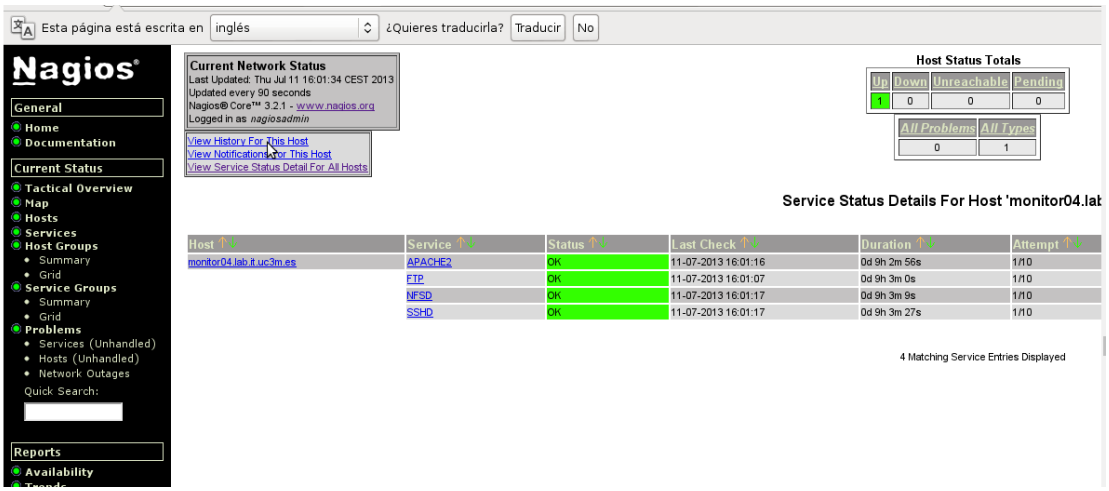


Ilustración 25: Pantalla principal del sistema de monitoreo Nagios

Fuente: Empresa ACME

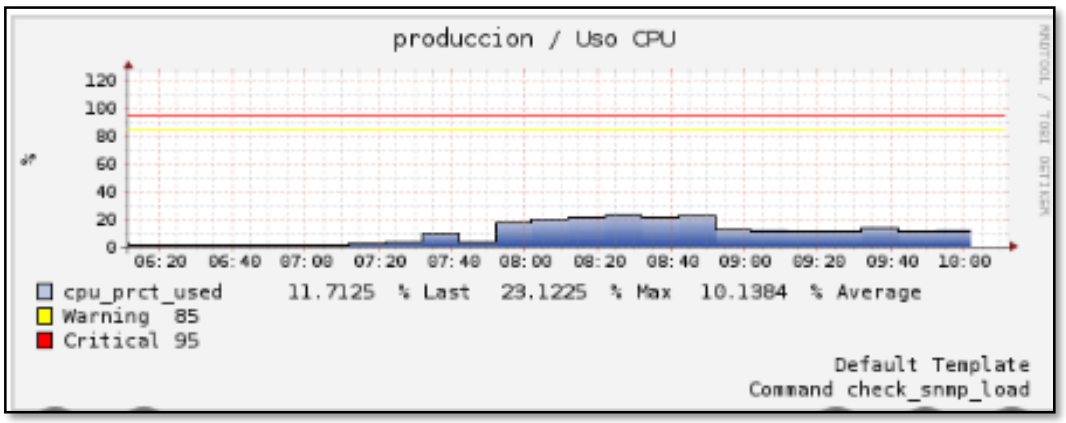


Ilustración 26: Grafía de monitoreo Nagios, uso del CPU de los servidores

Fuente: Empresa ACME

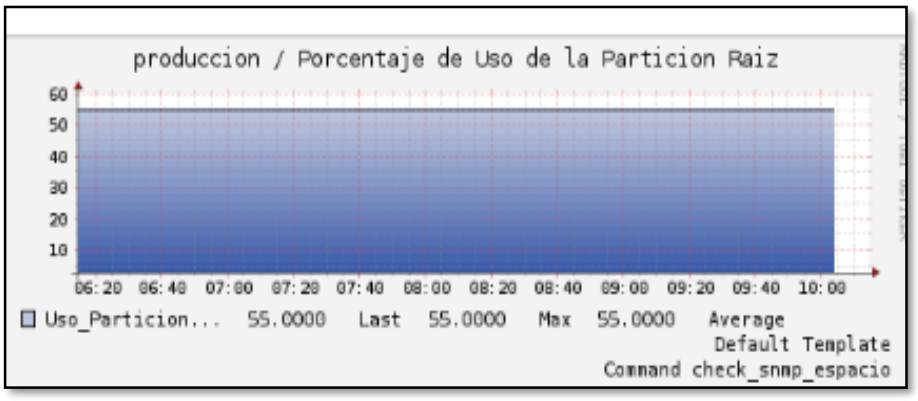


Ilustración 27: Grafía de monitoreo Nagios, porcentaje de particiones

Fuente: Empresa ACME

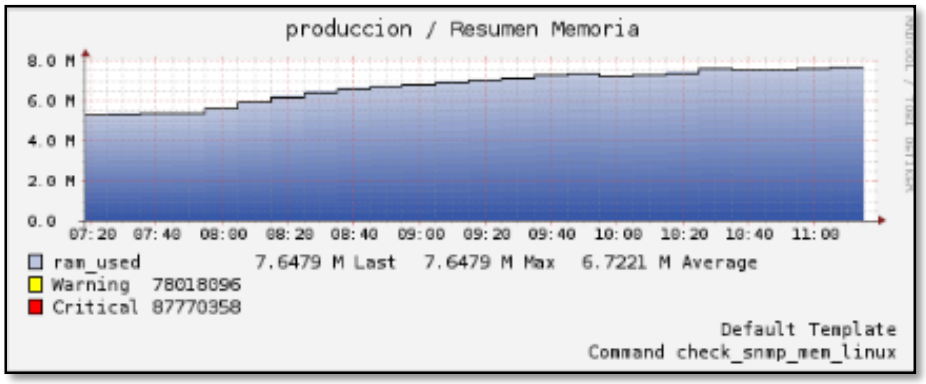
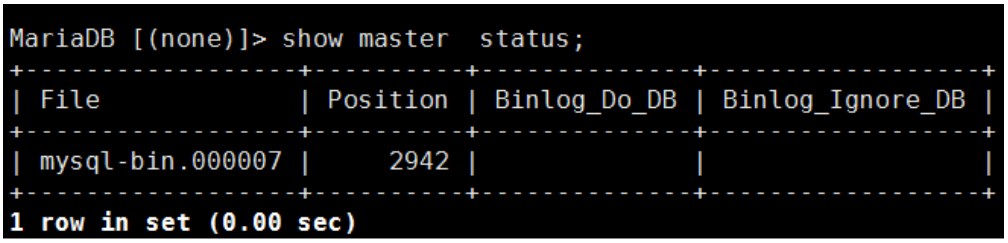


Ilustración 28: Grafía de monitoreo, uso de memoria en los servidores

Fuente: Empresa ACME

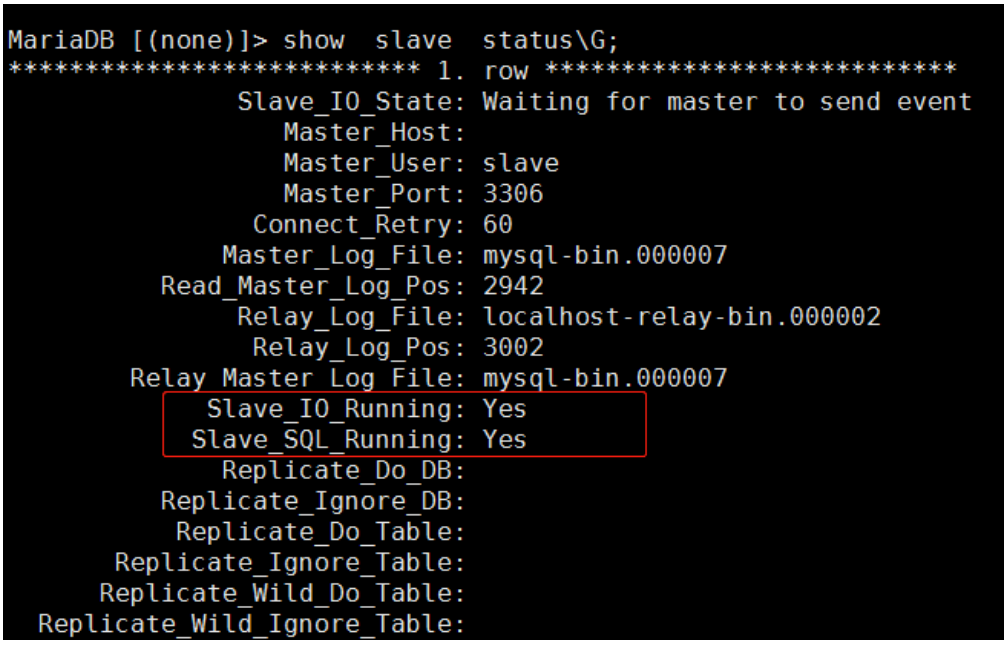
7.2. Anexo 2: Monitoreo Manual de Servidores



```
MariaDB [(none)]> show master  status;
+------------------+----------+--------------+------------------+
| File             | Position | Binlog_Do_DB | Binlog_Ignore_DB |
+------------------+----------+--------------+------------------+
| mysql-bin.000007 |     2942 |              |                  |
+------------------+----------+--------------+------------------+
1 row in set (0.00 sec)
```

Ilustración 29: Evidencia de replicación de base de datos productiva

Fuente: Empresa ACME



```
MariaDB [(none)]> show  slave  status\G;
*************************** 1. row ***************************
               Slave_IO_State: Waiting for master to send event
                  Master_Host:
                  Master_User: slave
                  Master_Port: 3306
                Connect_Retry: 60
              Master_Log_File: mysql-bin.000007
          Read_Master_Log_Pos: 2942
               Relay_Log_File: localhost-relay-bin.000002
                Relay_Log_Pos: 3002
        Relay_Master_Log_File: mysql-bin.000007
             Slave_IO_Running: Yes
            Slave_SQL_Running: Yes
              Replicate_Do_DB:
          Replicate_Ignore_DB:
           Replicate_Do_Table:
       Replicate_Ignore_Table:
      Replicate_Wild_Do_Table:
  Replicate_Wild_Ignore_Table:
```

Ilustración 30: Evidencia del estado de replicación en el servidor esclavo

Fuente: Empresa ACME

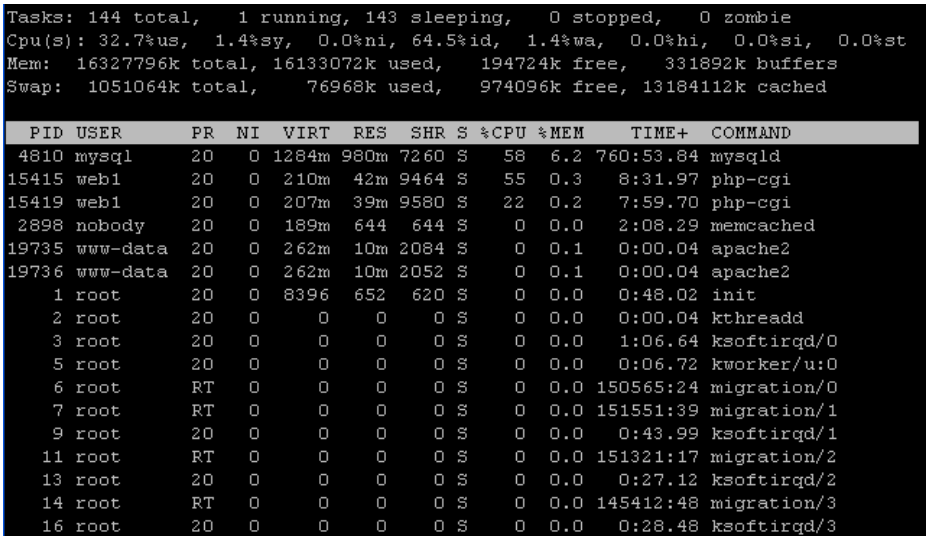


Ilustración 31: Monitoreo manual de recursos de servidores Linux

Fuente: Empresa ACME

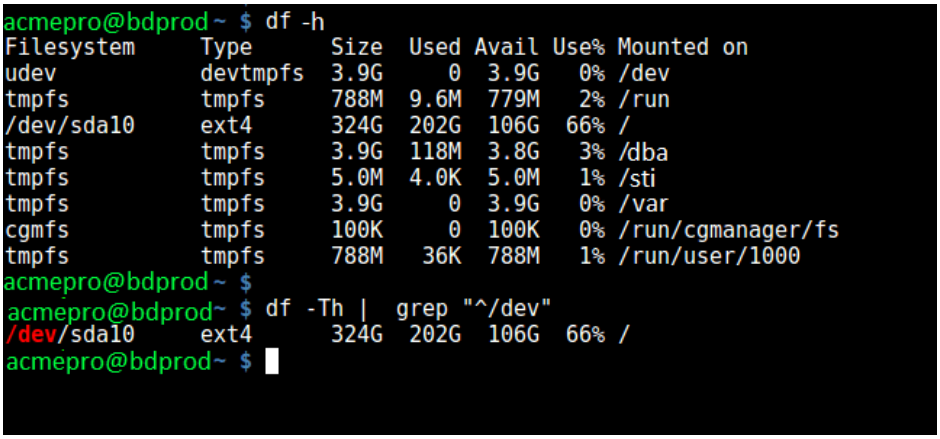


Ilustración 32: Verificación manual de partición en servidores Linux

Fuente: Empresa ACME

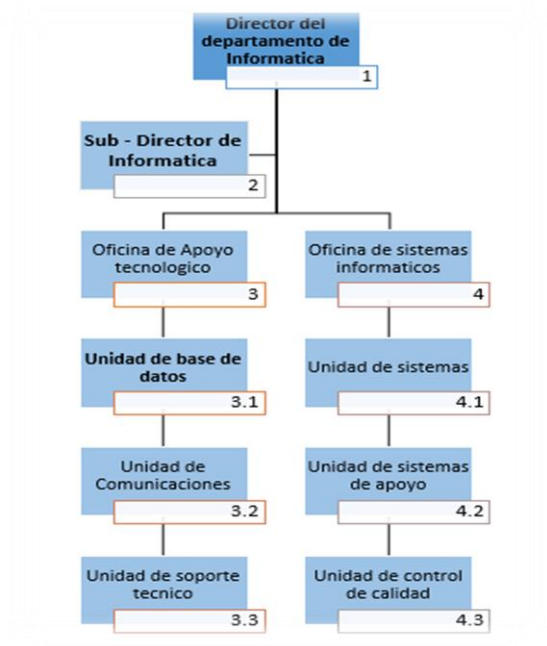


Ilustración 33: Organigrama Departamento de Informática

Fuente: Empresa ACME

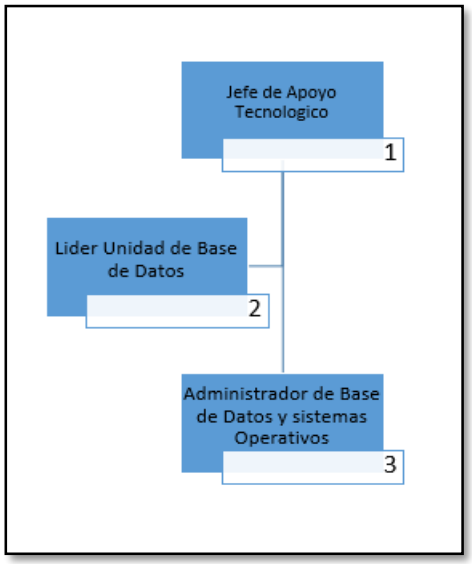


Ilustración 34: Unidad de bases de datos

Fuente: Empresa ACME

Control general

Nombre Dir	Tamaño	Fecha	Direccion IP	Existe / Mov	Dba /Responsable	Verificado por	Fecha verif	Ubicación de los archivos	Observaciones
NombreDirectorio	81M	31/8/2017	DirecionIP	Existe	RaulGomez	Jose Garcia	1/9/2017	Ubicación en servidor de respaldo	Ninguna
NombreDirectorio	7,1G	31/8/2017	DirecionIP	Existe	RaulGomez	Jose Garcia	1/9/2017	Ubicación en servidor de respaldo	Ninguna
NombreDirectorio	137M	31/8/2017	DirecionIP	Existe	RaulGomez	Jose Garcia	1/9/2017	Ubicación en servidor de respaldo	Ninguna
NombreDirectorio	1021M	31/8/2017	DirecionIP	Existe	RaulGomez	Jose Garcia	1/9/2017	Ubicación en servidor de respaldo	Ninguna
NombreDirectorio	247M	31/8/2017	DirecionIP	Existe	RaulGomez	Jose Garcia	1/9/2017	Ubicación en servidor de respaldo	Ninguna
NombreDirectorio	4,0K	31/8/2017	[redacted]	Existe	RaulGomez	Jose Garcia	1/9/2017	Ubicación en servidor de respaldo	Ninguna
NombreDirectorio	106G	31/8/2017	DirecionIP	Existe	RaulGomez	Jose Garcia	1/9/2017	Ubicación en servidor de respaldo	Ninguna
NombreDirectorio	15G	31/8/2017	DirecionIP	Existe	RaulGomez	Jose Garcia	1/9/2017	Ubicación en servidor de respaldo	Ninguna
NombreDirectorio	43M	31/8/2017	DirecionIP	Existe	RaulGomez	Jose Garcia	1/9/2017	Ubicación en servidor de respaldo	Ninguna
NombreDirectorio	6,4G	31/8/2017	DirecionIP	Existe	RaulGomez	Jose Garcia	1/9/2017	Ubicación en servidor de respaldo	Ninguna
NombreDirectorio	9,7G	31/8/2017	DirecionIP	Existe	RaulGomez	Jose Garcia	1/9/2017	Ubicación en servidor de respaldo	Ninguna
NombreDirectorio	2,3G	31/8/2017	DirecionIP	Existe	RaulGomez	Jose Garcia	1/9/2017	Ubicación en servidor de respaldo	Ninguna
NombreDirectorio	4,0K	31/8/2017	DirecionIP	Existe	RaulGomez	Jose Garcia	1/9/2017	Ubicación en servidor de respaldo	Ninguna
NombreDirectorio	5,3M	31/8/2017	DirecionIP	Existe	RaulGomez	Jose Garcia	1/9/2017	Ubicación en servidor de respaldo	Ninguna
NombreDirectorio	61M	31/8/2017	DirecionIP	Existe	RaulGomez	Jose Garcia	1/9/2017	Ubicación en servidor de respaldo	Ninguna
NombreDirectorio	5,8M	31/8/2017	DirecionIP	Existe	RaulGomez	Jose Garcia	1/9/2017	Ubicación en servidor de respaldo	Ninguna
NombreDirectorio	4,0K	31/8/2017	DirecionIP	Existe	RaulGomez	Jose Garcia	1/9/2017	Ubicación en servidor de respaldo	Ninguna
NombreDirectorio	4,0K	31/8/2017	DirecionIP	Existe	RaulGomez	Jose Garcia	1/9/2017	Ubicación en servidor de respaldo	Ninguna
NombreDirectorio	583M	31/8/2017	DirecionIP	Existe	RaulGomez	Jose Garcia	1/9/2017	Ubicación en servidor de respaldo	Ninguna
NombreDirectorio	7M	31/8/2017	DirecionIP	Existe	RaulGomez	Jose Garcia	1/9/2017	Ubicación en servidor de respaldo	Ninguna
NombreDirectorio	2,4G	31/8/2017	DirecionIP	Existe	RaulGomez	Jose Garcia	1/9/2017	Ubicación en servidor de respaldo	Ninguna
NombreDirectorio	17M	31/8/2017	DirecionIP	Existe	RaulGomez	Jose Garcia	1/9/2017	Ubicación en servidor de respaldo	Ninguna
NombreDirectorio	4,0K	31/8/2017	DirecionIP	Existe	RaulGomez	Jose Garcia	1/9/2017	Ubicación en servidor de respaldo	Ninguna
NombreDirectorio	1,8G	31/8/2017	DirecionIP	Existe	RaulGomez	Jose Garcia	1/9/2017	Ubicación en servidor de respaldo	Ninguna
NombreDirectorio	27M	31/8/2017	DirecionIP	Existe	RaulGomez	Jose Garcia	1/9/2017	Ubicación en servidor de respaldo	Ninguna
NombreDirectorio	4,0K	31/8/2017	DirecionIP	Existe	RaulGomez	Jose Garcia	1/9/2017	Ubicación en servidor de respaldo	Ninguna
NombreDirectorio	595M	31/8/2017	DirecionIP	Existe	RaulGomez	Jose Garcia	1/9/2017	Ubicación en servidor de respaldo	Ninguna
NombreDirectorio	298M	31/8/2017	DirecionIP	Existe	RaulGomez	Jose Garcia	1/9/2017	Ubicación en servidor de respaldo	Ninguna

Ilustración 35: Formato de Reporte diario de Respaldos

Fuente: Empresa ACME

7.3. Anexo 3: Entrevista a Líder de apoyo tecnológico

Para ayudar a identificar fácilmente los resultados obtenidos en el departamento de informática en cuanto a la administración de los sistemas de bases de datos se realizó una entrevista, como se muestra a continuación.

1. **¿Qué motores de base de datos usa actualmente la empresa para la gestión de su información?**

R= **E**n el siguiente grafico se puede comprobar los distintos motores utilizados por la empresa, sobresaliendo el motor de Mysql MariaDB, este motor es donde la mayor parte de bases de datos están creadas.

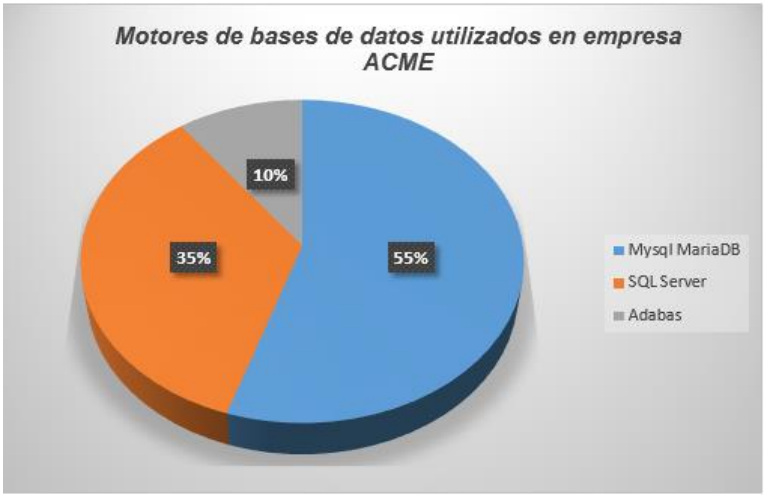


Ilustración 36: Repuesta #1 de la Entrevista

2. **¿Sobre qué sistemas se ejecutan los motores de bases de datos?**

R = La mayor parte de los motores de base de datos de la empresa se ejecutan en el sistema GNU/Linux y la otra parte en Microsoft Windows.

Ilustración 37: Repuesta #2 de la Entrevista

3. **¿Cuál es el tipo de mantenimiento más usado en los servidores de bases de datos?**

R = En el siguiente grafico se aprecia que los mantenimientos no planificados son los que tienen mayor porcentaje, la mayoría de las ocasiones se realizan mantenimientos por algún problema que ocurre en los sistemas o servidores.

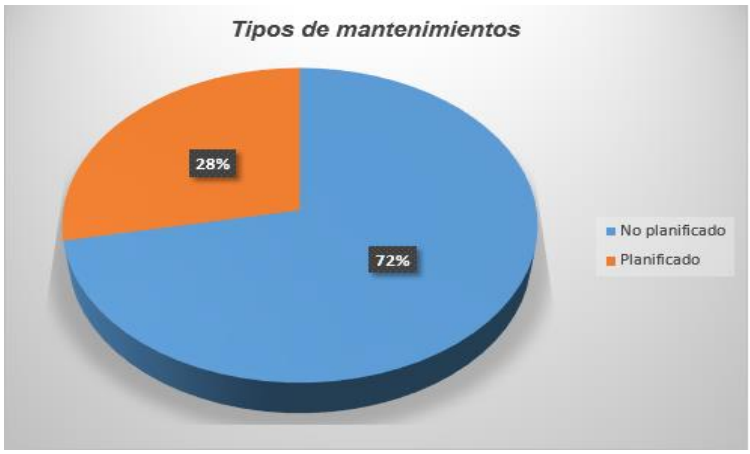


Ilustración 38: Respuesta # 3 de la Entrevista

4. **¿En qué porcentaje puede calificar el control de los permisos de usuarios a las bases de datos?**

R = En el siguiente grafico se aprecia que en un 80% por ciento se controlan los permisos que solicitan los usuarios desarrolladores, pero hay un 20% por ciento que no se controlan adecuadamente.

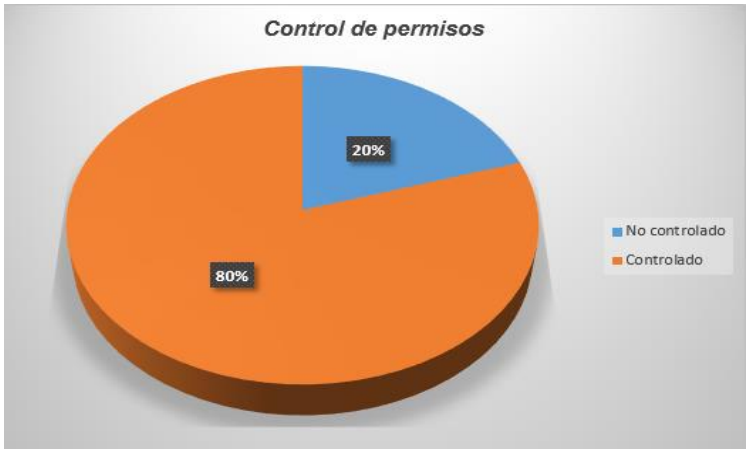


Ilustración 39: Repuesta #4 de la Entrevista

5. **¿En qué porcentaje puede clasificar la verificación de los respaldos de las bases de datos?**

R = En el siguiente grafico se aprecia que en un 30% por ciento se realiza la verificación de los respaldos de las bases de datos, sin embargo, hay un 70% que no se realiza adecuadamente una verificación de integridad de los respaldos.

Ilustración 40: Repuesta #5 de la Entrevista

6. **¿Cuáles son los tipos de monitoreo que realizan a los servidores de base de datos?**

R = ACME cuenta con la herramienta de monitorización que vigila los equipos de (hardware) y servicios de (software).

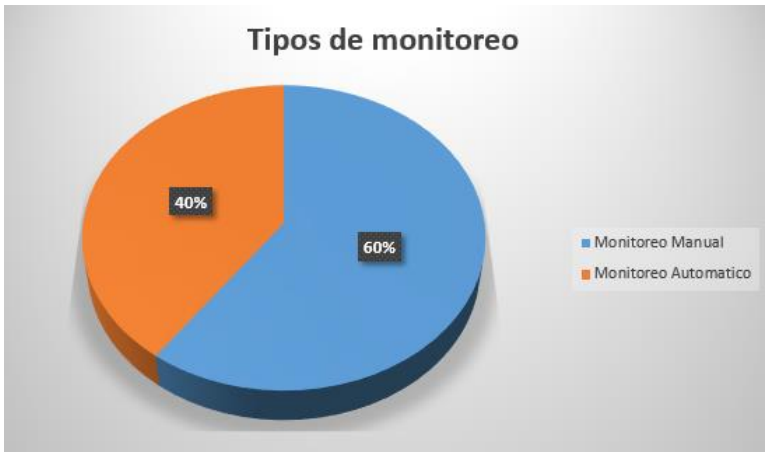


Ilustración 41: Repuesta #6 de la Entrevista

7. **¿En qué porcentaje puede clasificar la alta disponibilidad a nivel de base de datos en los sistemas de la empresa ACME?**

R = No existe una solución de alta disponibilidad para ayudar a mitigar el tiempo de repuesta en caso de algún incidente.

Ilustración 42: Repuesta #7 de la Entrevista

8. **¿Qué porcentaje de bases de datos productivas hacen uso de la tecnología de replicación?**

R = Existe un 60 por ciento de sistemas de bases de datos que implementan la replicación de esquemas y datos, esta replicación no se considera como una tecnología de alta disponibilidad ya que las réplicas son utilizadas únicamente para hacer consultas y evitar cargar el servidor productivo.

Ilustración 43: Repuesta #8 de Entrevista

9. **¿El procedimiento para copias de seguridad y restauración de los sistemas de bases de datos se encuentra documentado?**

R = Actualmente el proceso de copias de seguridad de las bases de datos de la empresa ACME no se encuentra documentado.

Ilustración 44: Repuesta #9 de la Entrevista

10. ¿Se envían copias de seguridad a un lugar externo de la Empresa?

R = Actualmente las copias de seguridad de las bases de datos productivas se envían a otro sitio fuera del departamento de informáticas.

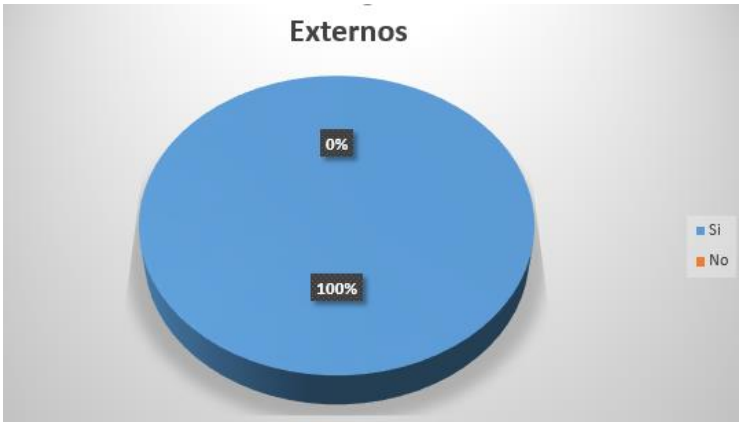


Ilustración 45: Repuesta #10 de la Entrevista

11. ¿Las copias de seguridad de los servidores de base de datos son encriptados para ser trasladados?

R = Actualmente las copias de seguridad de las bases de datos productivas no cuentan con un mecanismo de encriptación en caso de algún robo.

Ilustración 46: Repuesta #11 de la Entrevista

Nivel de probabilidad		DESCRIPCIÓN
Nivel	Valor	
Muy probable	10	Es probable que ocurra un evento de esta naturaleza en un periodo de 3 meses.
Probable	7	El evento ocurrirá en algún momento en un periodo de 3 a 6 meses
Moderado	5	El evento ocurrirá en algún momento en un periodo de 6 meses a un año.
Poco probable	3	Es poco probable que el evento suceda, pero podría ocurrir en algún momento de un periodo de 1 a 2 años.
Muy poco probable	1	Es muy poco probable que el evento se presente en un periodo de dos años.

Ilustración 47: Niveles de probabilidad

Fuente: Elaboración Propia

Niveles de Impacto		DESCRIPCIÓN
Nivel	Valor	
Critico	10	El evento provoca una interrupción completa de los servicios de bases de datos en el departamento de informática de la empresa ACME.
Significativo	7	El evento provoca una interrupción entre parcial y completa de los servicios de bases de datos en el departamento de informática de la empresa ACME.
Moderado	5	El evento provoca una interrupción en los servicios. Las actividades críticas se ven afectadas.
Menor	3	El evento provoca un impacto leve en las operaciones del Departamento de informática, sin generar interrupciones.
Insignificante	1	El evento no provoca impacto en los procesos. La interrupción de los servicios de base de datos afecta a uno o algunos usuarios, pero no dura lo suficiente para provocar un impacto en sus procesos.

Ilustración 48: Niveles de Impacto

Fuente: Elaboración Propia

ACME Análisis de Riesgo

Impacto

El impacto mide el nivel de daño provocado una vez manifestado el riesgo, con el objetivo de realizar dicha medición se definen los siguientes niveles.

Niveles de impacto

Niveles de Impacto		DESCRIPCIÓN
Nivel	Valor	
Crítico	10	El evento provoca una interrupción completa de los servicios de bases de datos en el departamento de informática de la empresa ACME.
Significativo	7	El evento provoca una interrupción entre parcial y completa de los servicios de bases de datos en el departamento de informática de la empresa ACME.
Moderado	5	El evento provoca una interrupción en los servicios. Las actividades críticas se ven afectadas.
Menor	3	El evento provoca un impacto leve en las operaciones del Departamento de informática, sin generar interrupciones.
Insignificante	1	El evento no provoca impacto en los procesos. La interrupción de los servicios de base de datos afecta a uno o algunos usuarios, pero no dura lo suficiente para provocar un impacto en sus procesos.

ACTIVO DE DATOS

[backup] Copias de seguridad de base de datos
[conf] Copias de seguridad de datos de configuración
[acl] Datos de control de acceso
[log] Registro de actividad

	1	3	5	7	10
Errores de Administrador	○	○	○	◉	○
Destrucción de la información	○	○	○	◉	○
Acceso no autorizado	○	○	◉	○	○
Abuso de privilegios	○	○	◉	○	○
Modificación deliberada de la información	○	○	○	◉	○

Abuso de privilegio de acceso	○	○	○	◉	○

Equipamiento Informático (Hardware)

[sbd] Servidores de Base de datos
[backup] Equipamiento de respaldo
[switch] Conmutadores
[routers] Encaminadores
[firewall] Cortafuegos

	1	3	5	7	10
Fuego	○	○	○	○	◉
Daño por agua	○	○	○	○	◉
Avería de origen Físico	○	○	○	○	◉
Errores de mantenimiento / Actualización de equipos hardware	○	○	○	◉	○
Caída del sistema por agotamiento de recursos	○	○	○	○	◉
Caída del sistema por espacio insuficiente en la partición de datos	○	○	○	○	◉

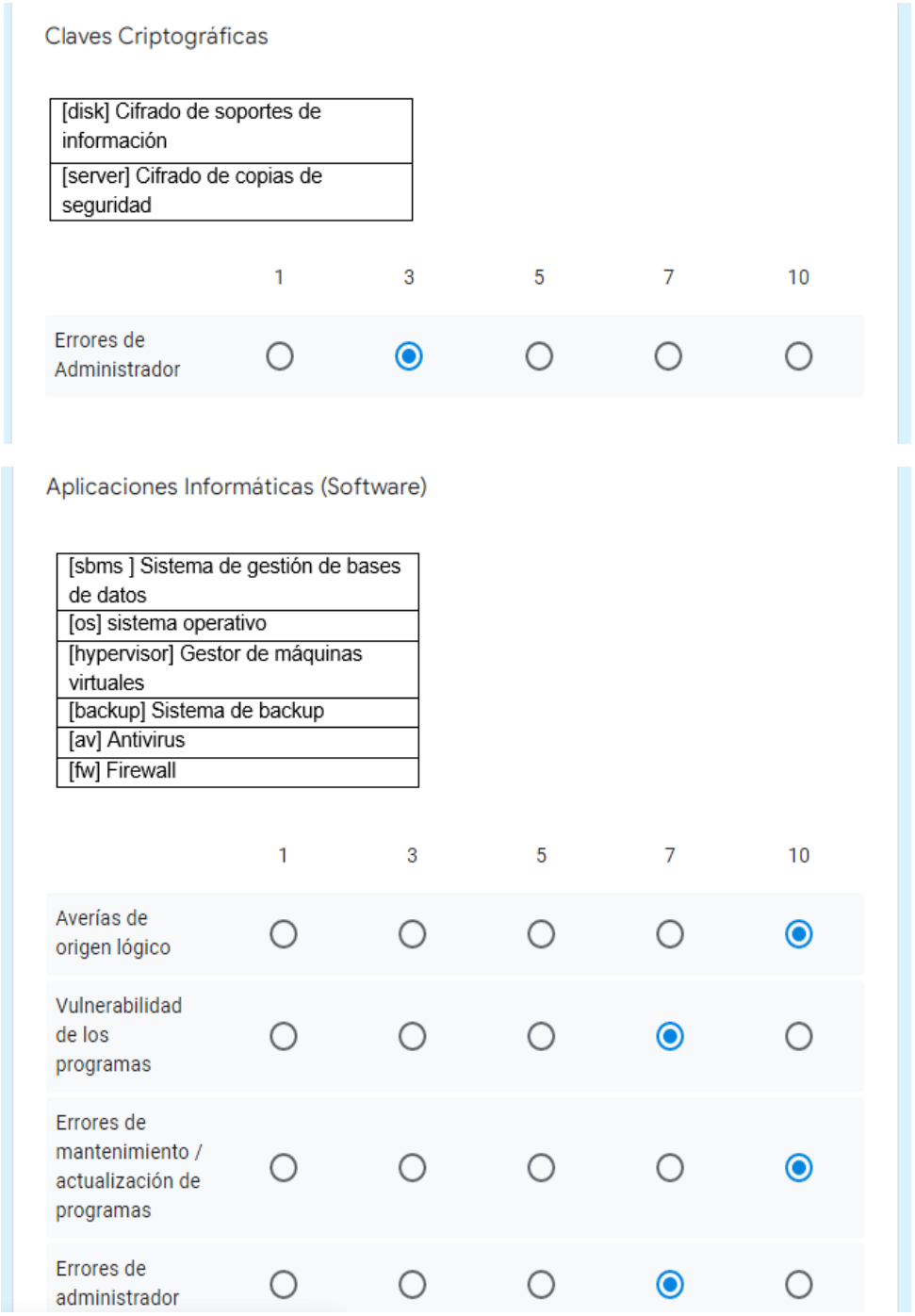


Ilustración 49: Formulario aplicado al área de BD, para medir el Impacto

Fuente: Elaboración propia, Google Forms

ACME Análisis de Riesgo

Probabilidad.

La probabilidad mide la capacidad de ocurrencia del riesgo en el tiempo, con el objetivo de realizar dicha medición, se definen los siguientes niveles.

Niveles de probabilidad

Nivel de probabilidad		DESCRIPCIÓN
Nivel	Valor	
Muy probable	10	Es probable que ocurra un evento de esta naturaleza en un periodo de 3 meses.
Probable	7	El evento ocurrirá en algún momento en un periodo de 3 a 6 meses
Moderado	5	El evento ocurrirá en algún momento en un periodo de 6 meses a un año.
Poco probable	3	Es poco probable que el evento suceda, pero podría ocurrir en algún momento de un periodo de 1 a 2 años.
Muy poco probable	1	Es muy poco probable que el evento se presente en un periodo de dos años.

ACTIVO DE DATOS

[backup] Copias de seguridad de base de datos
[conf] Copias de seguridad de datos de configuración
[acl] Datos de control de acceso
[log] Registro de actividad

	1	3	5	7	10
Errores de Administrador	○	○	◉	○	○
Destrucción de la información	◉	○	○	○	○
Acceso no autorizado	○	○	◉	○	○
Abuso de privilegios	○	○	◉	○	○
Modificación deliberada de la información	◉	○	○	○	○

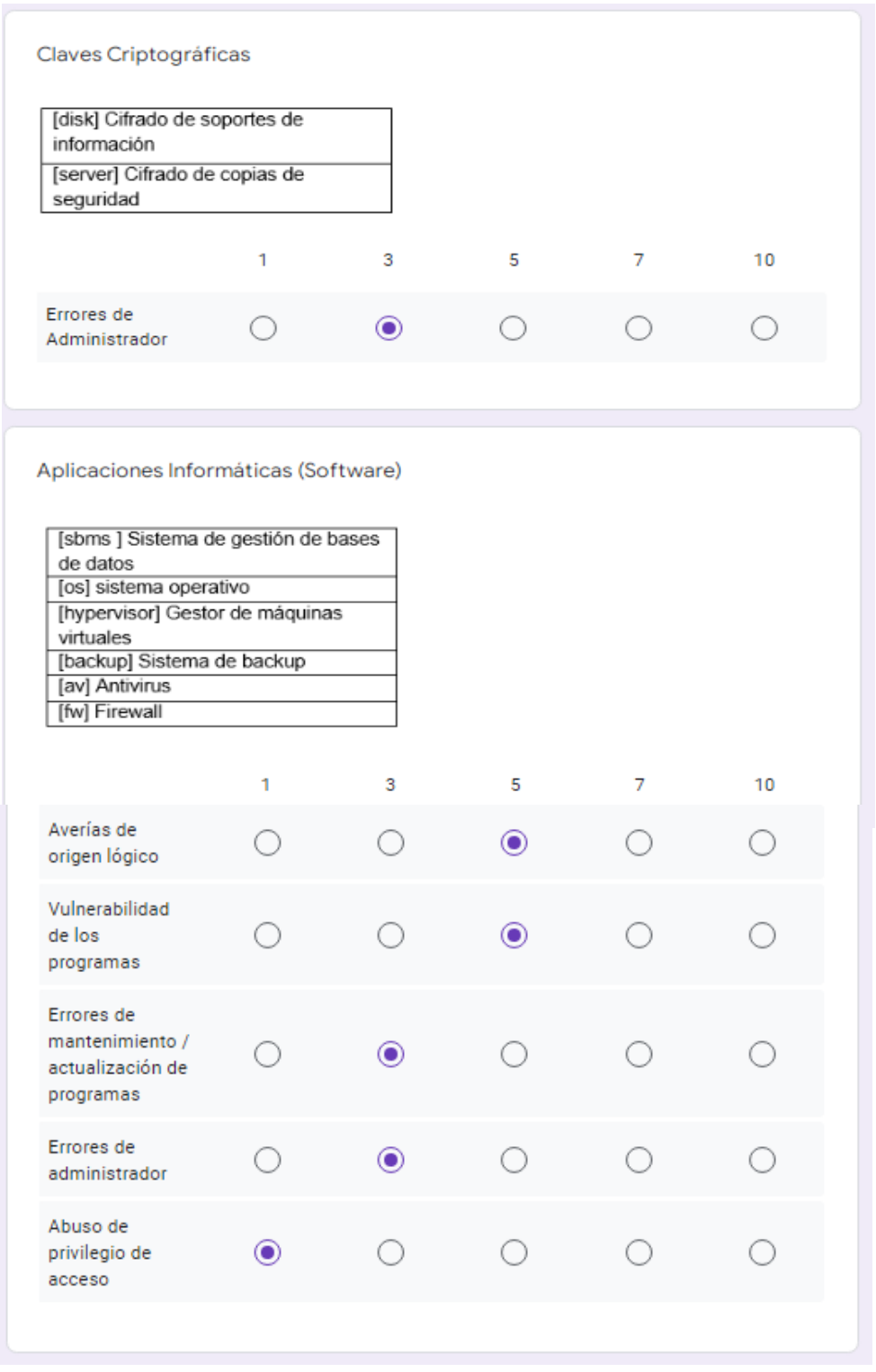


Ilustración 50: Formulario aplicado al área de BD, para medir la probabilidad.

Fuente: Elaboración propia, Google Forms