UNIVERSIDAD TECNOLÓGICA ISRAEL

Maestría en Telemática, mención Calidad en el Servicio.

Tema:

Plan de recuperación de desastres de la Infraestructura de Tecnologías de Información, para empresas de prestación de servicios tecnológicos.

Autor:

Jaime Santiago Cajamarca Yunga

Tutor:

Pablo. M Recalde Varela. MSc. Ing.

Quito, marzo del 2019

AGRADECIMIENTO

A Dios por la salud y vida; por ser mi guía a lo largo de toda mi carrera y por brindarme fortaleza y sabiduría para culminar con mis proyectos.

A mis padres María y Luis por apoyarme en todo momento e inculcarme buenos valores que más que ser un buen profesional me han guiado a ser una buena persona, por su sacrificio para darme la educación durante toda mi carrera.

A mis hermanos, sobrinos y cuñados que con sus características individuales hemos logrado complementarnos para con unión familiar fortalecernos y apoyarnos unos a otros.

RESUMEN

El trabajo de investigación propone un marco de referencia para implementación de un plan de recuperación ante desastres de una empresa de cualquier tipo en el Ecuador, su implementación hace énfasis a empresas del área de soluciones tecnológicas, en la misma se dan a conocer las principales directrices y estándares internacionales como la ISO 22301 y siguiendo las mejores prácticas recomendadas por los fabricantes líderes en el área de tecnología con mejor calificación dentro del cuadrante de Gartner.

Se parte de una visión conceptual en la que topamos tópicos referentes a sistemas y estándares del plan de continuidad de negocios y plan de recuperación de desastres, mismo que servirán de guía para la implementación de los mecanismos de recuperación de errores y caídas de sistemas, así como verificación de métodos de alta disponibilidad de aplicaciones y sistemas.

La metodología utilizada propone los lineamientos y procesos a seguirse y cómo actuar frente a la incidencia de un desastre, propone el plan a seguirse para recuperación y puesta nuevamente a producción de cada sistema; un aspecto importante dentro de esta fase es llegar a un conocimiento de pleno la infraestructura existe, conocer su estado actual y sus falencias lo que permitirá estar preparados ante un evento catastrófico.

En base a los resultados obtenidos, se implementa una guía del plan de recuperación de errores como un caso de implementación práctico aplicado a una empresa de soluciones tecnológicas del Ecuador, cuyos resultados fueron satisfactorios, pues al contar con un plan de recuperación de desastres a más de generar tranquilidad para todo el personal, al saber que cuentan con un nivel de protección ante cualquier incidente también genera valor a nivel de las empresas de la competencia, pues este producto servirá también para ser comercializado generando réditos económicos a más de haber subido la imagen corporativa de la empresa.

Finalmente se incluyen las conclusiones, recomendaciones y lecciones aprendidas durante todo el proceso de implementación.

ABSTRACT

The research work proposes a frame of reference for the implementation of a disaster recovery plan for a company of any kind in Ecuador, its implementation emphasizes companies in the area of technological solutions, in which the main guidelines are announced. and international standards such as ISO 22301 and following the best practices recommended by the leading manufacturers in the area of technology with the best rating within the Gartner quadrant.

It is based on a conceptual vision in which we touch on topics related to systems and standards of the business continuity plan and disaster recovery plan, which will serve as a guide for the implementation of error recovery mechanisms and system crashes, as well as verification of high availability methods of applications and systems.

The methodology used proposes the guidelines and processes to be followed and how to act against the incidence of a disaster, proposes the plan to be followed for recovery and put back into production of each system; An important aspect within this phase is to reach a full knowledge of the existing infrastructure, to know its current status and its shortcomings, which will allow us to be prepared for a catastrophic event.

Based on the results obtained, a guide to the error recovery plan is implemented as a case of practical implementation applied to a technology solutions company in Ecuador, whose results were satisfactory, since having a disaster recovery plan to generate peace of mind for all staff, knowing that they have a level of protection against any incident also generates value at the level of the companies of the competition, because this product will also serve to be marketed generating economic returns after having uploaded the image company's corporate

Finally, conclusions, recommendations and lessons learned are included throughout the implementation process.

Tabla de contenido

Introducción 9

Delimitación 10

Problema científico 10

Formulación del problema 10

Objetivos de la investigación 12

Objetivo general 12

Objetivos específicos 12

Justificación 13

Capítulo I - Marco Teórico Conceptual 14

1.1. Sistemas de alta disponibilidad 14

1.2. Arquitecturas de alta disponibilidad y escalabilidad 14

2.1.1. Alta disponibilidad de infraestructura 15

2.1.2. Alta disponibilidad de aplicación 15

1.3. Plan de continuidad de Negocio (BCP) 16

1.3.1. Introducción al BCP 16

1.3.2. Beneficios 16

1.4. Plan de Recuperación de desastres (DRP) 18

1.5. Diferencia entre BCP y DRP 18

1.6. Análisis de impacto al negocio (BIA) 19

1.6.1 Características 19

1.6.2 Actividades fundamentales según la ISO 22301 19

1.7. Objeto de Punto de Recuperación (RPO) 20

1.8. Objetivo de Tiempo de Recuperación (RTO) 21
1.9. Metodologías y Estándares para Elaborar un BCP/DRP 21
1.9.1. BS 25999 21
1.9.2. ISO / IEC 27031:2011 22
1.9.3. COBIT 5.0 22
1.9.4. ISO 22301 22
1.10. Virtualización de Servidores – Vmware 24
1.11. Respaldo y Replicación de Servidores – Veeam Backup 25
Capítulo II - Marco Metodológico 26
2.1. Enfoque metodológico de la investigación 26
2.1.1. Población 27
2.1.2. Muestra 27
2.1.3. Métodos empleados para la recolección de información 28
Procesamiento de la información 28
2.1.4. Recolección de Información 29
2.1.5. Inventario de Hardware y Software 29
2.1.6. Inventario de Ambiente Virtual 30
2.1.4. Escenarios de Contingencia 36
2.1.5. Roles y responsabilidades 37
2.1.6. Levantamiento de aplicaciones críticas de la empresa. 41
2.2. Selección del estándar aplicado 43
2.2.4. Criterios de selección 43
2.2.5. Metodología Seleccionada - ISO 22301 44

2.3. Herramientas y Materiales 47
Capítulo III - Análisis y propuesta 49
3.1. Fundamentación del Proyecto 49
3.2. Desarrollo del Plan de Recuperación de Desastres 49
3.2.1 Gestión e iniciación del proyecto 51
3.2.2 Análisis de impacto sobre el negocio BIA: 58
3.2.3 Estrategia de recuperación: 61
3.2.4 Diseño y desarrollo del DRP 62
3.2.5 Prueba, mantenimiento, y entrenamiento: 63
3.3. ANÁLISIS DE RESULTADOS 65
3.3.1. Levantamiento de información 65
3.3.2. Análisis de datos 65
3.3.3. Herramientas implementadas 71
Conclusiones 73
Recomendaciones 75
Bibliografía 76
Anexos 78

Índice de Figuras

Figura 1. Alta disponibilidad 15
Figura 2. Plan de continuidad del negocio (BCP) 18
Figura 3. RPO versus RTO 21
Figura 4. Componentes de virtualización 25
Figura 5. Respaldo y replicación de máquinas virtuales 25
Figura 6. Resumen ambiente virtualización 30

Figura 7. Resumen configuración Host DELL 31
Figura 8. Alertas de error sobre Host 31
Figura 9. Resumen configuración Host HPE 32
Figura 10. Estado de carga sobre Clúster 33
Figura 11. Resumen de Sistemas Operativos dentro de la Infraestructura 35
Figura 12. Fases del DRP 44
Figura 13. Organigrama del plan de recuperación ante desastres 51
Figura 14. Cadena de Notificación de Incidentes 53
Figura 15. Cálculo de Análisis de Riesgo 59
Figura 16. Ejemplo Proceso Recovery 62
Figura 17. Arquitectura de Backup y Replicación 69
Figura 18. Arquitectura de Recuperación Instantánea 70
Figura 19. Arquitectura de Replicación 71

Índice de Tablas

Tabla 1. Distribución TIC a nivel nacional 27
Tabla 2. Aplicaciones Críticas 28
Tabla 3. Inventario de Infraestructura 29
Tabla 4. Estado de Encendido de Máquinas Virtuales 33
Tabla 5. Estado de error de Máquinas Virtuales 34
Tabla 6. Cantidad de Virtuales por capacidad de memoria 34
Tabla 7. Cantidad de máquinas Virtuales por tipo de Host 35
Tabla 8. Cantidad de Máquinas Virtuales por Sistema Operativo 35
Tabla 9. Cantidad de Usuarios por aplicación 41
Tabla 10. Cantidad de Usuarios por aplicación 42
Tabla 11. Cantidad de Usuarios por aplicación 42
Tabla 12. Roles y responsabilidad 52
Tabla 13. Aplicaciones Críticas 59
Tabla 14. Frecuencia de Respaldos 60
Tabla 15. Respuesta ante Incidentes 61
Tabla 16. Información de Sistemas 62

Tabla 17. Actividades de Mantenimiento del DRP 64

Índice de Anexos

Anexo 1. Formato levantamiento de información de Sistemas 78
Anexo 2.Matriz de Respaldos 83
Anexo 3.Matriz de respuestas ante incidentes 84

Introducción

La constante evolución de las Tecnologías de la Información y Comunicaciones (TIC), así como la facilidad de acceso al internet a nivel mundial, ha provocado que, sin importar el tamaño de las empresas, éstas generen gran cantidad de información sensible y de vital importancia que debe ser debidamente protegida.

Debido a estas facilidades de acceso a internet el porcentaje de servicios basados en herramientas tecnológicas es alto; es por esto, que es de vital importancia para una empresa el contar con un plan de recuperación de desastres que garanticen la continuidad de los servicios críticos de la institución.

El plan de continuidad de negocio (BCP), por sus siglas Bussiness Continuity Plan y el plan de recuperación de desastres (DRP), se ha convertido en la última línea de defensa de una entidad; cuando los controles han fallado, el plan de continuidad es el control final, que puede prevenir eventos drásticos, pérdidas de información, paralización de operaciones o el fracaso de una organización.

Lo expuesto, permite a las empresas crear una cultura de autoconocimiento constante y gestión de los riesgos, permitiendo no solo la optimización de los recursos de Tecnologías de la Información (TI) sino también logrando una mejora en sus procesos.

Miguel Angel Mendoza. (2014). de *welivesecurity*, señalan que cualquier incidente de paralización de servicios o pérdida de información de una empresa provoca alarmas en las organizaciones afectando no solo a los bienes tangibles de las instituciones sino también a la imagen corporativa de esta, lo que ocasiona grandes pérdidas económicas debido a la indisponibilidad de los servicios.

Es por ello por lo que, el contar con un sistema de recuperación ante desastres puede reducir al mínimo el tiempo de inactividad tecnológica y pérdida de datos con una recuperación rápida y ordenada después de un desastre.

Delimitación

El plan de recuperación ante desastres abarcará la protección referente a las TIC, involucradas en los procesos críticos para la continuidad del negocio; la aplicación de la metodología se basa en la norma ISO 22301 referente a los Sistemas de Gestión para la Continuidad del Negocio y como caso de estudio, se implementó el Plan de Recuperación ante Desastres (DRP) en la Empresa de Soluciones Tecnológicas y considerando que el 98% de sus aplicaciones está virtualizado, se utilizó como herramienta de virtualización vmware vsphere y como herramienta de respaldo y replicación "Veeam Backup & Recovery".

Problema científico

La prevención y control de incidentes informáticos permite a las empresas a disminuir caídas inesperadas en los sistemas y aplicaciones. (welivesecurity, 2014)

La planificación en los procesos de restauración de aplicaciones permite a las empresas a restaurar sus actividades de manera ordenada en el menor tiempo.

Los sistemas de alta disponibilidad a nivel de hardware, software y sitios de contingencia aumentan los niveles de disponibilidad de sus servicios.

Formulación del problema

Numerosos estudios realizados principalmente por fabricantes de tecnologías como veeam y vmware, acerca de los problemas que presentan las entidades al no poderse recuperar de desastres naturales o de índole informáticos las infraestructuras tecnológicas. En la actualidad donde dependemos cada vez mas de estas tecnologías cualquier incidente traen consigo daños graves.

Según estadísticas recogidas en un informe de la empresa "International Business Machines" (IBM), de las instituciones con pérdidas de información por desastres, solo un seis por ciento perdura a largo plazo, 51% quiebran en menos de un año y 43% no abren más (IBM, 2016).

Toda empresa en algún momento ha sufrido algún incidente que ocasione perdida de información e indisponibilidad de aplicaciones y servicios causados por diferentes factores como: hardware, software, eléctricos, humanos, etc; ocasionando daño y/o pérdida en los servicios dejando a la empresa días completos sin productividad lo cual ocasiona no solo pérdidas económicas sino también afecta a la imagen corporativa de ésta ocasionado desconfianza en los clientes y consecuentemente su migración hacia la competencia. (Veeam, 2018)

El problema no solo es la pérdida de información, sino también el tiempo que se requiere para volver sus servicios a producción con la menor afectación posible.

En ecuador no existe una normativa u organismo que obligue a las empresas a disponer de un plan de recuperación de desastres (DRP) por sus siglas en inglés (Disaster Recovery Plan) a excepción de las instituciones bancarias que están reguladas por la superintendencia de Bancos, quien si obliga a este tipo de instituciones a implementar un plan de contingencia y continuidad de negocio y se lo puede verificar dentro del capítulo V que habla de la gestión del riesgo operativo y bajo el artículo 15, numerado con la resolución Nro. JB-2008-1202 del 23 de octubre del 2008.

Con el antecedente expuesto se ha revisado algunos estudios y trabajos previos realizados en este ámbito dentro del territorio ecuatoriano, tomando como referencia tres casos tipo, como son:

Desarrollo de un plan de recuperación de desastres para la unidad de tecnología de la EPMAPAP (Empresa Pública Municipal De Agua Potable Y Alcantarillado De Portoviejo), realizado por el Ing. José Luis Loor Zambrano como tesis previo a la obtención de la maestría en Evaluación y Auditoría de Sistemas Tecnológicos en la Escuela Politécnica del Ejército (ESPE) en mayo del 2014; a pesar que la institución no se vio afectada en el terremoto del 2016, la empresa estaba preparada para su recuperación tecnológica en caso de una incidencia.

Otro estudio referenciado fue el realizado por el Consejo Nacional de Competencias en el año 2017, en cuya primera edición consta un documento de 32 páginas, realizado por el ingeniero Miguel Angel Moreno y aprobado por la Ing. María Lorena Santillán, denominado

"Plan de Contingencia Informático", se referenció a este trabajo al ser una institución pública ya que la misma podría servir de referencia para instituciones del estado que requieran implementar un Plan de Recuperación de Desastres; verificamos que el DRP toma como base la norma ISO 22301, lo que nos da una pauta que el DRP cumple estándares internacionales.

El siguiente estudio evaluado se le denomina, Propuesta de un método para elaborar un plan de recuperación de desastres (DRP) en el Área de tecnología de la información para Cooperativas de Ahorro y Crédito del Ecuador, este trabajo fue realizado por el Ing. Washington Vásquez Naranjo en Junio del 2017, y se lo realizó como tesis previo a la obtención de la maestría en seguridad informática en la Escuela Politécnica de Chimborazo; el trabajo se lo realizó con el fin de cumplir la reglamentación de la superintendencia de Bancos resol_JB-2014-3066, Su aplicación se la realizó en la Cooperativa de Ahorro y Crédito San José LTDA ubicada en el cantón San José de Chimbo provincia de Bolívar, basándose principalmente en la identificación de procesos, tiempos y recursos críticos que se pueden presentar en las instituciones financieras, posteriormente se procedió a realizar el análisis respectivo para evidenciar cuál sería su impacto financiero en caso de tener interrupciones, el método propuesto se desarrolló tomando como base la normativa del organismo de control fundamentados con la ayuda del estándar internacional ISO 22301 para Sistema de Gestión Continuidad del Negocio y en las experiencia del desarrollador en instituciones financieras.

Objetivos de la investigación

Objetivo general

Desarrollar una guía de recuperación de desastres de la Infraestructura de TIC, que garantice la continuidad de los procesos críticos de la empresa basados en las normas ISO 22301.

Objetivos específicos

1. Investigar los sistemas de redundancia, normas y estándares orientados a alta disponibilidad de aplicaciones y servicios de TI.

2. Analizar la infraestructura, los sistemas de recuperación de la información y tipos de fallos comunes que ocurren en empresas de soluciones tecnológicas.
3. Diseñar un plan de recuperación de desastres de la infraestructura de TI para empresas de soluciones tecnológicas.
4. Implementar el plan de recuperación de desastres bajo la norma ISO 22301.

Justificación

Según (isotools, 2016) las empresas continuamente experimentan situaciones de emergencia o catástrofes que ponen en peligro las operaciones o servicios que brindan, por lo que un Plan de Recuperación de Desastres (DRP) describe como reiniciar las operaciones críticas de la organización después de una interrupción. El DRP se enfoca en recuperar los sistemas, operaciones y servicios críticos después de una caída no planificada, por tanto, es fundamental que cada institución cuente con un plan actualizado donde se detallen las estrategias de reanudación y permita proteger los procesos críticos y operativos del negocio disminuyendo el impacto en pérdidas de tipo financiero, de credibilidad y productividad.

Akros es una empresa integradora de soluciones tecnológicas misma que al contar con un plan de recuperación de desastres (DRP) basados en estándares internacionales como es la ISO 22301, y con miras a obtener la certificación, emitirá lineamientos que permitan garantizar su capacidad para operar de manera continua y minimizar las perdidas en caso de una interrupción del negocio.

Por lo tanto, la presente investigación está dirigida a dar respuesta a esta necesidad de seguridad y continuidad frente a riesgos tecnológicos, mediante la recopilación de las mejores prácticas o referentes para la confección de un DRP, que permitan generar una propuesta del plan de continuidad del negocio para empresas integradoras de servicios tecnológicos.

Capítulo I - Marco Teórico Conceptual

El capítulo siguiente describe los principales conceptos relacionados con la temática a desarrollar y que serán utilizados como parte de la propuesta. En el mismo se desarrollarán los principales marcos de referencia y estándares internaciones que se relacionan con un plan de recuperación de desastres dentro de una institución. Estos conceptos y estándares serán analizados tomando en consideración lo establecido dentro de las normas ISO22301 que proporciona un marco de referencia en la identificación y mitigación de riesgos y amenazas. Establece las acciones para reducir el daño que pueda darse dentro de la organización

1.1.Sistemas de alta disponibilidad

El portal Gobierno de Canarias, hace referencia que los sistemas de alta disponibilidad deben encontrarse activos y sin interrupciones 24/7 durante todo el año para los usuarios autorizados a acceder a los mismos. Estos sistemas expuestos a interrupciones que deben estar completamente funcionales. Estas interrupciones pueden ser planificadas, que se realizan cuando se paraliza el sistema para realizar cambios, mantenimientos o mejoras en las aplicaciones o no planificadas; que envuelve aquellas que ocurren de forma imprevista (apagones eléctricos, problemas de hardware, desastres naturales, infección por virus, etc.)

1.2.Arquitecturas de alta disponibilidad y escalabilidad

Una arquitectura en forma de clúster con alta disponibilidad puede definirse como pc conectados en paralelo y comparten servicios y que se monitorean entre sí constantemente. Estos sistemas se clasifican en dos tipos (Canarias, 2016).

2.1.1. Alta disponibilidad de infraestructura

En caso de producirse un problema en el hardware de alguna de las máquinas que forman parte del clúster, los servicios de los otros ordenadores que forman parte del mismo mantienen su disponibilidad. Estos servicios vuelven a funcionar normalmente en el ordenador principal una vez se haya recuperado de fallo, garantizando una gran disponibilidad de los servicios, por lo que los usuarios no perciben algún fallo.

2.1.2. Alta disponibilidad de aplicación

Si el problema ocurre en el hardware o en alguna aplicación de los ordenadores que forman parte del clúster, los servicios son restablecidos por el software en los ordenadores del clúster manteniendo la disponibilidad de la aplicación. Al recuperase del fallo, los servicios son restablecidos, tal como se muestra en la Fig1. Por lo que la integridad de los datos queda garantizada y los usuarios no perciben el problema del sistema, evitando molestias a los mismos.

De lo descrito debemos notar que el clúster de disponibilidad alta es diferente a un clúster con rendimiento alto, la segunda definición refiere aquel clúster que proporciona gran capacidad de cálculo en comparación con ordenadores individuales; sin embargo, el caso de un clúster con alta disponibilidad como ya habitaos mencionado tiene como objetivo un funcionamiento sin interrupciones.

Figura 1. Alta disponibilidad
Fuente: (VMware, Inc, 2019)

1.3. Plan de continuidad de Negocio (BCP)

En este epígrafe se realizó un estudio de cómo ha evolucionado el Plan continuidad de Negocio (BCP), referido al entono mundial y en el Ecuador; describiendo los beneficios y problemas que pueden generase en una entidad que cuente o no con el mismo.

1.3.1. Introducción al BCP

Las organizaciones deben poseer capacidad táctica y estratégica que es permita planificar de forma adecuada y responder de forma oportuna a cualquier incidente que pueda ocurrir en las mismas y que permitan dar continuidad a los servicios de una manera correcta.

El BCP es una metodología, que permite crear y validar actividades logísticas a través de una serie de instrucciones y planes de seguridad en función de recobrar de forma parcial o total las funciones más críticas una entidad ante la ocurrencia de un problema o desastre.

El plan de continuidad de negocio establece los procesos que los trabajadores de una entidad deben seguir ante problemas inesperados que inciden de forma negativa en el funcionamiento correcto de los procesos de negocio. Este plan asegura continuidad en las actividades ante situaciones inesperadas.

Un BCP debe garantizar una alta cobertura desde el punto de vista técnico y organizativo en las áreas críticas de la organización, manteniendo los servicios claves de la entidad y disminuyendo los impactos frente a cualquier evento.

1.3.2. Beneficios

Al implementar un BCP en una entidad pueden darse determinados beneficios como son:

- **Ventaja competitiva**: permite mejorar la imagen de la entidad, proveyendo de confianza a proveedores, clientes e inversionistas.
- **Prevenir pérdidas**: permite determinar el impacto que provoca algún incidente en las interrupciones de las actividades de la entidad.
- **Recuperación ante fallos**: permite asegurar los procesos de la entidad, acrecentando la disponibilidad de los mismos.

- **Eficiencia en la asignación de inversiones en seguridad**: Esto se logra mediante el estudio de riesgos de la entidad, permitiendo establecer prioridades según la criticidad de los procesos. A partir del cual se designa los esfuerzos y se asigna el presupuesto.

Como estrategias de la entidad que permiten hacer competitiva las mismas mediante la implementación de un BCP pueden mencionarse:

- **Maximizar de capacidades**: permite la sociabilización de la información y el conocimiento obtenido; permitiendo una continuidad en las operaciones de la entidad si existe algún problema con algún empelado.
- **Mejorar procesos**: permite mejorar los procesos de la entidad a través de un análisis de impacto, determinando la prioridad de los mismos y los recursos que nos ayuden a resolver los problemas.
- **Conocimiento del contexto**: en la implementación de un BCP se tienen en cuenta los procesos legales que pueden darse ante una situación determinada; conociéndose de antemano las posibles soluciones a dar a algún cliente.
- **Capacidad de servicio**: prepara al personal para reaccionar ante algún incidente en la entidad, logrando que el mismo trabaje bajo presión. Además, debe instruirse al personal y crear la habilidad de trabajo ante cambios.
- **Disponibilidad**: Permite la disponibilidad de las actividades y servicios a los clientes, apoyándose en herramientas de virtualización o proveyendo la posibilidad de que sus empleados puedan trabajar desde la casa para atender los problemas que se presenten.
- **Proteger la marca de la entidad**: Con la implantación de un BCP, la empresa no pierde credibilidad si ocurre algún problema. Los trabajadores concientizan la necesidad del trabajo en equipo.

Estos beneficios generan un crecimiento en la productividad de la empresa, ayudando a comunicación entre los trabajadores frente a alguna situación de emergencia; además de mejorar la calidad del trabajo y garantizar la continuidad de los procesos.

1.4. Plan de Recuperación de desastres (DRP)

Un Plan de Recuperación de Desastres (DRP), refiere al desarrollo de un conjunto de acciones y estrategias que tienen en cuenta las diferentes opciones de recuperación ante determinados incidentes que pueden afectar las actividades de la empresa a través de su infraestructura (Casillas, 2018).

Un plan de reducción de desastres permite disminuir todos los efectos que pueden producir incidentes en las actividades de una entidad, logrando la continuidad de las funciones.

Debemos tener en cuenta que las características de un DRP deben estar en función de las necesidades identificadas en la entidad como el tipo de empresa, procesos y actividades que realiza y la necesidad de seguridad de las mismas.

1.5. Diferencia entre BCP y DRP

La principal diferencia entre el BCP y el DRP radica en el alcance de los mismos. El primero de ellos, como se había mencionado constituyen todas las acciones que permiten continuidad en las actividades y procesos de la empresa ante algún incidente. El plan DRP está asociado a recuperar y restablecer las actividades de tecnología de información que soportan los procesos más importantes de la organización. En la figura 2, se describe la relación entre los dos planes, donde se puede ver que el DRP es parte del BCP, aunque los dos son imprescindibles para el correcto funcionamiento de las actividades de la empresa.

Figura 2. Plan de continuidad del negocio (BCP)
Fuente: (welivesecurity, 2019)

1.6. Análisis de impacto al negocio (BIA)

Otro mecanismo manejado para estimar afectaciones de una entidad es el análisis de impacto al negocio (BIA).

El análisis de impacto al negocio es una metodología especializada en identificar tipos de impactos a diferencia de una metodología de identificación y evaluación de riesgos que se centra en las afectaciones de una entidad identificando y valorando las amenazas subyacentes en función de un nivel de impacto y su probabilidad de que ocurra.

De aquí que el análisis de impacto al negocio es una actividad que forma parte del plan de recuperación de desastres y del BCP antes descritos, y permite a una entidad realizar estimaciones sobre el impacto que puede darse en las mismas desde el punto de vista financiero y operacional ante un incidente.

1.6.1 Características

El análisis de impacto al negocio provee por un lado una base que permite la identificación de tareas críticas Enel funcionamiento de una empresa y, por otro lado, permite priorizar actividades según el nivel de impacto que tengan dentro de la organización.

Este análisis se encuentra asociado a las tareas criticas respeto al tiempo, por lo cual nos ayuda a estimar aquellos recursos imprescindibles para cada una de las actividades sobre todo aquellas más sensibles al tiempo e impacto.

De aquí que utilice una variable llamada Tiempo Objetivo de Recuperación (RTO), que se define como el lapso de tiempo en el que se recupera una actividad, proceso o recursos de la empresa ante un incidente. Además, se define el llamado “Punto Objetivo de Recuperación” (RPO), que está asociada a la cantidad de información tolerada por la pérdida de un proceso.

1.6.2 Actividades fundamentales según la ISO 22301

- Identificar los sistemas críticos del negocio
- Identificar las dependencias de recursos del sistema

- Identificar el personal o equipos de apoyo clave
- Calcular los efectos de interrupción
- Determinar la prioridad de recuperación de recursos

Disponer de este conocimiento granular del impacto sobre el negocio de los sistemas críticos, no sólo le ayudará durante una situación real de desastre, sino que le permitirá comprobar su preparación para el desastre. Saber hacia dónde enfocar sus esfuerzos de planificación le permitirá, en gran medida, simplificar y dar prioridad a los ejercicios o pruebas de recuperación de desastres.

El BIA no es sólo un inventario de los sistemas técnicos, sino que deberá trabajar con la parte empresarial para definir el RPO (objetivo de punto de recuperación) y el RTO (objetivo de tiempo de recuperación) para los servicios claves de la empresa y los servicios de TI dependientes. El establecimiento de objetivos aporta a los responsables de la planificación y gerentes de DR un punto de partida para el diseño y gestión que abordarán. Sin una definición de estos requisitos fundamentales para la planificación de recuperación ante desastres, corre el riesgo de realizar elevadas inversiones en un nivel superior de protección de datos del que realmente su empresa requiere. El otro riesgo es que no proporcione suficiente protección para sus recursos críticos y acabe costándole a su empresa mucho más tiempo y dinero en el caso de que se produzca un desastre. En la siguiente sección abordaremos por qué es fundamental la planificación del RPO y RTO.

1.7. Objeto de Punto de Recuperación (RPO)

Durante su BIA debería invertir una cantidad de tiempo desarrollando una comprensión profunda acerca de cómo su negocio genera dinero, así como identificar los recursos claves y los procesos necesarios para habilitar la creación de ingresos. En algunas empresas, esta puede identificarse como una actividad comercial única que se traducirá en una clara orientación sobre los requisitos del RTO/RPO. Si bien, en empresas más grandes, que cuentan con una mayor diversificación de productos y servicios, es probable que necesite emplear diferentes estrategias de recuperación de desastres (DR) para hacer frente a múltiples situaciones empresariales. Sin importar el tamaño de la empresa, el proceso de

planificación de DR es similar, y aplicamos el mismo proceso para clasificar los casos reales que descubrimos en nuestras evaluaciones de DR.

1.8. Objetivo de Tiempo de Recuperación (RTO)

Recovery Time Objetive (RTO), está asociada al mayor tiempo en el cual un servicio, actividad, o sistema informático se encuentra interrumpido. En la figura 3, se puede observar la interacción de estos dos conceptos.

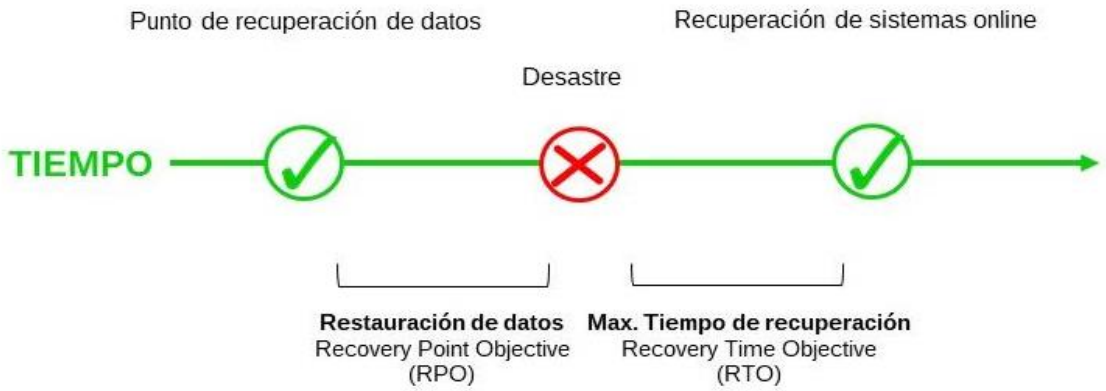


Figura 3. RPO versus RTO
Fuente: (welivesecurity, 2019)

1.9. Metodologías y Estándares para Elaborar un BCP/DRP

Para la elaboración del plan de recuperación ante desastres DRP, se realiza el estudio de las metodologías existentes con el propósito de seleccionar la metodología que mejor se acople a los objetivos propuestos.

1.9.1. BS 25999

La metodología BS 25999 instituida por el Instituto “Disaster Recovery” (DRI). Establece buenas prácticas que ayudan a través de la determinación de riesgos a la continuación de los procesos de una entidad. Esta metodología se basa en el plan de continuidad de negocio y contempla dos fases; por un lado, tiene en cuenta el desarrollo del BCP y por otro lado la implementación de este.

1.9.2. ISO / IEC 27031:2011

Esta norma establece las definiciones importantes que pueden ser aplicadas a cualquier tipo de entidad y recoge los elementos asociados a las tecnologías de la información y comunicación, continuidad de los procesos de una entidad. Además, provee referencia en cuanto a los criterios de diseño, rendimiento que permiten mejorar las TIC de una empresa.

1.9.3. COBIT 5.0

La Asociación para la Auditoria y Control de Sistemas de Información, ISACA (Information System Audit and Control Association) y su IT Governance Intitute, ITGI, desarrollaron los "objetivos para el control de las tecnologías de la información "COBIT". Este estándar establece elementos, herramientas y metodologías aceptadas por toda la comunidad internacional y que permiten mejorar el valor de los sistemas de información. COBIT 5 ha surgido con la complementación de otras normas y recursos de COBIT 4.1.

Dentro de los beneficios se puede mencionar que COBIT 5 ayuda a empresas de todos los tamaños a:

- Optimización y reducción de costos en los servicios de tecnologías de información.
- Provee apoyo al cumplimiento de los reglamentos, acuerdos o políticas establecidos.
- Gestionar las TIC.

1.9.4. ISO 22301

La primera entidad de estandarización en el Reino Unido y en el Mundo, *British Standards Institution* (BSI), cuenta con una reconocida reputación de independencia en la realización de estándares e información. Dentro de estas normas encontramos la BS/ISO 22301 del año 2012, que constituye buenas prácticas de gestión que permite la continuidad de los procesos en una entidad y se basa en el estándar BS 25999.

Este estándar permite proteger una organización de incidentes potenciales como: situaciones meteorológicas extremas, incendios, inundaciones, desastres naturales, etc; a

través de la identificación de amenazas relevantes de la entidad y las funciones críticas del negocio que podría tener un impacto.

La continuidad del negocio contribuye al desarrollo de una sociedad más resiliente, organizaciones sin un BCP eficaz en la gestión y prevención de vulnerabilidades a las que son expuestas, podría llegar a generar impactos negativos en sus empleados, usuarios, clientes y proveedores. El estándar se puede utilizar para evaluar la capacidad de una organización para satisfacer sus propias necesidades y obligaciones de continuidad.

En este estándar se aplica el modelo "Planear-Hacer-Verificar-Actuar" (PHVA), a través de requisitos que permiten realizar cada una de las acciones descritas; mejorando los sistemas de gestión. Este estándar incluye los siguientes temas:

1. Alcance
2. Referencias normativas
3. Términos y definiciones
4. Contexto de la organización
5. Liderazgo
6. Planificación
7. Recursos
8. Operación
9. Evaluación de desempeño
10. Mejora

Es importante indicar que la norma ISO 22301 al ser un estándar internacional puede ser aplicada a todo tipo de empresa, pues toda empresa está expuesta en cualquier momento de su existencia a sufrir un incidente de tipo humano, tecnológico o natural; por ese motivo es indispensable dotar a las empresas de disponibilidad operacional en situaciones de emergencia, con lo cual, la implementación de esta capacidad basada en la ISO 22301 aumentará las ventajas competitivas como proveedor preferido y dará a los clientes la tranquilidad de poder hacer negocios con éstas empresas.

En Ecuador, las pequeñas y medianas empresas también requieren de la aplicación de estas normas, pues toda empresa desea y necesita proteger su activo más importante, que es

la información y con ello crear métodos que permitan prepararse y dar una respuesta de recuperación de sus procesos críticos en forma ordenada ante un incidente. (INEC, 2017)

1.10. Virtualización de Servidores – Vmware

El proceso de virtualización se define como aquel que permite ejecutar un software determinado de forma virtual y no física como se realiza normalmente. Constituye una forma de disminuir costos tecnológicos al poder aplicarse a ordenadores, servidores, redes u otros almacenamientos; aumentando eficiencia de los procesos de las empresas (VMware, Inc, 2019).

Ventajas

El proceso de virtualización permite que los procesos de tecnologías de la información sean escalables, flexibles y agiles, disminuyendo de forma significativa los costos. Además, permite mayor velocidad en los procesos de cargas, permite aumentar el rendimiento y disponibilidad de las operaciones.

A continuación, algunas de las ventajas más significativas:

- Reducir costos de operación.
- Disminuir el tiempo Enel que el sistema se encuentra sin servicio
- Permite aumentar la capacidad de respuesta y eficiencia de los procesos tecnológicos.
- Permite una fácil recuperación ante incidentes que trae consigo una continuidad de los procesos de la entidad.
- Mejorar la administración de los datos.

Virtualización de servidores

Según el portal web de VMWARE, casi todos los servidores aprovechan menos de un 14% de toda la capacidad que poseen. Realizando un proceso de virtualización se consigue aprovechar mucho mejor los mismos a poder instalar múltiples sistemas operativos en un mismo ordenador físico. Los recursos son compartidos por todas las máquinas virtuales.

Si queremos aumentar la eficiencia podemos añadir un clúster de servidores para un único recurso. Este proceso logra que las cargas de trabajos se ejecuten de una forma más rápida y un aumento de la disponibilidad y rendimiento. Se puede sintetizar a un servidor como el conjunto de componentes de hardware sobre los cuales se implementan diferentes sistemas operativos, tal como lo podemos esquematizar en la figura 4.

Figura 4. Componentes de virtualización
Fuente: (VMware, Inc, 2019)

1.11. Respaldo y Replicación de Servidores – Veeam Backup

"Veem Backup" constituye un software potente y de fácil funcionamiento que permite respaldar la información, proporcionando una recuperación de la información virtualizada de forma rápida. Realiza en las funciones de replicar y almacenar de forma virtual la información en una mimas aplicación; y soporta entornos virtuales de soluciones como VMware, Sphere y Hyper-V.

Esta solución ejecuta copias de seguridad mediante puntos de recuperación (RTPO) de menos de quince minutos para toda la información; ofreciendo alta disponibilidad para las entidades. A continuación, podemos observar en la figura 5 la forma en la que se integra esta herramienta (Veeam , 2019).

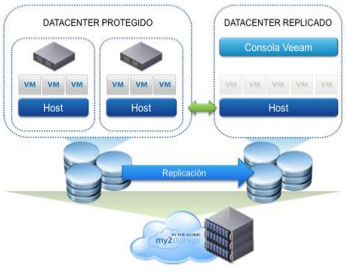


Figura 5. Respaldo y replicación de máquinas virtuales
Fuente: (VMware, Inc, 2019)

Capítulo II - Marco Metodológico

Para lograr los objetivos inicialmente propuestos se realizó un análisis de las metodologías en la línea del Plan de Recuperación de Desastres logrando de esta manera establecer el enfoque metodológico de la investigación y demás componentes de esta que se los trata a continuación.

2.1.Enfoque metodológico de la investigación

Investigar significa llevar a cabo diferentes acciones, procesos o estrategias con el propósito de descubrir algo, de esta manera dichos actos aportan para la obtención y aplicación de nuevos conocimientos, explicar una realidad determinada y a obtener diferentes maneras de resolución de situaciones de interés; por lo que la investigación es la base del conocimiento científico, aunque no toda investigación sea de esta índole.

Se puede investigar desde diferentes perspectivas, con diferentes objetivos o teniendo en cuenta diferentes tipos de datos, procedimientos o métodos para obtenerlos; siguiendo una de las clasificaciones de los tipos de investigación; dicho estudio y de acuerdo con el tipo de datos empleados se ha clasificado como investigación cuantitativa.

La investigación cuantitativa mide de forma cuantitativa las variables estudiadas, permitiendo explicar sucesos para probar hipótesis.

Como parte de este plan de recuperación de desastres, se ha analizado la situación actual de la empresa realizando reuniones, mediciones, estadísticas, encuestas, observaciones, lo cual permitirá contrastar la situación actual y una situación futura luego de la implementación y uso de las mejores prácticas descritas en la presente investigación.

2.1.1. Población

El conjunto de individuos, objetos o elementos sobre el que se basa el estudio hace referencia a todos los sistemas y aplicaciones de TI de la empresa; además, se debe considerar que el centro de datos cuenta con aplicaciones y servicios en plataformas físicas y virtuales a más de los componentes de redes que son base fundamental en las comunicaciones internas y externas y todos los sistemas y equipos denominados como estaciones de trabajo; la empresa cuenta con cuatro sucursales a nivel nacional en las ciudades de Quito, Guayaquil, Cuenca y Ambato; los servicios están centralizados en el datacenter principal en Quito y desde cada sucursal se cuenta con un equipo servidor para autenticación local, la distribución de los equipos de infraestructura se la presenta en la tabla 1.

Tabla 1. Distribución TIC a nivel nacional

Ciudad	Servidor Físicos	Servidores Virtuales	Estaciones de Trabajo
Quito	3 Server DELL 4 Server HPE 3 Server Cisco	65 servidores de Producción 13 servidores de Desarrollo	|120 estaciones físicas
Guayaquil	2 Server DELL 2 Server HPE	8 servidores de Producción	50 estaciones físicas
Cuenca	2 Server HPE	4 servidores de producción	18 estaciones físicas
Ambato	1 Server HPE	3 servidores de producción	8 estaciones físicas

2.1.2. Muestra

En base a la población del presente estudio, con el objetivo de obtener mejores resultados de la investigación se ha tomado como muestra a los sistemas críticos de la misma; el ambiente de producción de la empresa y todos sus sistemas está basada en su mayoría en sistemas virtualizados bajo la plataforma VMware, de manera que el estudio, encuestas, estadísticas y análisis serán relacionadas en cuanto al rendimiento y protección de este ambiente.

Las aplicaciones críticas están virtualizadas mediante software de virtualización VMware y están centralizado en el centro de datos principal en Quito. Los sistemas críticos de la empresa se listan en la tabla 2.

Tabla 2. Aplicaciones Críticas

Ident.	Nombre Máquina Virtual	Descripción
SRV-001	GPGYE	ERP Dynamics Replica GYE
SRV-002	SRI-GUIAS	Emisión Guías remisión al SRI
SRV-003	APPSGC	SGC Aplicación
SRV-004	APPSGCi	SCG aplicación Cloud
SRV-005	BDDSGC	SGC BDD Aplicación
SRV-006	BDDSGCi	SGC BDD Cloud
SRV-007	CRMDYNAMICS	ERP Dynamics, sistema financiero
SRV-008	DBSHAREPOINT	BDD Sistema de colaboración empresarial
SRV-009	DYNAMICSGP	ERP Dynamics, sistema financiero
SRV-010	GPUIO	ERP Dynamics versión 2008
SRV-011	POWERBI	Análisis del negocio
SRV-012	PROCAPP1	Servidor sgc aplicaciones pruebas
SRV-013	PROCBDD1	ERP Dynamics bdd
SRV-014	PROJECT	Servidor de Proyectos
SRV-015	SHAREPOINT	Sistema de colaboración empresarial

2.1.3. Métodos empleados para la recolección de información

La realización del proyecto se basa en una investigación documental que permite establecer el nivel de detalle pertinente sobre la temática del plan de recuperación de desastres. Para ello utilizó el método de observación y la entrevista, lo cual permitió conocer los procesos internos del DRP y desarrollar los documentos que describen las actuaciones ante incidentes.

Finalmente se realizó un análisis de la situación actual de los sistemas y componentes de TI con los que cuenta la empresa y su nivel de protección ante incidentes, los mismos que permiten justificar la factibilidad y necesidad de la implementación del DRP desarrollado.

Procesamiento de la información

Para la ejecución del plan de recuperación ante desastres es necesario conocer el ambiente de la infraestructura tecnológica existente en la empresa, partiendo de esa premisa

a continuación se exponen los datos recolectados mediante diferentes herramientas de gestión y monitoreo existente.

2.1.4. Recolección de Información

A nivel empresarial se puede clasificar los sistemas tecnológicos en dos grupos dependiendo del tipo de servicios y aplicaciones que éstos ejecutan, de esta manera podemos mencionar a equipos para servicios de usuarios finales, denominados estaciones de trabajo y los equipos que ejecutan los servicios que atiende los requerimientos institucionales globales denominados servidores; el estudio se orienta a la protección de los servicios y aplicaciones que se ejecutan a nivel de los servidores; partiendo desde esta indicación la recolección de datos se la realiza de la siguiente manera:

2.1.5. Inventario de Hardware y Software

La herramienta utilizada para recolección de información es Microsoft System Center Configuration Manager SCCM 2012, misma que Proporciona un conjunto de herramientas que ayudan a identificar y supervisar los activos de la empresa:

- **Inventario de hardware**: recolección de información del hardware u otros dispositivos de la entidad.
- **Inventario de software**: recolección de la información de los archivos almacenados en los ordenadores y servidores de la entidad.
- **Asset Intelligence**: Provee de soluciones que permiten recolectar información sobre el inventario y monitorear el uso de licencias de software en la entidad.

Una vez analizado y recolectado toda esta información, los resultados se los plasma en la tabla 3.

Tabla 3. Inventario de Infraestructura

Tipo	Descripción	Tipo/Marca	Capacidad	Cantidad
Storage	Equipos de almacenamiento Compartido	DELL EqualLogic	16 TB	1
Storage	Equipos de almacenamiento Compartido	HPE StoreOnce	6 TB	1
Storage	Equipos de almacenamiento Compartido	HPE P2000	16 TB	1
Storage	Equipos de almacenamiento Local	DELL/HPE Server Local	4 TB	1

Server	Equipo de cómputo (CPU, memoria, otros)	DELL PE R730 xd	2CPU/128gb	3
Server	Equipo de cómputo (CPU, memoria, otros)	HPE BL460	2CPU/128gb	4
Switch	Equipo de comunicación LAN	Aruba 2245	48 puertos	2
Switch	Equipo de comunicación LAN	Cisco 2900	48 puertos	2
Switch	Equipo de comunicación SAN	DELL 6224	24 puertos	1
Switch	Equipo de comunicación SAN	Procurve 6120XG	24 puertos	2
Switch	Equipo de comunicación SAN	DELL 6224	24 puertos	1

2.1.6. Inventario de Ambiente Virtual

Para la recolección y análisis de esta información se utiliza las herramientas básicas proporcionadas por el fabricante VMware, no se dispone de herramientas avanzadas que faciliten esta tarea y que proporcionen información más precisa y en tiempo real, la herramienta utilizada es la consola de administración VMware VCenter Server 6.0, la información proporcionada es la siguiente:

El ambiente de producción virtual consiste en 7 host (servidores físicos) en el cual existe 67 máquinas virtuales, con dos cluster de Virtualización (DELL) y (HPE), cuatro virtual switches y once DataStore como se puede ver en la figura 6 del resumen de configuraciones.

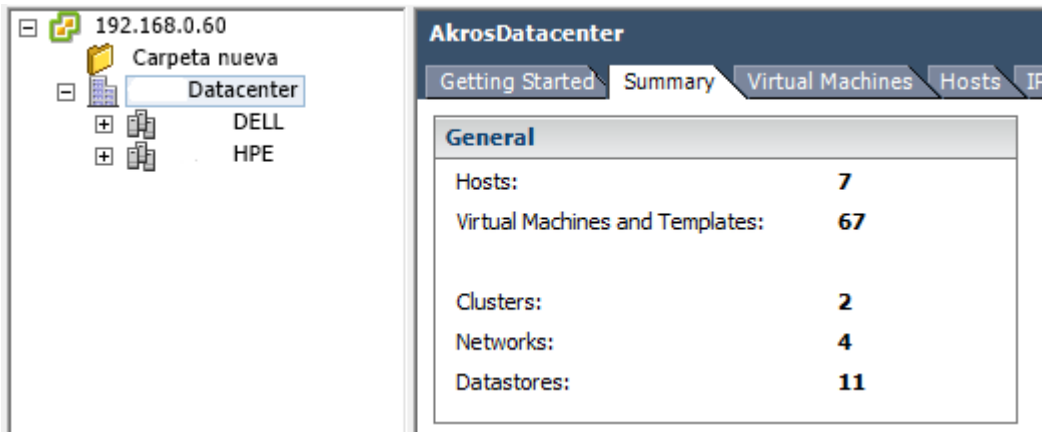


Figura 6. Resumen ambiente virtualización
Fuente: Tomado desde ambiente de producción.

Los hosts (servidores físicos) que forma parte del clúster de producción son de dos fabricantes como lo descubrimos mediante el reporte de Microsoft System Center, en la figura 7, se puede verificar las características físicas de los tres servidores DELL que mantiene similares configuraciones.

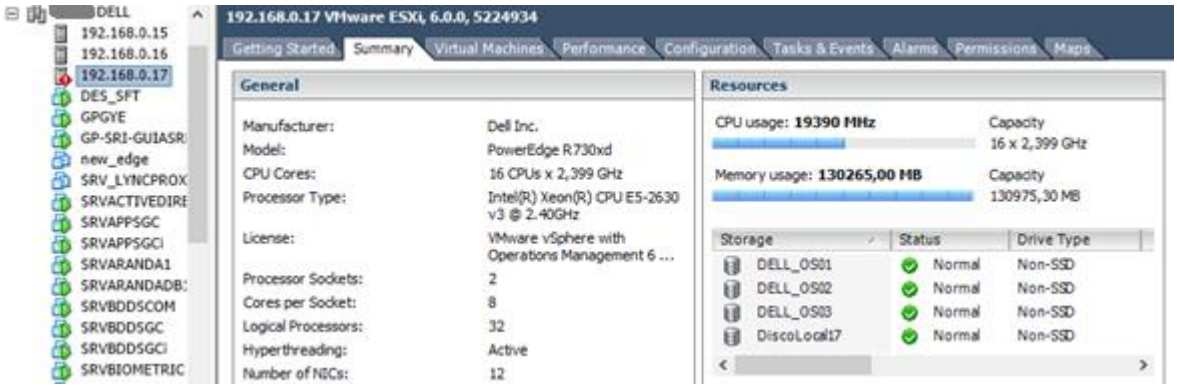


Figura 7. Resumen configuración Host DELL

Fuente: Tomado desde ambiente de producción.

Para verificar la capacidad actual de consumo de recursos del host en mención se debe realizar mediante la herramienta proporcionada por VMware, misma que al ser una herramienta básica la debemos realizar verificando el resumen de configuraciones de cada componente, de ésta mera no se dispone de una herramienta que permita centralizar y verificar el consumo completo del cluster y menos obtener proyecciones de crecimiento; para ejemplo, uno de los host está alertando por consumo y sobrecarga de memoria como lo se observa en la figura 8, pero no existe un sistema de alertas automático, esto hace que los procesos sean manuales y requiera mayor tiempo en tareas de administración por parte de los encargados de la plataforma.

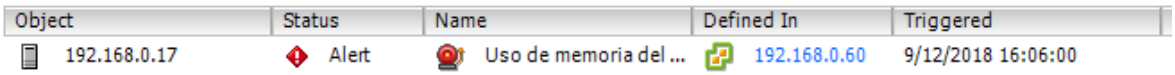


Figura 8. Alertas de error sobre Host

Fuente: Tomado desde ambiente de producción.

De la misma manera se realiza un análisis de las características físicas de los servidores HPE, dentro del clúster de este fabricante se tiene 4 servidores con las características que se observan en la figura 9.

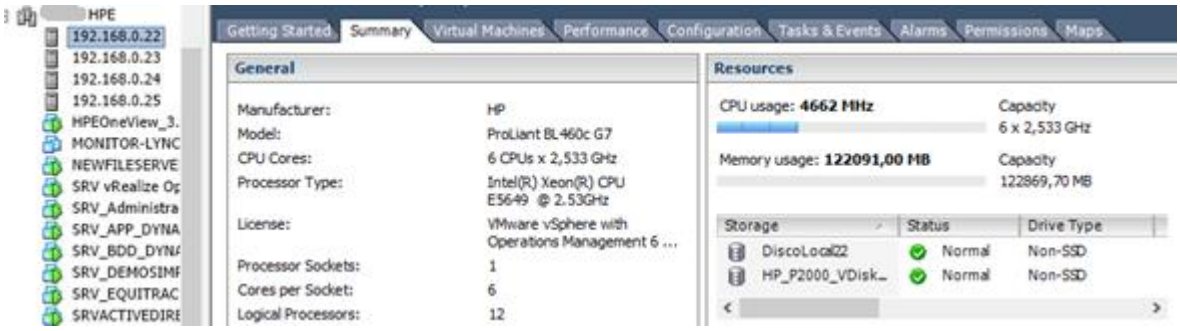


Figura 9. Resumen configuración Host HPE
Fuente: Tomado desde ambiente de producción.

Similar al grupo de servidores DELL, en este ambiente también tenemos servidores que presentan alarmas de sobre saturación a nivel de memoria como lo podemos observar en la figura 10.

Una vez analizados todos los recursos y componentes virtuales de la infraestructura virtual y física, resumimos los principales componentes en los siguientes ítems.

Total Recursos de infraestructura

Procesador: 72 core

Virtual CPU: 275

Memoria: 776 GB

Storage: 33 TB

Recursos Usados:

Máquinas virtuales: 67

Virtual CPU: 160

Memoria: 790GB

Storage: 26TB

Disponibilidad de Recursos:

CPU: 115

Memoria: -14 GB físico, sobre saturación Virtual al 26%

Storage: 7TB

Como resultado final del estudio inicial, podemos observar en la figura 10, que existe una sobre saturación de memoria al 27%.

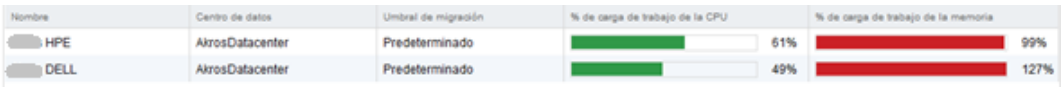


Figura 10. Estado de carga sobre Clúster

Fuente: Tomado desde ambiente de producción.

2.1.7. Resumen de Infraestructura Virtual

Para el levantamiento de esta información se usa la herramienta RVTools, misma que es de carácter gratuito y nos provee un inventario completo de todos los recursos y componentes que forman parte de un clúster a nivel de VMware; el archivo generado es bastante extenso por lo que se ha generado una ficha de observación tipo resumen en la que compactamos toda la información; para el análisis de datos se ha usado microsoft excel mediante tablas dinámicas, cuyos resultados son los siguientes:

Cantidad de máquinas virtuales y estado de encendido.

En la tabla 4, podemos observar que hay siete equipos encendidos dentro de la plataforma de virtualización, lo que ocasiona que se esté desperdiciando recursos de almacenamiento y procesamiento.

Tabla 4. Estado de Encendido de Máquinas Virtuales

Etiquetas de fila	Cuenta de Host
poweredOff	7
poweredOn	57
Total general	**64**

En la tabla 5, se resume el estado de alerta de algunas máquinas virtuales, podemos observar que 17 virtuales tienen estado gray, es decir en estado de advertencia de un posible error y 6 virtuales están en estado de error, lo que indica que esas máquinas requieren

atención inmediata ya que ocasionan error en las aplicaciones o servicios que estos equipos virtuales prestan.

Tabla 5. Estado de error de Máquinas Virtuales

Etiquetas de fila	Cuenta de Host
gray	17
green	41
red	6
Total general	**64**

En la tabla 6, se recopila la cantidad de memoria asignada a las máquinas virtuales, esta asignación no tiene justificación de uso de recursos por lo que, es necesario realizar un análisis de carga de memoria por máquina virtual para optimizar el uso de memoria.

Tabla 6. Cantidad de Virtuales por capacidad de memoria

Etiquetas de fila	Cuenta de Host
4.096	9
6.144	3
7.168	2
8.192	21
10.240	3
11.264	1
12.288	6
16.384	8
18.432	2
20.480	1
24.576	4
26.624	1
32.768	3
Total general	**64**

Dentro del ambiente virtual de la empresa, se verifica que existe dos ambientes o grupos de servidores por marca, con los que se ha implementado dos tipos de clúster denominados DELL y HPE, a simple visto se puede pensar que las máquinas virtuales están balanceadas, pero se requiere analizar capacidad de los componentes de cada clúster.

Tabla 7. Cantidad de máquinas Virtuales por tipo de Host

Etiquetas de fila	Cuenta de Host
Akros DELL	34
Akros HPE	30
Total general	**64**

El análisis de rendimiento de las aplicaciones está relacionado por el tipo y versión de sistema operativo utilizado, la tabla 8 y figura 11, muestra el resumen de sistemas operativos residentes dentro de la infraestructura institucional; podemos observar que no existe homogeneidad, misma que debe ser analizada con el propósito de mantener sistemas operativos actualizados y compatibles con las aplicaciones existentes.

Tabla 8. Cantidad de Máquinas Virtuales por Sistema Operativo

Etiquetas de fila	Cuenta de Host
CentOS 4/5/6/7 (64-bit)	2
Microsoft Windows 7 (64-bit)	2
Microsoft Windows 8 (64-bit)	3
Microsoft Windows Server 2008 (32-bit)	1
Microsoft Windows Server 2008 (64-bit)	1
Microsoft Windows Server 2008 R2 (64-bit)	8
Microsoft Windows Server 2012 (64-bit)	31
Microsoft Windows Server 2016 (64-bit)	11
Other 2.6.x Linux (64-bit)	1
Red Hat Enterprise Linux 5 (32-bit)	1
Red Hat Enterprise Linux 6 (64-bit)	1
SUSE Linux Enterprise 11 (64-bit)	2
Total general	**64**

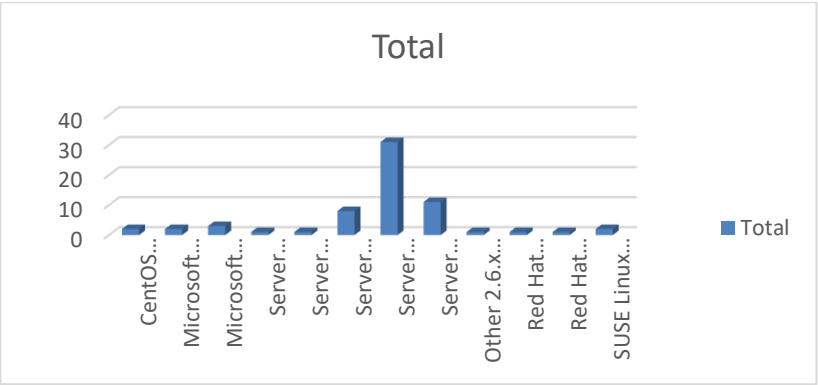


Figura 11. Resumen de Sistemas Operativos dentro de la Infraestructura

2.1.4. Escenarios de Contingencia

A continuación, se describen los posibles escenarios de contingencia a los que están expuestos los componentes de TIC de la empresa, se ha levantado los componentes principales de la infraestructura de TI y se realiza una evaluación por cada componente principal.

a) A nivel del DataCenter

El Datacenter, según datos recolectados a través de entrevistas a los encarados de sistemas de la empresa, está expuesto a una interrupción de funcionamiento por las siguientes causas:

- ✓ Daño en el sistema de suministro eléctrico (generador, UPS, PDU)
- ✓ Daño en el sistema de aire acondicionado
- ✓ Incendios
- ✓ Inundaciones
- ✓ Erupciones volcánicas

b) A nivel de Hardware

Los componentes del Datacenter y equipos de TIC están expuesto a una interrupción de funcionamiento por falla en alguno de los siguientes componentes:

- ✓ Enclousure de servidores
- ✓ Servidores
- ✓ Storage
- ✓ Switches SAN
- ✓ Switches LAN
- ✓ Sistemas de Telefonía
- ✓ Sistemas de comunicaciones (Firewall, Router, Switch, balanceadores, etc)

c) A nivel de Software

Los componentes del Datacenter y equipos de TIC están expuesto a una interrupción de funcionamiento por las siguientes causas:

- ✓ Reinicio de aplicaciones por actualizaciones no programadas (parches, firmware)
- ✓ Ataques informáticos no intencionados (Virus, troyanos, gusanos, etc)
- ✓ Daños de sistema operativo, (de fábrica, disco lleno)
- ✓ Ataques informáticos intencionados. (ataques internos o por mal uso)

2.1.5. Roles y responsabilidades

La administración de los componentes de infraestructura ya sea a nivel de hardware y software están bajo la responsabilidad del departamento de sistema, esto en lo referente a sus planes de mantenimiento y administración; sin embargo, a nivel de aplicaciones no existe un responsable especialista del mantenimiento de estos, sino que se actúa de forma reactiva; al tratarse de una empresa de soluciones tecnológicas, se cuenta con especialistas en todas las áreas, pero no existe un responsable especifico en caso de una contingencia. Para determinar lo indicado se realizó encuestas a todos los especialistas, pues a más del ambiente de producción existe un ambiente de demos y pruebas que los diferentes especialistas hacen uso para implementar ambientes de pruebas según sus necesidades y especialidad.

La encuesta se realizó a un total de 27 especialistas a cargo de las aplicaciones, las preguntas fueron de carácter cerrado en su mayoría, solicitando una respuesta del tipo SI/NO y se obtuvieron los siguientes resultados:

A) Conocimiento del Datacenter, marcas, modelos, fabricantes.

Resultados de la pregunta ¿Conoce el DataCenter de la institución?

Si	No	Total
13	14	27

El análisis de resultados nos demuestra que más del 50% de personal técnico encargado de administrar algún sistema de la empresa no conoce el datacenter, lo que sin lugar a duda denota un problema en caso de una contingencia no sabrían dónde están ubicados sus sistemas.

Resultados de la pregunta ¿Conoce la tecnología (Fabricantes) con que trabaja la empresa?

Si	No	Total
7	20	27

El 74% de los especialistas encargados de la administración de los sistemas, no conoce la tecnología del fabricante con el que trabaja la institución y menos conoce los procedimientos que se deberían aplicar en caso de una contingencia o evento por ejemplo en el momento de aplicar una garantía.

Resultados de la pregunta ¿A nivel de Storage conoce la tecnología utilizada?

Si	No	Total
2	25	27

El 92% de los especialistas encargados de la administración de los sistemas, no conoce la tecnología y/o fabricante con el que trabaja la institución a nivel de almacenamiento, es decir no conocen el sitio o dispositivo donde están almacenados la información referente a sus sistemas.

¿A nivel de dispositivos de comunicación LAN, conoce la tecnología utilizada?

Si	No	Total
7	20	27

El 74% de los especialistas encargados de la administración de los sistemas, no conoce la tecnología del fabricante con el que trabaja la institución a nivel de redes, si bien es cierto no es relevante este conocimiento tampoco existe archivos o documentación de respaldo de configuraciones que pudieran servir en caso de una contingencia o se requiera reconfigurar un dispositivo de comunicaciones.

¿A nivel de dispositivos de comunicación SAN, conoce la tecnología utilizada?

Si	No	Total
2	25	27

El 92% de los especialistas encargados de la administración de los sistemas, no conoce la tecnología del fabricante con el que trabaja la institución a nivel de almacenamiento, si bien es cierto no es relevante este conocimiento tampoco existe archivos o documentación de respaldo de configuraciones que pudieran servir en caso de una contingencia en estos dispositivos.

B) Conocimiento de Sistemas software y aplicaciones

¿Conoce la plataforma de sistemas operativos de la empresa?

Si	No	Total
24	3	27

El 88% de los especialistas encargados de administrar los sistemas de la empresa conoce el ambiente de sistemas operativos sobre el que trabaja su aplicación; en este si se dispone de un repositorio de software para recuperación del sistema operativo en caso de una contingencia.

¿El sistema que administra, mantiene sistemas de respaldos?

Si	No	Total
3	24	27

El 88% de los especialistas encargados de la administración de los sistemas indica que no dispone de un mecanismo o sistema de respaldos, lo que hace obviamente que éste sea un gran riesgo para la integridad de la información, solo 3, hacen respaldos de los archivos de configuración y base de datos.

¿El sistema que administra, mantiene niveles de replicación?

Si	No	Total
0	27	27

El 100% de los especialistas administradores de los sistemas, indican que sus sistemas no cuentan con un nivel de protección de replicación, los mismos que servirían en caso de presentarse una contingencia a nivel del datacenter completo, pues los mismos servirían para la implementación de un sitio de contingencia

¿Dispone de manuales de instalación y configuración del sistema que administra?

Si	No	Total
5	22	27

El 81,4% de los administradores de sistemas no tiene un manual de instalación, configuración y/o administración, lo que ocasiona dependencia de personas por parte de cada sistema.

¿En caso de contingencia en el sistema, está documentado el proceso de recuperación?

Si	No	Total
0	27	27

El 100% de los administradores de sistemas no tiene un manual y/o proceso de recovery, lo cual ocasionaría dependencia sobre el personal que administra la aplicación.

¿Ha sufrido una caída del sistema que ocasionó interrupción del servicio?

Si	No	Total
15	12	27

El 55% de los administradores del sistema, admite haber sido víctima de la interrupción de servicios por afectación en los sistemas, con ese porcentaje se determina que es de vital importancia disponer de un plan de recuperación ante desastres.

2.1.6. Levantamiento de aplicaciones críticas de la empresa.

Cada usuario tiene una percepción distinta de criticidad de aplicaciones, generalmente dada por el uso y utilidad de estas para las funciones que su puesto requiere, debido a lo indicado, se ha levantado una encuesta en la que los usuarios describen las aplicaciones que usan y el tiempo de uso de cada uno; de acuerdo a sus resultados se determina los sistemas críticos para el funcionamiento de institución; la encuesta se realizó a nivel nacional, pues los sistemas son centralizados y de un total de 135 usuarios la información obtenida se la resumen en la tabla 9.

¿Especifique las aplicaciones necesarias indispensables para realizar su trabajo?

Tabla 9. Cantidad de Usuarios por aplicación

Aplicación	**Usuarios**
Correo Electrónico	135
Internet	135
Herramientas de Ofimática	135
Otros	135
SGC - Sistema Gestión Incidentes	92
Project – PowerBI	35
ERP - Dynamics GP	14
Sistemas de Terceros - Fabricantes	7

De la información recopilada se analiza que, el correo electrónico, el internet y herramientas de ofimática es la que todos los usuarios la usan, estos sistemas requieren especial atención, sin embargo, se debe considerar también el tiempo de uso de cada aplicación y el tiempo máximo que un usuario podría trabajar sin dicha aplicación. En la tabla 10, verificamos el tiempo de uso diario (por horas) por cada aplicación.

¿Qué tiempo de uso asigna a las aplicaciones? Horas de Uso al día por Aplicación.

Tabla 10. Cantidad de Usuarios por aplicación

Aplicación	**1h a 2h**	**2h a h4**	**más de 4h**
Correo Electrónico			135
Internet	5	50	80
Herramientas de Ofimática	19	78	38
Otros			
SGC - Sistema Gestión Incidentes	11	13	68
Project – PowerBI	8	13	14
ERP - Dynamics GP			14
Sistemas de Terceros - Fabricantes			7

Otra medición clave, dentro del proceso de establecimiento de criticidad de aplicaciones es el tiempo que un usuario podría prescindir de un sistema sin afectar sus actividades normales, si bien es cierto, el usuario manifiesta que no podría prescindir de un sistema ni un solo minuto, se ha trabajado con las jefaturas de cada área y se establece el tiempo máximo que un usuario podría dedicar a otra actividad relacionada con su trabajo sin depender del sistema crítico, la tabla 11, resume lo mencionado.

¿Qué tiempo un sistema podría estar indispuesto, sin que llegue a afectar su productividad?

Tabla 11. Cantidad de Usuarios por aplicación

Aplicación	**1h a 2h**	**2h a h4**	**más de 4h**
Correo Electrónico		107	28
Internet	27	52	56
Herramientas de Ofimática		12	123
Otros			
SGC - Sistema Gestión Incidentes	59	31	2
Project – PowerBI	29	6	
ERP - Dynamics GP	14		
Sistemas de Terceros – Fabricantes		7	

2.2. Selección del estándar aplicado

En el desarrollo de la investigación propuesta se evaluaron varios estándares en función de seleccionar aquella que mejor se ajusta a la realidad y necesidad de la entidad y que nos ofrezca resultados favorables en cuanto a la mitigación de riesgos. Por ellos se tuvo en cuenta:

- El estándar "British Standard BS 25999"
- La norma ISO 22301:2012 (ISO 22301, 2012) y
- La ISO 27001 Sistema de la Seguridad de la Información (SGSI) (ISO 27001, 2011).

Previo a la selección de la metodología a ser usada se realizó un análisis de los beneficios que éstos pueden prestar y que mejor se acoplen a las necesidades institucionales, además se verificó la integración de otras normas con la ISO 22301, mismas que se las menciona a continuación:

- ISO 9001, Gestión de Calidad
- ISO 27000, Seguridad de la información
- ISO 31000, Gestión del Riesgo
- ISO 20000, Gestión de los Servicios TI
- ISO 15504, Calidad del SW

2.2.4. Criterios de selección

Una vez analizadas las diferentes metodologías de ejecución de un BCP/DRP y tomando en cuenta los criterios de selección de la institución enmarcados principalmente en los estándares de la industria, se verifica que los mismos cumplen con la tarea de demostrar que norma se ajusta a la realidad institucional, analizando entre otros factores su aplicabilidad y flexibilidad de implementación. Adicionalmente se establece un criterio comercial, ya que como empresa de venta de soluciones tecnológicas es de interés también la distribución de este tipo de soluciones de manera que generen también un rédito económico.

Por lo mencionado la metodología seleccionada es la ISO 22301, que es la norma internacional para la Continuidad del Negocio diseñada para proteger a su organización de un incidente inesperado.

2.2.5. Metodología Seleccionada - ISO 22301

Según describimos en la sección 1.3, los sistemas de gestión de la continuidad del negocio ayudan a una institución a restituir los procesos de negocios ante algún incidente; protegiendo la reputación de la entidad, satisfacción del cliente y evita problemas financieros.

a) Fases de un plan de recuperación de desastres (DRP)

Según la ISO 22301, las fases tradicionalmente consideradas de un BCP, DRP son:

a) Inicio del proyecto, plan de recuperación ante desastres
b) Análisis de impacto sobre el negocio (BIA)
c) Estrategias de recuperación
d) Diseño y desarrollo de estrategias de recuperación para el DRP
e) Pruebas, mantenimiento y entrenamiento del DRP

En el diagrama de bloques de la figura 12, se establece la interacción entre las diferentes fases del DRP basados en la ISO 22301.

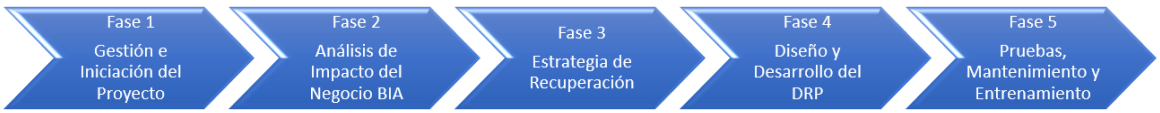


Figura 12. Fases del DRP
Fuente: (ISO, 2012)

b) Inicio del proyecto plan de recuperación ante desastres

En esta etapa se realiza un acercamiento a la entidad, evaluándose toda la documentación que existe. Se describen los beneficios a lograr y definen los recursos humanos que participaran en el proyecto con sus respectivas responsabilidades. Pueden algunas actividades como:

- Revisar las actividades críticas a tener en cuenta para el DRP
- Entender la tecnología de información.
- Valorar de una forma correcta los riesgos
- Evaluar el nivel de la empresa, junto a las acciones que permitan disminuir los niveles de respuesta frente a incidentes que incidan de forma negativa en los servicios.

c) Análisis de impacto sobre el negocio (BIA)

El BIA como vimos en apartados anteriores constituye un elemento de gran significación a tener en cuenta en un diseño de plan de recuperación de desastres, pues permite determinar los incidentes que afectan la estabilidad de los procesos o actividades más críticas asociadas a la información

d) Estrategias de Recuperación

Gestionar los riesgos en un elemento primordial en el mantenimiento de la seguridad. Representa una mezcla de varios resultados al respecto, basándose en análisis cualitativos y cuantitativos. De aquí que se asegure la agilidad y facilidad durante el proceso y la determinación de coeficientes de riesgo. Enel desarrollo de esta tarea utilizamos las normas anteriormente descritas: COBIT 5, ITIL V3, ISO27001 e ISO 27002.

- **Identificar amenazas**

La identificación de amenazas de las actividades críticas en la organización se realiza a través de la aplicación de entrevistas estructuradas a expertos que forman parte de la empresa. Estos informarán y determinarán el nivel de impacto de las amenazas teniendo en cuenta que los servicios ofrecidos tengan continuidad, así como puedan afectar desde el punto de vista financiero o de imagen.

- **Identificar vulnerabilidades de los sistemas**

Las vulnerabilidades encontradas en los sistemas de información constituyen uno de los problemas más importantes y representan una gran preocupación para la empresa; pues

pueden ser utilizadas por los softwares maliciosos para dañar la información y la infraestructura de la entidad.

De aquí que se necesite metodología que nos ayude a identificar estas vulnerabilidades y mitigar las amenazas encontradas. El diseño e implementación de un ERP para la organización permite informar de forma oportuna estos problemas encontrados. Se determina las vulnerabilidades de cada actividad critica de la empresa que podrían ser utilizadas para afectar las tareas del sistema.

- **Cálculo de la probabilidad de ocurrencia de un evento**

La probabilidad en la que ocurre un incidente se determina a través de estudios realizados en entidades del país e informes publicados por compañías líderes en seguridad de la información como “Symantec”, “Microsoft” e “Infosecurity”.

e) Diseño y desarrollo de estrategias de recuperación para el DRP

Los resultados obtenidos en el análisis de impacto en el negocio se utilizan para diseñar las diferentes estrategias de recuperación. El análisis de los datos resultado de las entrevistas y las actividades que modelan el negocio proporcionan un ranking de prioridades de recuperación atendiendo a la criticidad de los procesos.

Los sistemas que tendremos en cuenta son:

- Centro de Datos
- Servidores
- Switch LAN
- Switch SAN
- Firewall
- Almacenamientos
- Herramientas para la Comunicación
- Software

Establecidos los sistemas que deben ser protegidos, se determinan las formas de prevención y mitigación de estos ante algún tipo de fallo. De igual forma se determinan las acciones que deberán ejecutarse para lograr una recuperación de este.

f) Pruebas, mantenimiento y entrenamiento del DRP

La calidad de los resultados de la implementación de un DRP ante incidentes puede ser validada a través de un plan de pruebas que simule las condiciones reales. Esta etapa debe tener las tareas de mayor significancia que necesiten ser funcionalmente estables. Deben llevarse a cabo por los responsables ante incidentes. Algunas de los pasos que pueden llevarse a cabo son:

1. Determinar los objetivos y el alcance de la prueba
2. Configurar del ambiente de testeo
3. Preparar los datos para el test
4. Identificar el personal de control y supervisión
5. Diseñar las preguntas para evaluar los resultados obtenidos.
6. Estimar un presupuesto

2.3. Herramientas y Materiales

Haciendo uso de las mejores prácticas recomendadas por el plan de recuperación de desastres, se establecen como herramientas de recolección y análisis de datos las provistas por cada fabricante; según las aplicaciones existentes en la empresa podemos mencionar las siguientes:

- **Microsoft System Center Configuration Manager,** herramienta utilizada para la administración de ambientes Microsoft, la misma nos permite la recolección de información mediante la cual creamos inventarios de hardware y software independientemente si se trata de ambientes físicos o virtuales.
- **VMware Vcenter Server,** Herramienta utilizada para administración del ambiente virtual en línea, provee propiedades de gestión de todos los componentes del clúster VMware.

- **Rvtools,** Será utilizada para la relevación de información del ambiente virtual VMware creando un inventario completo de los componentes virtuales; permite ser exportado a Excel con lo cual podemos generar reportes manuales personalizados.
- **VMware Vrealize Operation Manager,** Gestión, proyección y predicción de fallas en ambientes virtuales
- **Veeeam Backup y Replication,** Administración gestión y monitoreo de backups y replicación de ambientes virtuales.
- **OneView,** herramienta de HPE (hewel Packard) para monitoreo y gestión de hardware

Capítulo III - Análisis y propuesta

En este capítulo se describe el resultado del estudio realizado y la implementación del plan de recuperación de desastres, así como, el análisis de resultados obtenidos luego de su aplicación y puesta en producción.

3.1. Fundamentación del Proyecto

En el análisis de la situación actual de la empresa se evidencio diferentes falencias en cuanto a la administración y gestión de los sistemas, tal como lo plasmamos en el capítulo II, se realiza un estudio para el relevamiento de los sistemas críticos de la empresa, se determina los riesgos a los que están expuestos y su probabilidad de ocurrencia, esta información permite establecer un plan de recuperación por componente de manera que permita el restablecimiento ordenado de funciones en caso de la ocurrencia de un evento no planificado.

Los aspectos importantes para tomarse en cuenta en el desarrollo del proyecto se los puede establecer de la siguiente manera:

Creación del DRP mediante la norma ISO 22301, para la creación del sitio alterno de contingencia en la ciudad de Guayaquil considerando que las aplicaciones están virtualizadas, se utilizará la herramienta líder en backup y replicación de máquinas virtuales como es Veeam Backup en su última versión.

3.2. Desarrollo del Plan de Recuperación de Desastres

Para el desarrollo del proyecto, y una vez realizado el análisis de la metodología a utilizarse se pone en práctica las fases del DRP recomendadas por la ISO 22301, se han tomado como pasos los que apliquen a la empresa, de ésta mera las fases del DRP son las siguientes:

1. Gestión e iniciación del proyecto:

- Establece un equipo de trabajo
- Establecer alcance del DRP
- Establecer funciones, procesos y estrategias de comunicación
- Establecer tareas del manejo de crisis y aplicación del DRP

2. Análisis de impacto sobre el negocio BIA:

- Análisis y estabilización de la plataforma (Inventario Hw, Sw, Aplicaciones)
- Identificación servicios/aplicaciones críticas de la empresa
- Establecer tiempos y puntos de recuperación (RTO/RPO)

3. Estrategia de recuperación:

- Análisis de riesgos, probabilidad e impactos
- Mecanismos de prevención y respuesta a incidentes
- Procedimientos de recuperación por aplicaciones y/o servicio. (Criticidad)
- Procedimientos de recuperación Local de Aplicaciones
- Procedimientos de recuperación Remota de aplicaciones – Sitio Alterno

4. Diseño y desarrollo del DRP:

- Documentación de los procesos y estrategias de recuperación
- Documentación y generación de la guía del DRP

5. Prueba, mantenimiento, y entrenamiento:

- Establecer plan de pruebas y resultados (Backups/Replicación)
- Mantenimiento y difusión del plan de recuperación de desastres DRP

3.2.1 Gestión e iniciación del proyecto

En esta fase se realiza un conocimiento de la empresa, se evalúa, la documentación existente, se define el grupo de trabajo y las personas que tendrán alguna responsabilidad en el proyecto, se establece el alcance del DRP y se especifica las tareas del manejo de crisis.

a) Establece un equipo de trabajo; se establece el personal de manejo de crisis y se establece las funciones de cada persona. En la figura 13, podemos observar el organigrama del DRP, el mismo que fue generado luego de las múltiples reuniones realizadas y los gerentes de operaciones y procesos definan los responsables de cada área.

Figura 13. Organigrama del plan de recuperación ante desastres

Junto con la creación del organigrama el siguiente paso es el establecimiento de roles y responsabilidades de cada integrante del organigrama del DRP, la table 12, establece las tareas y acciones que se debe realizar antes, durante y después de un incidente que requiera la ejecución del DRP.

Tabla 12. Roles y responsabilidad

Rol	Antes del evento	Durante el evento	Después del evento
Líder del DRP	✓ Velar por la distribución y pruebas del DRP. ✓ Gestionar la asignación de los responsables de las diferentes fases del DRP ✓ Comunicar/difundir el plan del DRP.	✓ Evaluar y activar el DRP y las estrategias de recuperación y contingencia. ✓ Comunicar a Gerencias el desastre, interrupción o evento contingente. ✓ Liderar la operación bajo contingencia y retorno a la normalidad.	✓ Evaluar el funcionamiento del DRP acorde con los inconvenientes y oportunidades de mejora visualizados durante el evento de interrupción. ✓ Informar a gerencias el retorno a la normalidad.
Líder de Sistemas	✓ Mantenimiento y actualización de los componentes del DRP. ✓ Participar en todas las fases del desarrollo y diseño del DRP. ✓ Proporcionar todas las facilidades de acceso a la infraestructura a los especialistas.	✓ Liderar la ejecución de las fases del DRP ✓ Proveer de los recursos requeridos para la ejecución del DRP. ✓ Gestionar/contactar con terceros. ✓ Gestionar los recursos en el centro de datos alterno. (si aplica)	✓ Evaluar el proceso de ejecución del DRP en pro de mejoras.
Líder de infraestructura, Líder de Networking & seguridades, líder de software.	✓ Comunicar necesidades y requerimientos. ✓ Mantenimiento de las tareas del DRP por especialidad. ✓ Participar en la ejecución de las pruebas al DRP.	✓ Evaluar el desastre, interrupción o evento contingente. ✓ Comunicar el evento y procedimiento a seguirse al Líder del DRP ✓ Verificar disponibilidad y notificar al personal requerido para atender el evento. ✓ Ejecutar procedimientos de contingencia y recuperación. ✓ Solicitar la corrección del componente afectado y realizar seguimiento de la solución.	✓ Actualizar el DRP según inconvenientes y oportunidades de mejoras.
Apoyo de mesa de ayuda	✓ Conocer de la guía del DRP. ✓ Mantener Lista de clientes, proveedores/ terceros requeridos por el DRP.	✓ Apoyar a los involucrados en el DRP, en actividades administrativas y logísticas ante una contingencia. ✓ Logística de desplazamiento de especialistas, si es requerido y proporcionar herramientas de apoyo (modem internet), acceso oficinas, etc ✓ Contacto con proveedores, si es requerido	✓ Reportar los inconvenientes y oportunidades de mejora del DRP

b) Alcance del DRP: Como parte de la gestión e iniciación del DRP, es importante en esta fase definir el alcance del DRP, en la cual debemos según el análisis del BIA se definen los sistemas críticos e importantes para el funcionamiento de la organización, por lo indicado el alcance del DRP se establece a todos los sistemas de la empresa con especial énfasis en las aplicaciones consideradas de misión crítica.

c) Funciones procesos y estrategias de comunicación: La cadena notificación cuando se presente un desastre, interrupción o evento contingente, se lo esquematiza en la figura 14.

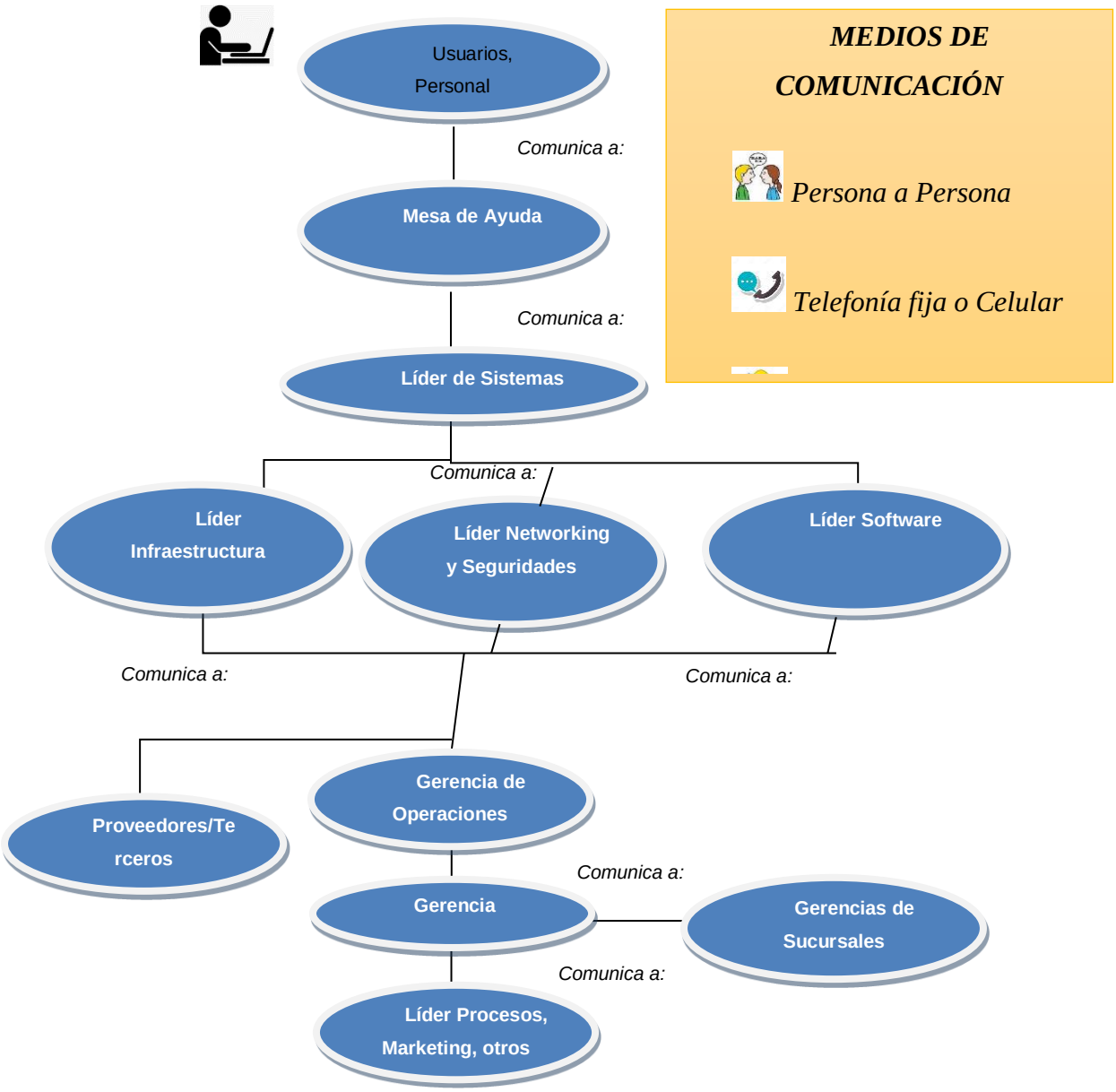


Figura 14. Cadena de Notificación de Incidentes

d) **Tareas del manejo de crisis:** se considera tareas del manejo de crisis a todas las actividades a realizarse luego de un incidente que requiera la aplicación y ejecución del DRP, dentro de las principales tares tenemos:

e) **Reporte de Incidentes**

El reporte de incidentes es evidenciado en primera instancia por los usuarios de los sistemas o a través de las alertas de monitoreo y control.

Los usuarios reportar un incidente a la mesa de ayuda cuando**:**

- No se pueden utilizar los sistemas de información.
- No hay red de comunicaciones.
- No hay servicio de correo electrónico.
- No hay acceso a los archivos electrónicos centralizados
- Cualquier otro evento de tecnología que afecte la prestación del servicio

El personal administrativo (vigilancia, servicios generales) debe reportar el incidente a Mesa de Ayuda o Líder de Centro de Cómputo cuando:

- Suena la alarma del centro de cómputo
- Hay inundación en cualquier piso
- Hay un conato de incendio
- Cualquier otro evento que afecte o pueda afectar el centro de cómputo

La mesa de ayuda debe atender el incidente de acuerdo con su procedimiento, si:

- El incidente afecta la disponibilidad de los sistemas, a nivel general.
- El incidente afecta la disponibilidad de la red de comunicaciones a nivel general.
- Ningún usuario tiene acceso al correo electrónico.
- Ningún usuario puede acceder a sus archivos electrónicos centralizados.

En cualquiera de los casos, debe escalarlo a los funcionarios responsables.

Evaluación de la magnitud e impacto del incidente:

El especialista de la plataforma afectada debe realizar un diagnóstico sobre el incidente presentado, teniendo en cuenta:

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

Finalmente, comunicarse con el Gerente de Operaciones para informar los resultados del diagnóstico.

f) ¿Cuándo debe activarse el DRP y el centro de datos alterno?

El Gerente de Operaciones, define si se activa o no el DataCenter Alterno, teniendo en cuenta los siguientes aspectos:

- Si el evento afectó considerablemente el DataCenter Principal
- Si la solución en el Datacenter principal tomará más de 24 horas.

En caso de que se active, el líder de sistemas debe comunicar la activación al proveedor de internet, teniendo en cuenta:

- Fecha y hora a partir de la cual se da inicio a la activación.
- Especialistas que participarán en el proceso de activación, para que se tramiten todas las facilidades necesarias.

El Líder de Infraestructura, coordina la ejecución de las actividades para recuperar la plataforma en el Data Center Alterno, teniendo en cuenta:

- Enrutamiento y activación de las comunicaciones hacia el Centro de Cómputo Alterno.
- Detención de la replicación de datos
- Verificación de la disponibilidad de información en el Data Center Alterno
- Activación servicio de controladores de dominio y sistema operativo en servidores
- Activación servicio de bases de datos y aplicaciones

El Líder de infraestructura, verifica la disponibilidad de la plataforma desde el Data Center Alterno, teniendo en cuenta:

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

El Gerente de Operaciones, define si comunica o no el incidente a Gerencias, caso en el cual se realizarían las actividades de manejo de crisis.

g) Actividades paralelas durante Contingencia

El Líder responsable de la plataforma afectada, activa las estrategias de contingencia locales, teniendo en cuenta los siguientes aspectos:

Si es un evento que afectó las comunicaciones,

- Configurar el Switch de contingencia, en caso de falla en el switch de Core.
- Contactar al proveedor de comunicaciones, en caso de falla en router de conexión con sucursales, falla en router ubicado en cada sucursal, falla en enlaces con ISP.
- Enrutar el tráfico por los demás switch que componen el stack, en caso de una falla de la fibra óptica de uno de ellos.
- Configurar el firewall de contingencia, en caso de falla del equipo principal.

Si es un evento que afectó la infraestructura de servidores

- Configurar/Verificar la activación del servidor de contingencia
- Confirmar la disponibilidad del storage.

Si es un evento que afectó Infraestructura de Almacenamiento y Respaldo

- Recuperación de información desde los respaldos, en caso de corrupción o borrado de la data de aplicaciones.
- Usar los datos replicados en caso de una falla del storage de respaldos local.

- **Actividades de Manejo de Contingencias**

A continuación, se listan las actividades y consideraciones necesarias para el manejo de una contingencia que afecte o pueda afectar la reputación, imagen, u operación de la empresa.

El gerente de operaciones comunica a gerencias, teniendo en cuenta los siguientes aspectos:

- Sistemas y servicios afectados
- Resultados del diagnóstico
- Acciones realizadas
- Tiempo estimado para normalizar actividades
- Riesgos a los que está expuesta la empresa y alternativas disponibles
- Cualquier otra decisión de índole gerencial.

Gerencia general junto con el equipo de manejo de crisis evalúa el incidente e impacto que puede tener para la reputación, imagen u operación de la entidad, al igual que define las acciones para afrontarla.

- **Comunicación de Crisis**

Gerencia General, a través de los funcionarios delegados, comunicará la crisis a nivel interno y externo, en caso de ser requerido. Se debe tomar en cuenta los siguientes aspectos:

- ¿Qué información concreta se tiene sobre la crisis (incidente presentado, diagnóstico, tiempo de solución)?
- ¿Qué información está en proceso de verificación e investigación?
- ¿Qué información válida se puede comunicar inmediatamente (mensaje)?
- ¿Qué información se debe manejar al interior de la entidad?
- ¿Quiénes fueron afectados por la crisis (audiencia)?
- ¿Cómo se comunicará la información a los interesados o afectados (medio)?

- **Principios en la comunicación**

La comunicación de la crisis deberá considerar los siguientes principios:

Comunicar de forma rápida y periódica: Ante una situación de crisis de alto impacto, la entidad debe establecerse como fuente primaria de información, asimismo, debe comunicar periódicamente la evolución de la atención de la crisis. Estos elementos le permitirán generar confianza y credibilidad.

Decir la verdad: Ser honestos en los comunicados, sin embargo, no significa transmitir TODA la información, sólo aquella que es suficiente para generar confianza y tranquilidad. Podrá existir información confidencial que deberá ser tratada como tal y no se necesite transmitir a los interesados.

Emitir reportes lo más exactos posible: Publicar la información que se tiene disponible, siempre y cuando ésta haya sido validada. No especular, adivinar ni presentar situaciones hipotéticas.

3.2.2 Análisis de impacto sobre el negocio BIA:

La base fundamental dentro de esta fase es contar con un inventario actualizado de los activos de la empresa, considerando que los activos se componen de los sistemas a nivel de hardware, software, servicios y aplicaciones; una vez relevada esta información corresponde hacer un análisis de los sistemas que se consideran críticos para las funciones de la empresa. Para este análisis se efectuaron encuestas a todos los usuarios y la información fue validada con las gerencias departamentales, los resultados obtenidos se los plasma en la tabla 13, donde describen los nombres de las máquinas virtuales y su descripción.

Tabla 13. Aplicaciones Críticas

Ident.	Nombre Máquina Virtual	Descripción
SRV-001	GPGYE	ERP Dynamics Replica GYE
SRV-002	GP-GUIASREMISION	Emisión Guías remisión al SRI
SRV-003	APPSGC	SGC Aplicación
SRV-004	APPSGCi	SCG aplicación Cloud
SRV-005	BDDSGC	SGC BDD Aplicación
SRV-006	BDDSGCi	SGC BDD Cloud
SRV-007	CRMDYNAMICS	ERP Dynamics, sistema financiero
SRV-008	DBSHAREPOINT	BDD Sistema de colaboración empresarial
SRV-009	DYNAMICSGP	ERP Dynamics, sistema financiero
SRV-010	GPUIO	ERP Dynamics versión 2008
SRV-011	POWERBI	Análisis del negocio
SRV-012	PROCAPP1	Servidor sgc aplicaciones pruebas
SRV-013	PROCBDD1	ERP Dynamics bdd
SRV-014	PROJECT	Servidor de Proyectos
SRV-015	SHAREPOINT	Sistema de colaboración empresarial

A más de las aplicaciones consideradas críticas parte de la gestión de sistemas se toman en cuenta los sistemas de apoyo, mismos que son necesarias para el funcionamiento de los sistemas, como son los servidores de Active Directory (AD), DNS y DHCP.

Para el cálculo del análisis de riesgo se utiliza la fórmula de la figura 15; el riesgo es igual a la probabilidad de la amenaza por la magnitud del daño, se establecen valores para cada variable y según los datos obtenidos en los sistemas se realiza la matriz de riesgos.

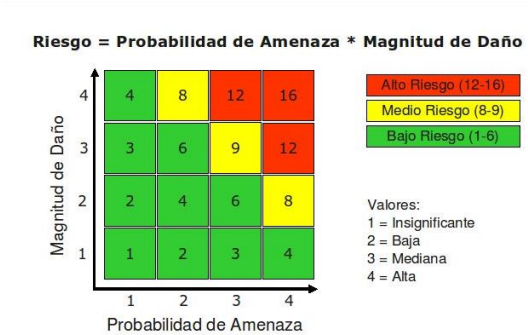


Figura 15. Cálculo de Análisis de Riesgo

Fuente: (protejete, 2019)

Una vez establecido los sistemas de gestión crítica y su nivel de criticidad corresponde establecer los tipos de protección y tiempos de recuperación; para los sistemas de criticidad alta se establecen respaldos completos semanales, incrementales diarios y replicación de la data a un sitio alterno de forma semanal; el resto de los sistemas se realizan tareas de backup semanal y no se realizar una replicación al sitio alterno, la frecuencia de los respaldos se los registra según la tabla14.

Tabla 14. Frecuencia de Respaldos

Frecuencia de respaldos según Criticidad RPO<6h			
Criticidad	**Completa**	**Incremental**	**Replicación**
Alta	Semanal	Diaria	Semanal
Media	Mensual	Semanal	No
Baja	Semestral	Mensual	No

Los puntos y tiempos de recuperación de objetos se los establece según la criticidad de los sistemas, se resumen de la siguiente manera:

Nivel de Alta Disponibilidad Local:

Para el cálculo de los niveles de disponibilidad de las aplicaciones se verifica el RPO (Recovery Point Objetive o Punto de Recuperación Objetivo) y el RTO (Recovery Time Objetive o Tiempo de Recuperación Objetivo) de la siguiente manera:

- ✓ Aplicaciones No Críticas
- ✓ Backups/Restore (RPO 12 horas) (RTO - 1hora a 4 horas), individualmente.
- ✓ Aplicaciones Críticas
- ✓ Backup/Restore (RPO 4 horas) (RTO – 5min – 3 horas), Individualmente

Nivel de Alta Disponibilidad Sitio Alterno:

- ✓ Aplicaciones No Críticas
- ✓ No existe contingencia remota
- ✓ Aplicaciones Críticas

- ✓ Activar DRP-Sitio alterno (RPO 1 semana) (RTO - 1horas – 3 horas), Individualmente

3.2.3 Estrategia de recuperación:

En esta fase se realizó el análisis de riesgos y probabilidad de ocurrencia de un incidente no planificado y el impacto que pueda causar dentro de la organización, este análisis se lo realizo por cada uno de los componentes, la tabla 15 muestra un ejemplo de respuesta a incidentes a nivel del datacenter y de hardware de servidores, el análisis completo de todos los componentes de la infraestructura se los adjunta en el anexo 1.

Tabla 15. Respuesta ante Incidentes

Datacenter							
Contingencia/Riesgo	Impacto		Probabilidad		Prioridad	Prevención/Mitigación	Respuesta Incidente
Sismo/Erupción Volc	Alto	3	Alto	3	9	DataCenter Alterno	Activar DRP
Inundación	Alto	3	Bajo	1	3	DataCenter Alterno	Validar Activar DRP
Incendio	Alto	3	Medio	2	6	DataCenter Alterno	Validar Activar DRP
Eléctricos	Alto	2	Medio	2	4	Generador Edificio/UPS	Activar Generador / UPS
Aire Acondicionado	Alto	2	Bajo	1	2	Mantenimiento	Spled Backups Proveedor
Hardware Servidores							
Contingencia/Riesgo	Impacto		Probabilidad		Prioridad	Prevención/Mitigación	Respuesta Incidente
Maimboard/Tarjetas	Alto	3	Bajo	1	3	Alta Disponibilidad de H	Automática - Cluster
Memoria	Medio	2	Medio	2	4	Dispositivo Redundante	Automático - Activación
Procesador	Alto	3	Medio	2	6	Dispositivo Redundante	Automático - Activación

En la tabla resumen se observa la respuesta al incidente que debe ser acompañada del procedimiento de recuperación a nivel de aplicación, para lo cual se establece una tabla resumen de configuración y procedimiento de recuperación ya sea local o remota de cada sistema que debe ser aplicado cuando se active el DRP, la información de cada sistema se verifica en la tabla 16, donde se establece los datos principales de cada aplicación.

Tabla 16. Información de Sistemas

INFORMACIÓN GENERAL				
Nombre de la aplicación	MS Exchange	**Administrador**	Nombre del Especialista de la aplicación	
Versión completa	MS Exchange Server 2016 SP1	**Tipo:**	(físico/virtual): Virtual	
Componentes de Aplicación	MSExchange MailBox MSExchange CAS	**Sistemas Dependientes**	Active Directory	
Función Detallada:	Servidor de mensajería que me permite el intercambio de correo electrónico entre usuarios internos y externos.	**Información básica:**	IP/máscara	Direccón Ip más tipo de red (192.168.100.x/24)
			Gateway	192.168.100.254
			DNS	192.168.100.10
			Nombre Equipo	Equipo.dominio.local
			Sistema Operativo, versión, idioma.	Windows server datacenter 2012 r2, inglés
			Discos:	C:80GB, D:300GB
			Memoria/CPU	16GB/8Core
Repositorio Instaladores	Fileserver\software			

Dentro de la información de los sistemas se genera también el proceso de recovery de cada aplicación, un ejemplo del procedimiento lo verificamos en la figura 16, en la cual describe el paso a paso de recovery en el sitio de contingencia de uno de los sistemas.

El siguiente procedimiento debe ser realizado en caso de que la máquina virtual en el sitio principal esté indisponible y se requiere acceder a la aplicación desde el sitio alterno (GYE)

- Desconectar tarjeta de red virtual
- Iniciar máquina virtual con administrador local
- Cambiar nombre máquina virtual
- Cambiar IP
- Eliminación/registro de IP y nombre en el servidor DNS
- Solicitar cambio de publicación de nuevas IPs en el firewall
- Sincronizar base de datos
- Sincronización con directorio activo.
- Pruebas de conectividad
- Verificación de estado y contingencia de Datos (RTO)
- Sincronización/actualización de datos
- Pruebas generales
- Puesta en producción.

Figura 16. Ejemplo Proceso Recovery

3.2.4 Diseño y desarrollo del DRP

Como resultado del estudio se obtiene la guía del plan de recuperación de desastres, en el cual se especifica la implementación de cada uno las fases del DRP, acompañada de la información generada en el estudio de los sistemas de la empresa; las tecnologías utilizadas

fueron seleccionadas en base a las herramientas líderes en el mercado según el cuadrante de Gardner.

3.2.5 Prueba, mantenimiento, y entrenamiento:

El DRP está enfocado a la protección de la plataforma tecnológica que soporta los **procesos críticos de la empresa**

Supuestos: La efectividad en la ejecución del DRP, ante la ocurrencia de un evento de desastre o interrupción que afecte la plataforma tecnológica, se fundamenta en los siguientes supuestos:

- ✓ Se dispone de la infraestructura y recursos que soportan las estrategias de contingencia y recuperación para los sistemas críticos. (HW, SW, Sitio alterno)
- ✓ Los Administradores de aplicaciones que ejecutan el DRP, se encuentran disponibles y no ha sido afectados por el desastre.
- ✓ El desastre no afectó simultáneamente al Datacenter principal y al Datacenter alterno.
- ✓ Se han realizado las pruebas de las estrategias y procedimientos al menos 1 vez al año, y han funcionado.
- ✓ Los administradores y personal involucrado han participado en las pruebas y capacitaciones realizadas.
- ✓ Se dispone de los sistemas de respaldos/replicación de las aplicaciones críticas de la empresa con las frecuencias establecidas.

3.2.5.1 Actividades de mantenimiento del DRP

Como parte de las políticas de la empresa, se establece como responsabilidad del Líder de Sistemas coordinar la actualización de las nuevas versiones al DRP, y la comunicación de estas a todo el personal involucrado.

La actualización y mantenimiento al DRP se debe realizar:

- ✓ Cuando ha transcurrido un año desde la última actualización.
- ✓ Cuando han ocurrido cambios en la plataforma tecnológica objeto del alcance de esta guía.

- ✓ Cuando los resultados de las pruebas requieren actualización del DRP o sus procedimientos.
- ✓ Cuando hay cambios en el personal responsable del DRP.

Para los demás integrantes y responsables del mantenimiento del DRP, la tabla 17 esquematiza las actividades, responsables y la frecuencia de ejecución de estas.

Tabla 17. Actividades de Mantenimiento del DRP

No	Actividad	Responsable	Frecuencia
1.	Actualización de los procedimientos de recuperación y contingencia de la plataforma tecnológica	Lider de sistemas; líderes Especialistas, Infraestructura, Networking&Seguridades, Software	Cada vez que se realice un cambio a la infraestructura de producción o se realice una prueba de contingencia
2.	Sincronización/verificación de información replicada en el Data Center Alterno	Lider de Infraestructura Lider y encargado de Sistemas	Semanal
3.	Ejecución/Monitoreo de la infraestructura respaldada en el Data Center Principal.	Lider de Infraestructura Lider y encargado de Sistemas	Permanente
4.	Ejecución de pruebas periódicas para verificar el correcto funcionamiento de los sistemas respaldados/replicados	Especialista de Infraestructura Lider de sistemas	Semestral
5.	Ejecución Tareas de mantenimiento infraestructura hardware/software	Lider de Sistemas	Semestral o cada vez que se realice un cambio a la infraestructura de producción

3.2.5.2 Distribución de la guía

Una vez aprobada deberá ser entregado bajo las siguientes consideraciones:

Se debe entregar una copia final COMPLETA del DRP a:

- Gerencia de Operaciones
- Líder de Sistemas

- Gerencia de Procesos
- Líderes técnicos

Las diferentes copias del documento guía deben ser controladas, y cada que se cambie de versión, se deberá recoger las versiones anteriores.

3.3. ANÁLISIS DE RESULTADOS

Para el análisis de resultados se considera algunos grupos de elementos según cada fase por lo que se realiza un análisis comparativo de un antes y un después del estado de los sistemas; los aspectos relevantes se los esquematiza de la siguiente manera:

3.3.1. Levantamiento de información

Existía información básica y no centralizada de algunos sistemas, como resultado de la investigación se entrega un inventario completo a nivel de hardware de todos los componentes de TI, (UPS, Servidores, Storage, Switches LAN, SAN, etc) a nivel de software se realiza un levantamiento de información completa de todos los aplicativos con los que cuenta la empresa, para facilidad de este levantamiento de información se implementó la herramienta de Microsoft System Center Configuration manager.

A nivel de aplicaciones, se realiza un relevamiento de la información tomando en cuenta a todos los usuarios finales y no solo a los administradores de los sistemas, con el cual se logró cubrir de forma completa el inventario inclusive en las sucursales de la empresa.

3.3.2. Análisis de datos

Una vez realizado el levantamiento de la información se inicia el análisis del estado actual de los sistemas y de los niveles de protección con los que contaban; se pudo evidenciar que cada sistema funcionaba de forma independiente y no guardaban ninguna sincronía entre los mismos a pesar de que en algunos casos existía dependencias, como resultado del análisis y luego de implementado los correctivos necesarios se evidencia los resultados y resumirlos a continuación.

a) ¿Conoce el DataCenter de la institución?

Como correctivo del caso se realizaron capacitaciones y charlas informativas en las cuales se realizaron visitas al Datacenter de la empresa; luego de aplicado el correctivo, podemos evidenciar que el 100% de los especialistas y administradores de sistemas conocen el Datacenter.

Antes:

Si	No	Total
13	14	27

Después:

Si	No	Total
27	0	27

b) ¿Conoce la tecnología (Fabricantes) con que trabaja la empresa?

Como correctivo a esta interrogante se realizaron capacitaciones y charlas informativas en las cuales se realiza una capacitación sobre las tecnologías con las que trabaja la empresa, logrando de esta manera que el 100% de los especialistas conozcan la infraestructura informática de la empresa.

Antes:

Si	No	Total
7	20	27

Después:

Si	No	Total
27	0	27

c) ¿Conoce la plataforma de sistemas operativos de la empresa?

Para la corrección a esta interrogante se realizó una capacitación y charlas informativas en las cuales se realiza una capacitación sobre las tecnologías de sistemas operativos con las que trabaja la empresa, con lo cual se logra que el 100% de los especialistas conozcan la infraestructura informática del DataCenter.

Antes:

Si	No	Total
24	3	27

Después:

Si	No	Total
27	0	27

d) ¿El sistema que administra, mantiene respaldos?

Como medida de solución a este vacío que existía en los sistemas se implementa la solución de respaldos de veeam backup, misma que es implementada dentro de la plataforma de virtualización y se integra a todo el ambiente virtual de la empresa, logrando que el 100% de los sistemas de la empresa estén respaldados, lo cual permite incrementar el nivel de protección y respuesta de recuperación ante un incidente de un sistema.

Antes:

Si	No	Total
3	24	27

Después:

Si	No	Total
20	7	27

e) ¿El sistema que administra, mantiene niveles de replicación?

Como correctivo a esta actividad, se implementa la solución de replicación de veeam backup, misma que es implementada dentro de la plataforma de virtualización y se integra a todo el ambiente virtual de la empresa, logrando que el 59% de los sistemas críticos de la empresa tengan una replicación de la máquina virtual en un sitio alterno o sitio de contingencia; para nuestra implementación, el sitio de contingencia está en el datacenter de la ciudad de Guayaquil.

Antes:

Si	No	Total
0	27	27

Después:

Si	No	Total
16	11	27

f) ¿Dispone de manuales de instalación y configuración del sistema que administra?

Se evidencia que la empresa no tiene documentación de los sistemas, como respuesta a esta falencia junto con el departamento de procesos de la empresa, se establece como un requerimiento obligatorio la generación de manuales de instalación y configuración de los sistemas, con lo cual se logra que el 100% de los sistemas dispongan de esta información dentro del repositorio institucional de la información.

Antes:

Si	No	Total
5	22	27

Después:

Si	No	Total
27	0	27

g) ¿En caso de contingencia en el sistema, está documentado el proceso de recuperación?

La empresa no tiene documentación de los sistemas, como respuesta a esta falencia junto con el departamento de procesos de la empresa, se establece como un requerimiento obligatorio la generación de manuales de contingencia en el cual consten el proceso de reconstrucción, reinstalación o proceso de recovery de un sistema, logrando que el 100% de los sistemas críticos de la empresa puedan recuperarse en caso de ser necesario.

Antes:

Si	No	Total
0	27	27

Después:

Si	No	Total
27	0	27

A nivel de componentes del Datacenter se obtienen las siguientes observaciones:

- La plataforma informática al momento se encuentra sobrecargada en cuanto a memoria (10% sobrecarga)
- Nivel de contingencia de hardware: 0; en el supuesto caída de un servidor DELL el 30% de máquinas virtuales no trabajarían.
- Los 3 servidores DELL están fuera de garantía (finalizó 2016)
- Los 4 servidores HPE están fuera de garantía y no se recomienda la actualización de esta debido a la obsolescencia de la tecnología que tiene más de 10 años.
- No existe proyección de crecimiento para aplicaciones futuras.
- A nivel de switches SAN no existen equipos redundantes.

Creación de documentación por sistemas

Una vez realizado el análisis de aplicaciones y según el análisis de impacto en el negocio (BIA) se crea una lista de aplicaciones críticas, estas aplicaciones se les presta especial cuidado y se establece un nivel de protección mayor a las aplicaciones normales. Para todos los sistemas se crea la documentación que permita conocer su configuración actual, su proceso de alta disponibilidad local y su proceso de replicación y recuperación

desde un sitio alterno en caso de una contingencia, la mencionada documentación no existía y resulta de gran importancia para el DRP.

Creación del DRP

Se ha mencionado durante el desarrollo de la investigación, la empresa no contaba con un plan de recuperación de desastres y finalmente se puede evidenciar que el DRP permite a la empresa contar con un nivel de respaldo ante alguna eventualidad proporcionando tranquilidad en todos los niveles organizacionales de la empresa.

Sitio de contingencia

Como recomendaciones del DRP se crea un sitio alterno o sitio de contingencia en la ciudad de Guayaquil, en la misma serán replicadas las aplicaciones críticas de la empresa logrando aumentar el nivel de protección; los lineamientos generales de la implementación son:

- Licencia Veeam Backup Enterprise Plus 12 CPUs
- Servidor 256 GB/2 Procesadores de 16 Core
- Storage con capacidad de 5.2 TB

Según GARTNER, las recomendaciones de los fabricantes líderes a nivel mundial según como VMWARE y HYPER-V bajo las mejores prácticas sugeridas, la implementación del sistema de backups a nivel local se la evidencia en la figura 17.

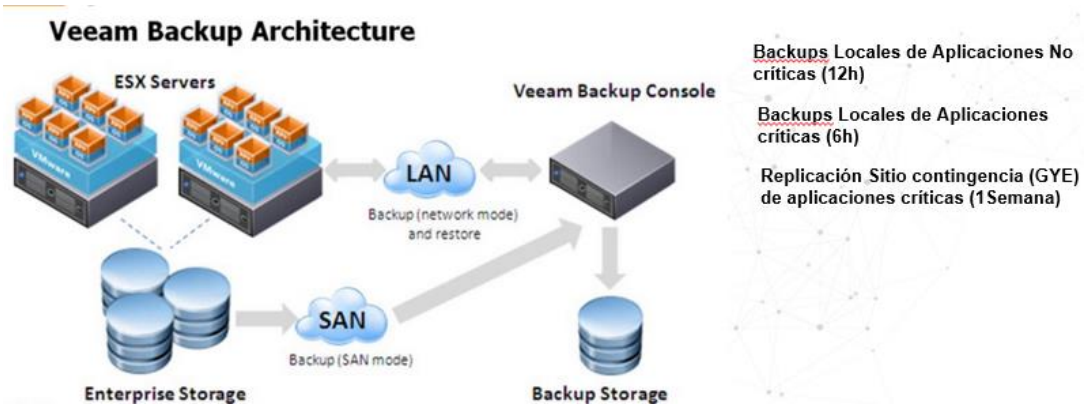


Figura 17. Arquitectura de Backup y Replicación
Fuente: (VMware, Inc, 2019)

Una de las características del software implementación es la opción de recuperación mediante la opción de vPower, ésta tecnología permite, en caso de una contingencia, iniciar una máquina virtual directamente desde el repositorio de respaldos sin necesidad de restaurar la data, con lo cual logramos el encendido inmediato de una aplicación, posteriormente el sistema en línea puede realizar la tarea de restauración sin afectar el rendimiento de la misma, la forma en la que trabaja ésta característica de la solución la esquematizamos en la figura 18. Las características de la tecnología permiten establecer menores tiempos de RTO y RPO en la recuperación de sistemas.

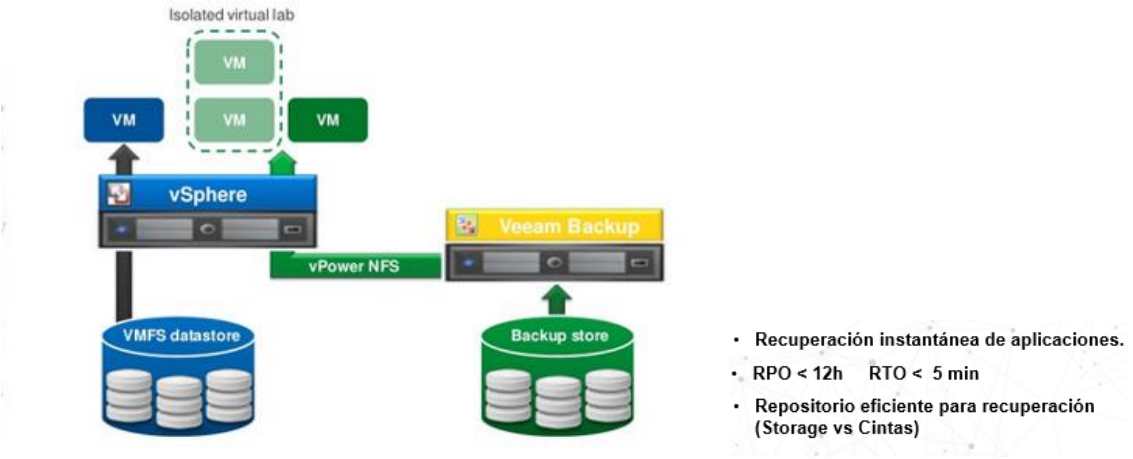


Figura 18.Arquitectura de Recuperación Instantánea
Fuente: (Veeam , 2019)

Para el sitio alterno o sitio de contingencia se implementó en la sucursal más grande de la ciudad de Guayaquil un sitio de Contingencia en el cual las aplicaciones críticas se replican y residen permitiendo de esta manera contar con un sistema con un nivel mayor

de disponibilidad y protegidos ante eventos catastróficos, su arquitectura se la evidencia en la figura 17.

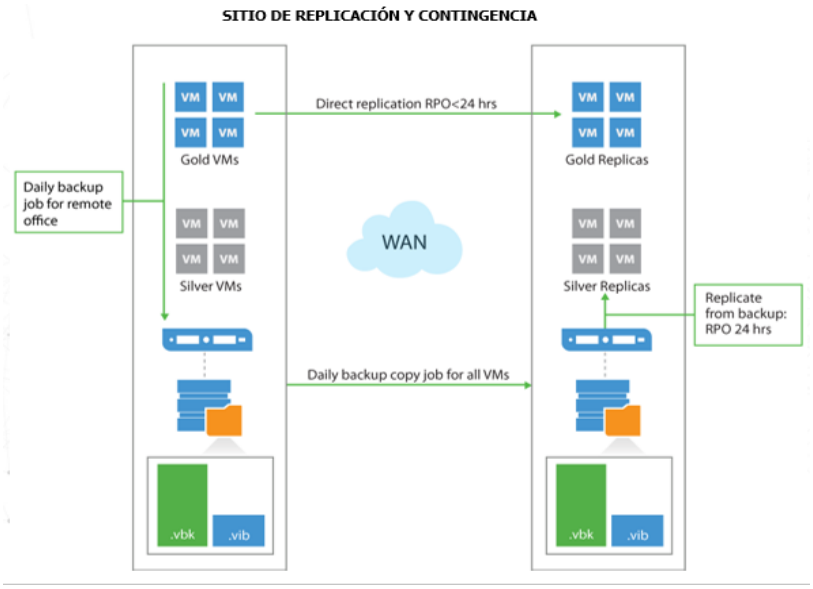


Figura 19.Arquitectura de Replicación

Fuente: (Veeam , 2019)

Con la implementación del sitio de contingencia en la ciudad de Guayaquil, se consigue subir el nivel de protección y contingencia de los sistemas de la empresa.

3.3.3. Herramientas implementadas

Debido a las nuevas necesidades que faciliten la administración y gestión de los sistemas, se implementó varias herramientas con los que no contaba la institución, que se las menciona a continuación.

a) **VMware Vrealize Operation Manager,** utilizada para la gestión, proyección y predicción de fallas en ambientes virtuales, con esta herramienta además de enviar notificaciones en caso de errores podemos realizar una predicción de recursos con lo cual los administradores pueden proveer recursos y emitir informes al área financiera para proyecciones de inversión justificadas en Tecnología.
b) **Veeeam Backup y Replication,** se contaba inicialmente con la herramienta solo con el módulo de backup, pero se amplió su funcionalidad en las funciones de replicación, con lo cual se mantiene el ambiente virtual de aplicaciones críticas de la empresa en el sitio remoto.

c) **OneView,** herramienta de HPE (Hewel Packard) para monitoreo y gestión de hardware con la cual se activan los monitoreos de hardware en el cual se reportan errores en este nivel de los ambientes del fabricante HPE.

La implementación de las herramientas mencionadas permite a la empresa mantener un monitoreo permanente y en línea de las aplicaciones y servicios.

Conclusiones

Se ha cumplido con los objetivos de la investigación propuestos, creando una guía con el plan de recuperación de desastres en donde se analizaron y se evaluaron las características principales de la empresa de Soluciones Tecnológicas, con el fin de identificar los posibles puntos de falla y de esta manera crear planes de prevención y remediación en caso de incidentes

La selección de la metodología se la realizó luego de un análisis de los estándares de la industria a nivel mundial, con el objetivo de extraer lo mejor de cada una, en donde se pudo establecer como base de la investigación, la norma ISO 22301.

En Ecuador se han suscitado varios eventos o catástrofes que han puesto en riesgo el accionar de las empresas, la historia evidencia que existen una gran problemática asociada a la continuidad de los procesos en las organizaciones del país. De aquí que, este tema se incorpore en los diseños curriculares de las carreras asociadas y para el caso de empresas de soluciones tecnológicos, como un producto a ser comercializado.

Para la elaboración e implementación del DRP fue esencial tener el apoyo de las gerencias, demostrando la significancia de este en función de las ventajas que tendrían las empresas.

Además, en la elaboración del DRP las etapas iniciales de “evaluación de amenazas y riesgos” y “análisis de impacto en el negocio” BIA, constituyen la base del plan propuesto. Las mismas proporcionan la información de partida, por lo que una mala evaluación de los riesgos y amenazas traerían consigo un deficiente diseño del BIA.

Se debe mencionar que no se pueden descubrir todas las amenazas, ni las mismas desaparecen solo por implantar un DRP, sino que el plan permiten, en gran medida disminuir

los impactos de las amenazas y recuperar las actividades en un menor tiempo en caso de algún problema en la organización.

Finalmente, queda señalar que en la propuesta se han agregado puntos específicos en cada fase, sugeridos sobre cómo aplicar el DRP, reforzándolo con puntos que, por investigaciones detalladas en este trabajo, van a funcionar de forma eficiente y eficaz logrando como resultado una metodología para la implementación y desarrollo de un Plan de Recuperación de Desastres.

A nivel empresarial, con un enfoque a las áreas de TI, se consigue:

- Evaluar y analizar la infraestructura de TIC
- Realizar una valoración de la criticidad de aplicaciones.
- Establecer las aplicaciones críticas de la empresa.
- Se establece lineamientos de backup y recuperación de aplicaciones locales.
- Se establece RPO menor a 4 horas para aplicaciones críticas y, menor a 12 horas para aplicaciones no críticas.
- Establecer recomendaciones de prevención y recuperación de infraestructura a nivel de hardware
- Crear un sitio alterno en la ciudad de Guayaquil (contingencia) para recuperación de aplicaciones críticas en caso de una contingencia.
- Establecer un RPO de una semana en el sitio alterno.
- Crear la documentación de los sistemas de la empresa y sus procesos de instalación, y recuperación.
- Establecer que el nivel de protección de los sistemas inicialmente estaba en el 20%, y luego de la implementación del plan de recuperación ante desastres, se logran niveles de protección de los sistemas críticos cercano al 100%, esto no quiere decir que el sistema es inmune; es mejor… pero hay que considerar que el punto de recuperación RPO o ventana de tiempo de "pérdida de información" oscila entre 0,25 a 8 horas.

Recomendaciones

La aplicación de la guía deberá ser revisada y aplicada por gerencias y departamentos de procesos.

El buen funcionamiento de la guía depende en gran parte de la difusión de esta, para lo cual debe ser establecida como un proceso institucional y por ende ser difundida a los departamentos y personal correctas con el objetivo de que sea visible y conocida por todos.

La guía no es estática, al contrario, en completamente dinámica y debe ser revisada y actualizada al menos una vez por año, cuando se ha generado un incidente o cuando exista un cambio o actualización en alguno de los componentes de tecnología.

Se debe establecer un cronograma y se debe cumplir el plan de pruebas recomendado, con el propósito de probar que los planes de acción establecidos funcionen cuando las circunstancias así lo requieran.

Se deberá aplicar las recomendaciones dadas a nivel de tecnología en lo referente a los componentes de TIC faltante para el cumplimiento total del DRP.

La aplicación práctica tiene como alcance los sistemas críticos de la empresa, sin embargo, se recomienda que la aplicación de estos métodos de protección y recuperación de ante fallas, sea extendida a todos los sistemas de la empresa.

El sitio de contingencia está configurado de forma activa-pasiva, se recomienda una inversión, con el propósito de lograr un sitio de contingencia tipo activo-activo, con lo cual se obtendrá un tiempo de recuperación ante desastres menor a 30 minutos.

Bibliografía

Casillas, M. (13 de Junio de 2018). *inbest.solutions*. Obtenido de https://inbest.solutions/que-es-un-drp/

Castro, A., & Bayona, Z. (2011). Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios. *Ingeniería, 16*(2), 56-66.

Gerónimo, R. (2014). Diseño de un plan de recuperación ante desastre (drp) para salvaguardar las operaciones del área de tecnologías de la información y la comunicación ante una situación de desastre. Caso: Institución Educativa Loyola. *Revista ingeniería en redes y telecomunicaciones, 1*(1), 18-29.

Gobierno de Canarias. (2017). *Seguridad y Alta Disponibilidad*. Obtenido de http://www3.gobiernodecanarias.org/medusa/ecoblog/flopmarl/seguridad-y-alta-disponibilidad

Heng, G. H. (2013). *A Manager's Guide to ISO 22301 Standard for Business Continuity Management System (LITE): An Organizational Journey to BC Management System. GMH Continuity Architects.* Australia: GMH Continuity Architects.

INEC. (2017). *Ecuador en Cifras.* Quito: INEC.

ISO. (2012). *Norma ISO 22301.* Switzerland: ISO Copyright office.

Isotools. (2016). *Normas ISO 22301*. Obtenido de https://www.isotools.org/2016/03/10/e-book-norma-iso-22301-y-continuidad-negocio/

Mendoza, M. A. (2 de Febrero de 2014). *En que consite un Plan de Recuperación ante Desastres.* Obtenido de https://www.welivesecurity.com/

Pastor, S., & Candy, S. (2014). *Análisis y diseño de un sistema de gestión de continuidad de negocio en caso de ocurrencia de sismos para una empresa aseguradora local basado en la ISO/IECD 22301.* Perú: Pontificia Universidad Católica del Perú.

protejete. (7 de 1 de 2019). *Gestión de Riesgo en la Seguridad Informática*. Obtenido de https://protejete.wordpress.com/gdr_principal/analisis_riesgo/

Rojas, J. D. (2017). *Propuesta de un plan de continuidad de negocio para una institución financiera del sector privado bancario del Ecuador.* Quito: Universidad de las Américas.

Veeam . (2019). *Veeam Backup & Replication* . Veeam Software.

VMware, Inc. (15 de Enero de 2019). *vmware.com*. Obtenido de https://www.vmware.com/latam/solutions/virtualization.html

welivesecurity. (21 de 1 de 2019). *welivesecurity*. Obtenido de https://www.welivesecurity.com/

Anexos

Anexo 1. Formato levantamiento de información de Sistemas

GUÍA DE CONFIGURACIÓN DE APLICACIONES Y SISTEMAS.

REVISIONES Y APROBACIONES:

REGISTRO DE CAMBIOS

No. VERSIÓN	FECHA	MODIFICACIÓN	REALIZADA POR:
1.0	30 de noviembre de 2018	Versión inicial	especialista
Haga clic aquí para escribir texto.	Haga clic aquí para escribir una fecha.	Haga clic aquí para escribir texto.	Haga clic aquí para escribir el nombre.

Tabla 18. Registro de Cambios

REVISORES

No. VERSIÓN	FECHA	MODIFICACIÓN	REVISADA POR:
1.0	30 de noviembre de 2018	Versión inicial	Líder Sistemas
1.0	30 de noviembre de 2018	Versión inicial	Líder del DRP
1.0	30 de noviembre de 2018	Versión inicial	Gerente de Operaciones

Tabla 19. Revisores

PERSONAL A CARGO

A continuación, se detalla el personal a cargo del levantamiento de la información de los sistemas de Akros:

Cargo	Personal	Descripción
Líder Técnico	NOMBRE	Líder Networking & Seguridades
Especialista	NOMBRE	Especialista Seguridades

ANTECEDENTES

La guía de recuperación de desastres de TI (DRP), requiere que los sistemas de la empresa estén debidamente documentados con la información de instalación y configuración, así como la descripción de funciones y servicios que presta y su cobertura.

OBJETIVOS

Mantener información de sistemas y aplicaciones actualizados que permitan:

- Disponer de información de configuración de sistemas y aplicaciones
- Disponer de procedimientos de prevención y protección de sistemas y aplicaciones
- Disponer de procedimientos de restauración de sistemas y aplicaciones

Información General

INFORMACIÓN GENERAL			
Nombre de la aplicación	MS Exchange	**Administrador**	Nombre del Especialista de la aplicación
Versión completa	MS Exchange Server 2016 SP1	**Tipo:**	(físico/virtual): Virtual
Componentes de Aplicación	MSExchange MailBox MSExchange CAS	**Sistemas Dependientes**	Active Directory

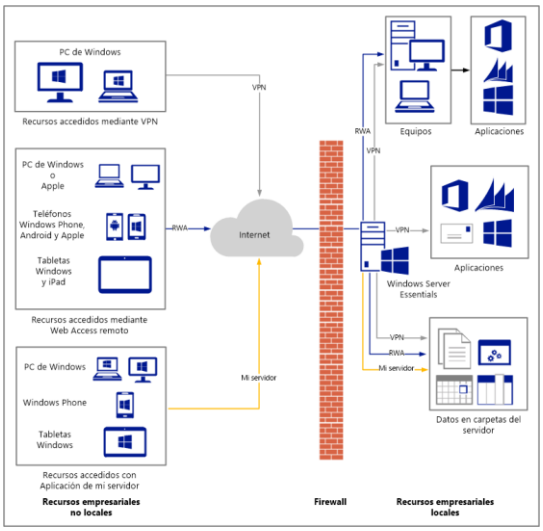
Función Detallada:	Servidor de mensajería que me permite el intercambio de correo electrónico entre usuarios internos y externos.	**Información básica:**	IP/máscara	Direccón Ip más tipo de red (192.168.100.x/24)
			Gateway	192.168.100.254
			DNS	192.168.100.10
			Nombre Equipo	Equipo.dominio.local
			Sistema Operativo, versión, idioma.	Windows server datacenter 2012 r2, inglés
			Discos:	C:80GB, D:300GB
			Memoria/CPU	16GB/8Core
Repositorio Instaladores	Fileserver\software			

PROCESO DE INSTALACIÓN:

A continuación, los lineamientos generales de instalación del aplicativo

- Instalación sistema operativo
- Instalación actualizaciones de Windows
- Asignación de (IP, nombre equipo)
- Integración al directorio activo
- Instalación MS Exchange server 2016
- Instalación Parches, CU Exchange
- Creación de base de datos de correo mailbox
- Creación de buzones
- Pruebas de envío / recepción

DIAGRAMAS FISICO/LOGICO DE CONEXIONES



RECOMENDACIONES DE BACKUP

- Respaldos de máquina virtual completo
- Respaldo de archivos de base de datos (priv, pub)
- Respaldo de archivos de configuración

PROCESO DE RECOVERY SITIO DE CONTINGENCIA

El siguiente procedimiento debe ser realizado en caso de que la máquina virtual en el sitio principal esté indisponible y se requiere acceder a la aplicación desde el sitio alterno (GYE)

- Desconectar tarjeta de red virtual
- Iniciar máquina virtual con administrador local
- Cambiar nombre máquina virtual
- Cambiar IP
- Eliminación/registro de IP y nombre en el servidor DNS
- Solicitar cambio de publicación de nuevas IPs en el firewall
- Sincronizar base de datos
- Sincronización con directorio activo.
- Pruebas de conectividad
- Verificación de estado y contingencia de Datos (RTO)
- Sincronización/actualización de datos
- Pruebas generales
- Puesta en producción.

LINEAMIENTOS GENERALES

- Incluye cualquier información relevante para el mantenimiento del sistema en cuestión.

TAREAS DE MANTENIMIENTO

- Desfragmentación de base de datos mensual
- Eliminación de LOGs semanal

APROBACIONES

Gerente Operaciones	Líder Sistemas
Firma:	Firma:
Líder Software	**Especialista software**
Firma:	Firma:

Anexo 2.Matriz de Respaldos

Nombre del Documento:	**Matriz de Respaldos de información**		
Nivel de Confidencialidad:	**Confidencial:** No debe ser conocido por personal ajeno al proceso de Gestión de Seguridad de la Información.		
Codificación:		Versión:	1.0
Fecha de última modificación:		Fecha de Creación:	10/12/2018
Elaborado por:	Jefe Sistemas		
Revisado por:	Lider de Infraestructura		
Aprobado por:	Gerente de Operaciones		

Confidencial: No debe ser conocido por personal ajeno al proceso de Gestión de Seguridad de la Información. No puede ser distribuído públicamente.

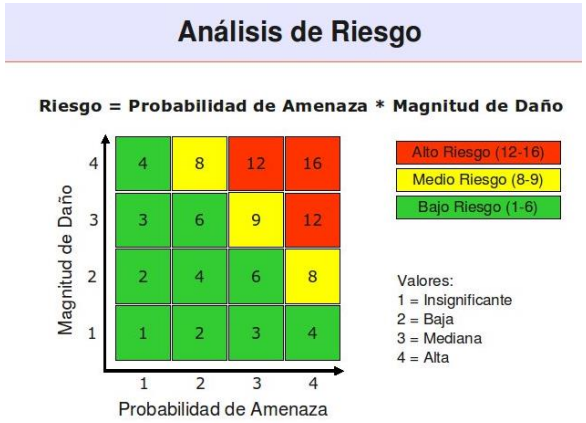
Identificador	Nombre	Descripción	Tipo	Ubicación	Almacenamiento VM	Responsable
SRV-001	Server-ADP	Servidor Dominio Principal	Máquina Virtual	DataCenter UIO	Storage HPE	Jefe Sistemas
SRV-002	Server-ADS	Servidor Dominio Secundario	Máquina Virtual	DataCenter GYE	Storage DELL	Jefe Sistemas

Nivel Criticidad	Respaldo Full	Respaldo Incremental	Retención	Repositorio	Tamaño Full	Tamaño Increm	Tiempo Full	Tiempo Incremetal
Alto	Semanal : Sábado 18h00	Diario : LMMJV 19h00	Mensual	StoreOnce				
Bajo								

Anexo 3.Matriz de Respuestas ante Incidentes

Calificación de Impacto	
Alto	3
Medio	2
Bajo	1

Calificación de Probabilidad	
Alto	3
Medio	2
Bajo	1



Prioridad= Impacto x Probabilidad

Riesgos, impacto, probabilidad y respuesta

Datacenter									
Contingencia/Riesgo	Impacto		Probabilidad		Prioridad	Prevención/Mitigación	Respuesta Incidente	Cumple	Alcance	Recomedaciones
Sismo/Erupción Volc	Alto	3	Alto	3	9	DataCenter Alterno	Activar DRP	Si	Solo Aplicaciones Críticas	Ampliar cobertura todas App
Inundación	Alto	3	Bajo	1	3	DataCenter Alterno	Validar Activar DRP	Si	Solo Aplicaciones Críticas	Ampliar cobertura todas App
Incendio	Alto	3	Medio	2	6	DataCenter Alterno	Validar Activar DRP	Si	Solo Aplicaciones Críticas	Ampliar cobertura todas App
Eléctricos	Alto	2	Medio	2	4	Generador Edificio/UPS	Activar Generador / UPS backup	Si	Datacenter	Disponer soporte activo con Proveedor
Aire Acondicionado	Alto	2	Bajo	1	2	Mantenimiento	Sped Backup	No	Datacenter	Disponer soporte activo con Proveedor

Hardware Servidores									
Contingencia/Riesgo	Impacto		Probabilidad		Prioridad	Prevención/Mitigación	Respuesta Incidente	Cumple	Alcance	Recomedaciones
Maimboard/Tarjetas	Alto	3	Bajo	1	3	Alta Disponibilidad de Hw	Automática - Cluster	No	Servidor Local	Adquirir Servidor/Componentes Backups
Memoria	Medio	2	Medio	2	4	Dispositivo Redundante	Automático - Activación	Si	Servidor Local	N/A

Procesador	Alto	3	Medio	2	6	Dispositivo Redundante	Automático - Activación	Si	Servidor Local	N/A
Disco	Medio	2	Alto	3	6	Dispositivo Redundante	Automático - Activación	Si	Servidor Local	N/A
Fuentes	Medio	2	Medio	2	4	Dispositivo Redundante	Automático - Activación	Si	Servidor Local	N/A

Hardware Storage										
Contingencia/Riesgo	**Impacto**		**Probabilidad**		**Prioridad**	**Prevención/Mitigación**	**Respuesta Incidente**	**Cumple**	**Alcance**	**Recomedaciones**
Controladoras	Alto	3	Alto	2	6	Controlador Redundante	Automática - Activación	Si	Storage Local	Mantenimiento
Discos	Medio	2	Bajo	3	6	Discos Redundantes	Automática - Activación	Si	Storage Local	Mantenimiento
Chassis	Alto	3	Medio	1	3	Chassis Redundante	x	No	Storage Local	Storage Backup

Hardware Switches LAN Core										
Contingencia/Riesgo	**Impacto**		**Probabilidad**		**Prioridad**	**Prevención/Mitigación**	**Respuesta Incidente**	**Cumple**	**Alcance**	**Recomedaciones**
Maimboard	Alto	3	Medio	2	6	Switch Stack	Automática - Activación	No	Switch Core "Infraestructura"	Adquirir un equipo de backup
Fuentes	Medio	2	Medio	2	4	Fuente Redundante	Automática - Activación	Si	Switch Core UIO	Plan de Mantenimiento
Puertos	Bajo	1	Bajo	1	1	Puertos disponibles	Cambiar puerto disponible	Si	Switch Core UIO	Plan de Mantenimiento

Hardware Switches SAN										
Contingencia/Riesgo	**Impacto**		**Probabilidad**		**Prioridad**	**Prevención/Mitigación**	**Respuesta Incidente**	**Cumple**	**Alcance**	**Recomedaciones**
Maimboard	Alto	3	Medio	3	9	Switch Backup	Instalación Switch	No	Switch UIO	Adquir switch SAN FC HPE
Fuentes	Medio	2	Medio	2	4	Fuente Redundante	Automática - Activación	Si	Switch UIO	Plan de Mantenimiento
Puertos	Bajo	1	Bajo	1	1	Puertos disponibles	Cambiar puerto disponible	Si	Switch UIO	Plan de Mantenimiento

Sistema Comunicaciones Unificadas										
Contingencia/Riesgo	**Impacto**		**Probabilidad**		**Prioridad**	**Prevención/Mitigación**	**Respuesta Incidente**	**Cumple**	**Alcance**	**Recomedaciones**
Maimboard	Alto	3	Medio	2	6	Alta Disponibilidad de Hw	Activar Garantía	No	Datacenter UIO	Plan de Mantenimiento
Fuentes	Medio	2	Medio	2	4	Fuente Redundante	Automática - Activación	Si	Datacenter UIO	Plan de Mantenimiento
Puertos	Bajo	1	Bajo	1	1	Puerto Redundante	Cambiar puerto disponible	Si	Datacenter UIO	Plan de Mantenimiento
Software	Medio	2	Medio	2	4	Backup Configuración	Restaurar Backup	Si	Datacenter UIO	Plan de Mantenimiento

Firewall - Componentes

Contingencia/Riesgo	Impacto		Probabilidad		Prioridad	Prevención/Mitigación	Respuesta Incidente	Cumple	Alcance	Recomedaciones
Fuentes	Alto	3	Medio	2	6	Fuente Redundante	Automática - Activación	Si	Firewall UIO	Plan de Mantenimiento
Equipo	Medio	2	Bajo	1	2	Cluster Firewall	Automática - Activación	Si	Firewall UIO	Plan de Mantenimiento

Sistema de Comunicaciones (Router, Switch, otros)										
Contingencia/Riesgo	Impacto		Probabilidad		Prioridad	Prevención/Mitigación	Respuesta Incidente	Cumple	Alcance	Recomedaciones
Maimboard	Alto	3	Medio	2	6	Equipo Backup	Contactar Proveedor	Si	Datacenter UIO	Disponer Soporte Activo Proveedor
Fuentes	Alto	3	Medio	2	6	Equipo Backup	Contactar Proveedor	Si	Datacenter UIO	Disponer Soporte Activo Proveedor
Puertos	Alto	3	Bajo	1	3	Puerto Redundante	Contactar Proveedor	Si	Datacenter UIO	Disponer Soporte Activo Proveedor

Software/Aplicación										
Contingencia/Riesgo	Impacto		Probabilidad		Prioridad	Prevención/Mitigación	Respuesta Incidente	Cumple	Alcance	Recomedaciones
Eliminación VM	Alto	3	Medio	2	6	Backups	Restauración	Si	Aplicaciones Virtuales	Plan de Pruebas
Daño Update, Virus, troyanos, etc	Alto	3	Bajo	1	3	Backups	Restauración	Si	Aplicaciones Virtuales	Plan de Pruebas
Manipulación configuraciones	Alto	3	Bajo	1	3	Backups/Doc Configuración	Reconfiguración	Si	Aplicaciones Virtuales	Plan de Pruebas

UNIVERSIDAD TECNOLÓGICA ISRAEL

Maestría en Telemática, mención Calidad en el Servicio.

Tema:

Plan de recuperación de desastres de la Infraestructura de Tecnologías de Información, para empresas de prestación de servicios tecnológicos.

Autor:

Jaime Santiago Cajamarca Yunga

Tutor:

Pablo. M Recalde Varela. MSc. Ing.

Quito, marzo del 2019

PLAN DE RECUPERACION DE DESASTRES DE LA INFRAESTRCUTRA DE TECNOLOGÍAS DE INFORMACIÓN, PARA EMPRESAS DE PRESTACIÓN DE SERVICIOS TECNOLÓGICOS

Autores: Jaime Santiago Cajamarca Yunga

Pablo Marcel Recalde Varela

e-mail: jaimecajamarca@hotmail.com

precalde@uisrael.edu.ec

RESUMEN: El trabajo de investigación propone un marco de referencia para implementación de un plan de recuperación ante desastres de una empresa de cualquier tipo en el Ecuador. Su implementación hace énfasis a empresas del área de soluciones tecnológicas. En la misma se dan a conocer las principales directrices y estándares internacionales como la ISO 22301 y siguiendo las mejores prácticas recomendadas por los fabricantes líderes en el área de tecnología con mejor calificación dentro del cuadrante de Gartner.

La metodología utilizada, propone los lineamientos y procesos a seguirse y cómo actuar frente a la incidencia de un desastre. Propone el plan a seguirse para recuperación y puesta a producción de cada sistema.

En base a los resultados obtenidos, se implementa una guía del plan de recuperación de desastres con un caso de implementación práctico aplicado a AKROS una empresa de soluciones tecnológicas del Ecuador, cuyos resultados fueron satisfactorios.

PALABRAS CLAVE: ISO 22301, Plan de Recuperación de Desastres, Tecnología, Veeam, VMWare.

ABSTRACT. The research work proposes a frame of reference for the implementation of a disaster recovery plan for a company of any kind in Ecuador. Its implementation emphasizes companies in the area of technological solutions. In it, the main guidelines and international standards such as ISO 22301 are presented and following the

best practices recommended by the leading manufacturers in the area of technology with the best rating within the Gartner quadrant.

The methodology used proposes the guidelines and processes to be followed and how to act against the impact of a disaster, proposes the plan to be followed for recovery and production of each system.

Based on the results obtained, a guide to the disaster recovery plan is implemented as a case of practical implementation applied to AKROS a technology solutions company in Ecuador, whose results were satisfactory.

Keywords: ISO 22301, Disaster Recovery Tlan, Technology, Veeam, VMWare.

1. **INTRODUCCIÓN**

La constante evolución de las Tecnologías de la Información y Comunicaciones (TIC), así como la facilidad de acceso al Internet a nivel mundial, ha provocado que, sin importar el tamaño de las empresas, éstas generen gran cantidad de información sensible y de vital importancia, que debe ser debidamente protegida.

Debido a las facilidades de acceso a Internet, el porcentaje de servicios basados en herramientas tecnológicas es alto; es por esto que, es de vital importancia para una empresa el contar con un plan de recuperación de desastres que garantice la continuidad de los servicios críticos de la institución.

El plan de continuidad de negocio (BCP), por sus siglas *Bussiness Continuity Plan* y el plan de recuperación de desastres (DRP), se ha convertido en la última línea de defensa de una entidad; cuando los controles han fallado, el plan de continuidad es el control final, que puede prevenir eventos drásticos, pérdidas de información, paralización de operaciones o el fracaso de una organización.

Miguel Ángel Mendoza. (2014) de *welivesecurity*, señalan que cualquier incidente de paralización de servicios o pérdida de información de una empresa provoca alarmas en las organizaciones afectando no solo a los bienes tangibles de las instituciones sino también a la imagen corporativa de esta, lo que

ocasiona grandes pérdidas económicas debido a la indisponibilidad de los servicios.

Es por ello que, el contar con un sistema de recuperación ante desastres puede reducir al mínimo el tiempo de inactividad tecnológica y pérdida de datos con una recuperación rápida y ordenada después de un desastre.

2. METODOLOGÍA

El presente trabajo se basa en el uso de varias metodologías y estándares de la industria tecnológica.

La población y muestra se basan en todos los sistemas y aplicaciones de TI de la empresa AKROS; y sus cuatro sucursales a nivel nacional en las ciudades de Quito, Guayaquil, Cuenca y Ambato.

Se establecen los *recovery time objetives* (RTOY y los *recovery points objetives* y RPO de las aplicaciones críticas a fin de priorizar los sistemas que deben ser recuperados en menor tiempo por los sistemas de negocio de la empresa.

Con estos puntos se establecen los pasos de la guía de recuperación de desastres y sus métodos de recuperación.

3. ANÁLISIS DE RESULTADOS

Las ISO 22301 es aplicable a cualquier tipo de empresa.

El uso de esta ISO en el caso de AKROS y la infraestructura que posee fue totalmente adaptable, usando principalmente los sitios alternos y las características de infraestructura de los fabricantes que se plantearon inicialmente, entre ellos Veeam y VMWare.

La solución más adecuada luego del seguimiento de la ISO 22310, fue la aplicación de un sitio de contingencia remoto en la ciudad de Guayaquil, del tipo activo-pasivo.

Esta guía es sólida y permite incorporar cualquier nuevo sitio al plan de recuperación de desastres planteado y es escalable, de manera que la incorporación de nuevos sistemas o aplicaciones serán integradas dentro de la guía.

REFERENCIAS

Mendoza, M. A. (2 de febrero de 2014). En que consiste un Plan de Recuperación ante Desastres. Obtenido de https://www.welivesecurity.com/

Casillas, M. (13 de junio de 2018). inbest.solutions. Obtenido de https://inbest.solutions/que-es-un-drp/

Castro, A., & Bayona, Z. (2011). Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios. Ingeniería, 16(2), 56-66.

Isotools. (2016). Normas ISO 22301. Obtenido de https://www.isotools.org/2016/03/10/e-book-norma-iso-22301-y-continuidad-negocio