Diseño de Plan de Recuperación de Desastres con base a la norma NIST 800-34 y al marco de PMBOK para una empresa aseguradora ecuatoriana

Design of a Disaster Recovery Plan based on the NIST 800-34 standard and the PMBOK framework for an ecuadorian insurance company

Karla S. Rivas P. & Gustavo D. Salazar Ch.

***Resumen*—Este documento resume el diseño de un plan de recuperación de desastres del área de tecnología para una empresa aseguradora del Ecuador. La primera sección expone los marcos legales, técnico y de gestión del proyecto; los cuales son: la Codificación de Seguros del Ecuador, la norma del Instituto Nacional de estándares y Tecnología 800-34 y el marco de gestión del Instituto de Gestión de Proyecto, respectivamente. En la segunda sección, a partir de los procesos de criticidad alta en el análisis de impactos, se determina la infraestructura crítica y sus estrategias de recuperación. Como resultado de la gestión del proyecto, se entregan la estructura de desglose de trabajo, la matriz de riesgos y el análisis de costos; que serán importantes para que la compañía apruebe la ejecución del proyecto.**

***Palabras Clave*–Plan de Recuperación de Desastres de TI, NIST 800-34, PMBOK, seguros y reaseguros, Plan de Continuidad del Negocio.**

***Abstract* - This document summarizes the design of a disaster recovery plan in the technology area for an insurance company in Ecuador. The first section sets out the legal, technical and project management frameworks; which are: the Codification of Insurance of Ecuador, the standard of the National Institute of Standards and Technology 800-34 and the management framework of the Project Management Institute, respectively. In the second section, the critical infrastructure and its recovery strategies are determined based on the processes of high criticality in impact analysis. As a result of the project management, the work breakdown structure, the risk matrix and the cost analysis are delivered; which will be important for the company to approve the execution of the project.**

***Index Terms*– IT Disaster Recovery Plan, NIST 800-34, PMBOK, insurance and reinsurance, Business Continuity Plan.**

Historia de Artículo:
Recibido: 10 de julio 2019
Aceptado: 03 de septiembre 2019

K. S. Rivas P., es maestrante del Centro de Posgrados, Departamento de Ciencias de la Computación de la Universidad de las Fuerzas Armadas ESPE, Sangolquí, Ecuador (e-mail: krivasp1504@hotmail.com)

G. D. Salazar Ch., es profesor y director de Tesis del Centro de Posgrados, Departamento de Ciencias de la Computación de la Universidad de las Fuerzas Armadas ESPE, Sangolquí, Ecuador (e-mail: gsalazar@inlea.com – ORCID: https://orcid.org/0000-0003-2394-3506)

I. INTRODUCCIÓN

La regulación de las compañías del sector de valores y seguros del Ecuador dispone la obligación de contar con un sistema de gestión y control de riesgos. La gestión de riesgos no solo comprende el cumplimiento del marco legal, además, previene las pérdidas financieras, operativas y de reputación causadas por la materialización de un riesgo que interrumpa la operación normal de la compañía.

Para cumplir con la normativa, las compañías generan un análisis de impactos del negocio (BIA) y un Plan de Continuidad del Negocio (BCP). El BCP requiere de los sistemas tecnológicos que soportan los procesos de la compañía, por lo cual, se necesita un Plan de Recuperación de Desastres de TI (DRP) [1].

Este trabajo es el diseño de un Plan de Recuperación de Desastres para el área de TI. En este documento se exponen las estrategias de recuperación de los sistemas tecnológicos subyacentes a los procesos calificados con criticidad alta en el

BIA de la compañía. Como referencia para el diseño se usa la norma NITS 800-34. Por otro lado, para gestionar el proyecto se utilizó el marco de PMBOK, y se documentaron: el acta de constitución, la Estructura de Desglose de Trabajo (EDT), el cronograma de actividades, el presupuesto, la matriz de riesgos del proyecto.

Se realizó una búsqueda de trabajos similares a éste, y las diferencias más importantes están en: las normas de referencia para el diseño del DRP, el marco de referencia para la gestión del proyecto, el marco legal de la compañía, las tecnologías y arquitecturas de los servicios de cada compañía. A nivel local, el trabajo de [2] es el más similar al presente. Las diferencias principales radican en las metodologías de diseño del plan de recuperación de desastres. En [2]se trabaja con la ISO 22301, mientras que en esta propuesta se trabaja con la NIST 800-34. Sin embargo, ambas metodologías tienen como principales los pasos: 2, 4, 6 y 7 de la Figura 2.

II. Marco Teórico para el desarrollo del diseño

A. Naturaleza de la compañía

Este diseño se realizó para una empresa del sector de seguros y reaseguros del Ecuador, con 20 años de experiencia en los ramos de vida, incendio, hogar, accidentes personales. Según estadísticas de la Superintendencia de Compañías, Valores y Seguros de Ecuador, la compañía ocupó el primer lugar en ventas de seguro de vida colectiva en el país durante el año 2017 [3].

B. Marco Legal

Las empresas de seguros y reaseguros del Ecuador están supervisadas por la Superintendencia de Compañías, Valores y Seguros y regidas por la Ley General de Seguros, Ley Orgánica de Medicina Prepagada, el Código Civil, y las codificaciones emitidas por la Junta de Regulación Financiera y Monetaria.

La Codificación de Resoluciones Monetarias, Financieras, de Valores y Seguros señala que "toda empresa de seguros y compañía de reaseguros deberán establecer esquemas eficientes y efectivos de administración y control de todos los riesgos a los que se encuentran expuestas en el desarrollo del negocio". La normativa define el riesgo operativo como "la posibilidad de que se produzcan pérdidas debido a eventos originados en fallas o insuficiencia de procesos, personas, sistemas internos, tecnología y en la presencia de eventos externos imprevistos". Y, dicta que, el análisis de riesgos lo realice la Unidad de Riesgos[1] o, en su defecto la Unidad de análisis Técnico[2] [4].

La compañía inició el diseño de un Plan de Continuidad del Negocio (PNC) para afrontar los riesgos operativos catastróficos y cumplir con la normativa. Como resultado se generó el Análisis del Impacto del Negocio (BIA), el cual determina la criticidad de los procesos de la compañía en función de: las pérdidas financieras y de información causadas por interrupción de dichos procesos, el marco legal, la distribución del personal y la producción por sucursales. Una vez levantado el BIA, se inició el diseño de un Plan de Recuperación de Desastres de Tecnología que se expone en este documento.

C. Normativa NITS 800-34

Este diseño del plan de recuperación de desastres del departamento de Tecnología de la Información se realizó con base a la norma 800-34 del Instituto Nacional de estándares de Estados Unidos (NITS) [1].

El BCP debe garantizar que los procesos críticos del negocio no sufran interrupciones que excedan las pérdidas financieras tolerables para la compañía. El DRP identifica los servicios e infraestructura tecnológicos subyacentes a esos procesos críticos y genera las estrategias su recuperación en caso de contingencia.

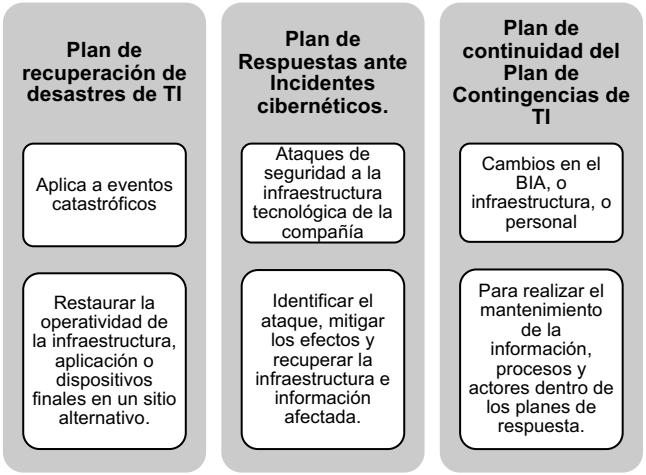


Figura 1. Tipos de Planes de Recuperación de TI [1].

La NIST 800-34 menciona varios tipos de planes para la recuperación de los sistemas de TI, como se muestra en la figura 1. La diferencia entre los planes de recuperación de TI (ver figura 1) es el alcance de cada uno de ellos y su objetivo. El DRP de TI se aplica a eventos donde el acceso a las instalaciones es difícil, o hay una interrupción de las operaciones normales del negocio durante un período prolongado, y por tanto, se requiere la reubicación de la infraestructura para restablecer la operación normal.

[1] Según la normativa, la Unidad de gestión de riesgos es "responsable de identificar, medir, monitorear, controlar/mitigar y divulgar cada uno de los riesgos de identificados que enfrenta la institución" y "deberá ser independiente de las áreas de negocios…a fin de evitar conflictos de intereses y asegurar una adecuada separación de responsabilidades." [11]

[2] La Unidad de Análisis Técnico de una compañía de seguros es el órgano que realiza el análisis "de aspecto financiero como técnico, matemático y estadístico, en orden a la obtención de un equilibrio de resultados" de la actividad de la compañía [12].

Figura 2. Fases de diseño del Plan de Recuperación de Desastres de TI según la NIST 800-34 [1].

El Plan de Respuestas ante Incidentes cibernéticos (ver Figura 1) puede considerarse dentro del BCP, pero no consta como parte del DRP y no se desarrolla en este diseño. El DRP de TI requerirá de constante mantenimiento de la información, procesos y actores dentro del mismo. La norma incorpora esta actividad en un plan separado del DRP, pero necesario para la continuidad de TI, que es el Plan de continuidad del Plan de Contingencias de TI (ver Figura 1).

Los pasos claves que establece la norma para el diseño e implementación de un DRP se muestran en la Figura 2 [1]. La sección III desarrolla los primeros cinco pasos de la norma para lograr el diseño del DRP.

D. Marco de Gestión de proyectos PMBOK

El PMBOK es un conjunto de buenas prácticas para la gestión de proyectos que establece cinco fases para un proyecto y 10 áreas de conocimiento. Las fases del PMBOK son: inicio, planificación, ejecución, control y cierre. Las áreas del conocimiento son: integración, alcance, cronograma, costo, calidad, recursos, comunicaciones, riesgos, adquisiciones e interesados. Según la fase del proyecto, hay más o menos actividades relacionadas con las áreas de conocimiento. La fase donde se contemplan todas las áreas del conocimiento es la planificación [5].

Un proyecto bien planificado puede optimizar recursos (humanos, económicos, físicos, temporales) y simplificar mucho la ejecución, control y cierre de un proyecto, es por ello que, el PMBOK se enfoca el mayor conjunto de actividades en esta fase [5].

En este artículo se contemplan la fase de inicio y de planificación del proyecto. Como entregables del inicio del proyecto se generó el Acta de Constitución del proyecto. Como entregables de la planificación del proyecto se generó el Plan de proyecto que contempla: la EDT, los cronogramas, el análisis de costos, el plan de comunicación y la matriz de riesgos identificados durante la planificación de riesgos.

También son parte de los entregables de la fase de planificación según el PMBOK: el plan de gestión de adquisiciones y el plan de calidad, pero dichos planes no se entregan en este diseño.

Es importante mencionar que todas las normas (en este caso la NIST 800-34 y el PMBOK) dan una guía de buenas prácticas que deben ser adaptadas a la realidad de cada empresa y que, aplicadas de forma correcta, mejoran la efectividad del proceso para el que fueron creadas, además de ahorrar costos y tiempo. Sin embargo, la aplicabilidad de todas las prácticas o un conjunto de seleccionado de ellas, queda a discreción de cada compañía.

III. Diseño del Plan de Recuperación de Desastres

A. Definición del proyecto y políticas que regirán el diseño

De forma inicial, las restricciones para el diseño del DRP fueron:

- Se considerarán los procesos críticos del BIA (Tabla 1) levantado por la Unidad de Riesgos de la compañía, además se establecieron como tiempo máximo de recuperación 8 horas (RPO[3]), y como tiempo máximo de pérdidas de información 8 horas (RTO[4]).
- El DRP tendrá dos fases; esta primera fase comprende el 60% de la capacidad de operación actual.

B. Identificación de servicios e infraestructrura tecnológica críticos de la compañía

Con base a los datos de la Tabla 1, se levantó la información de:

- Los aplicativos que utilizan los usuarios para realizar los procedimientos y sus arquitecturas.
- Los recursos de software, hardware, base de datos y servicios asociados a dichos aplicativos.
- Los proveedores relacionados con los aplicativos o responsables de dar soporte a los aplicativos.

En la tabla 2 se muestra la información listada para cada proceso crítico de la compañía. Varios servicios o recursos tecnológicos se utilizan en más de un procedimiento/proceso, por lo que, en resumen, se tienen los siguientes:

- Redes de comunicaciones: LAN, WAN, enlaces de internet y telefonía, DHCP y plataforma de seguridad perimetral (sección C.1)
- Servicio de autenticación de usuarios en la red y DNS (sección D.2)
- Servicio de correo electrónico (sección D.2)
- Plataforma de Contacto Telefónico al cliente y gestor de grabaciones de llamadas (sección D.2)
- Servicios del sistema del giro del negocio (sección D.3)
- Servicio de carga, actualización de listas de información reservada y parametrización de búsquedas de clientes en listas de información reservada (sección D.3)
- Herramienta de cotización y emisión de seguros en línea (sección D.3)
- Herramienta de administración de información e interacciones con los clientes (CRM) (sección D.3)
- Servicio de gestión de documentación y procesos (BPM) (sección D.3)

[3] El punto de recuperación objetivo (RPO), "es el tiempo en el cual la información debe ser respaldada, para poder procesarla" y reconstruir la información que se pierda en la contingencia [1].

[4] El Tiempo de recuperación objetivo (RTO) es "el tiempo máximo que puede transcurrir antes de que la indisponibilidad del sistema cause pérdidas severas para la organización" [1]

– Servicio de bases de datos de aplicativos (sección D.3)

TABLA 1. PROCESOS CRÍTICOS DE LA COMPAÑÍA EN EL BIA

Macroproceso	***Proceso***	***Procedimiento***
Gestión del control	Prevención de Lavado de activos	Revisión de Clientes en lista de información reservada
Gestión Comercial	Comercialización de seguros	Comercialización de productos en distintos canales de venta (B2C, B2B, B2B2C)
Gestión de experiencia del cliente	Gestión de Quejas, requerimientos y recepción de reclamos.	Recepción de siniestros, quejas, requerimientos, modificaciones, anulaciones y cancelaciones
Gestión de Siniestros	Gestión de Siniestros	Apertura de casos, recepción de información, análisis, aprobación/negativa y pago de siniestros
Gestión de Tecnología	Administración de la plataforma tecnológica	Administración de infraestructura tecnológica y de comunicaciones. Administración de Base de Datos. Administración de aplicativos internos y externos

C. Descripción de estrategias por servicios tecnológicos

Una vez que se completó el mapeo de los aplicativos y sus respectivos recursos (Figura 7) se establecieron las estrategias de recuperación de los aplicativos y bases de datos, conforme a los siguientes a la arquitectura de software y base de datos de las aplicaciones; la tasa de cambio de la información de las aplicaciones y el juicio de los expertos y quienes diseñaron las aplicaciones.

1) Centro de cómputo y redes de comunicaciones: LAN, WAN, enlaces de internet y telefonía, DHCP y DNS y plataforma de seguridad perimetral.

El sitio contingente debe localizarse en un área geográfica que no esté afectada por el mismo evento de desastre del sitio principal [1]. La compañía cuenta con centros de cómputos en la localidad de Quito, por lo que se optó por uno en la ciudad de Guayaquil, con servicio de arrendamiento.

D. Descripción de estrategias por servicios tecnológicos

Una vez que se completó el mapeo de los aplicativos y sus respectivos recursos (Figura 7) se establecieron las estrategias de recuperación de los aplicativos y bases de datos, conforme a los siguientes a la arquitectura de software y base de datos de las aplicaciones; la tasa de cambio de la información de las aplicaciones y el juicio de los expertos y quienes diseñaron las aplicaciones.

1) Centro de cómputo, redes de comunicaciones, plataforma de comunicaciones unificadas y seguridad perimetral.

El sitio contingente debe localizarse en un área geográfica que no esté afectada por el mismo evento de desastre del sitio principal [1]. La compañía cuenta con centros de cómputos en la localidad de Quito, por lo que se optó por uno en la ciudad de Guayaquil, con servicio de arrendamiento.

TABLA 2. SERVICIOS TECNOLÓGICOS ATADOS A LOS PROCESOS CRÍTICOS

Proceso crítico	***Procedimiento***	***Aplicativos / servicios tecnológicos***
Prevención de Lavado de Activos	Búsqueda y Análisis de Clientes en listas de información reservada	Sistema de carga y actualización de listas de información reservada (Bridger Insight)
		Enlaces de Internet
		Sistema de configuración y parametrización de búsquedas de clientes en listas de información reservada (Risk Control)
	Revisión de Clientes en espera y aprobación o negación	Módulo de aprobación de clientes en espera
		Enlaces de Internet
		Correo electrónico
Comercialización de Seguros	Comercialización de productos en distintos canales de venta (B2C, B2B y Telefónico)	Herramienta de administración de información e interacciones con los clientes (CRM)
		Herramienta de cotización y emisión en línea
		Gestor de documentación y procesos (BPM)
		Plataforma de Contacto Telefónico al cliente y gestor de grabaciones de llamadas
		Enlaces de telefonía
Servicio al cliente	Recepción de siniestros, quejas, requerimientos, anulaciones y cancelaciones	Herramienta de administración de información e interacciones con los clientes (CRM)
		Sistema Core del Negocio (SIP)
		Gestor de documentación y procesos (BPM)
		Plataforma de Contacto Telefónico al cliente y gestor de grabaciones de llamadas
		Enlaces de telefonía
		Plataforma de entrega de aplicaciones remotas
		Enlaces de Internet
Gestión de Siniestros	Apertura de casos, recepción de información, análisis, aprobación/negativa y pago de siniestros	Gestor de documentación y procesos (BPM)
		Sistema Core del Negocio
Administración de la plataforma tecnológica	Seguridades necesarias para la infraestructura de la compañía	Plataforma de Seguridad Perimetral: Firewall, Proxy y Antispam
		Plataforma de Autenticación de usuarios: Directorio Activo
		Plataforma de Administración de Redes LAN: DHCP, DNS
		Plataforma de virtualización y consolas de administración
		Enlaces de Internet

Para la segmentación de redes de en el centro de datos alterno, las redes de las consolas de administración de infraestructura física y de virtualización, se diferenciarán con el propósito de identificar qué localidad se administra; y, las redes de servidores se configurarán dentro del mismo rango para ambas localidades, como una LAN extendida, para facilitar la migración de servicios del ambiente de producción a contingencia en caso de que el DRP se active como se muestra en la Figura 3.

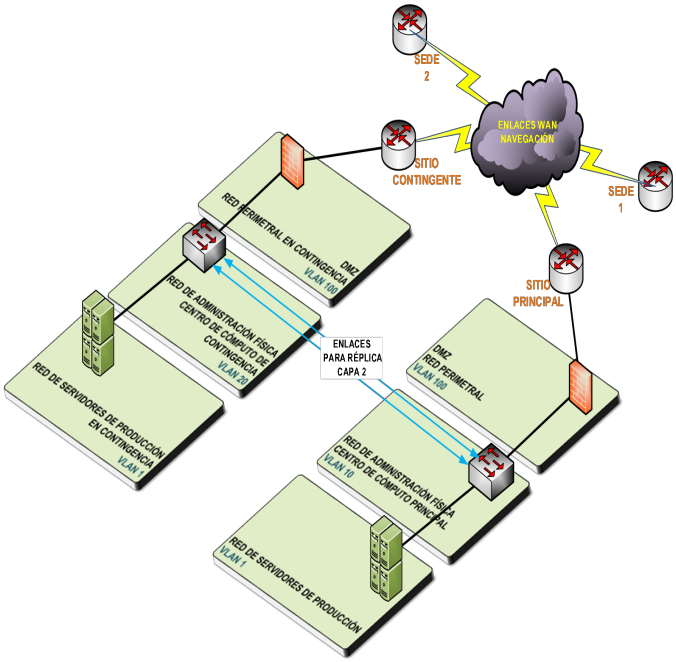


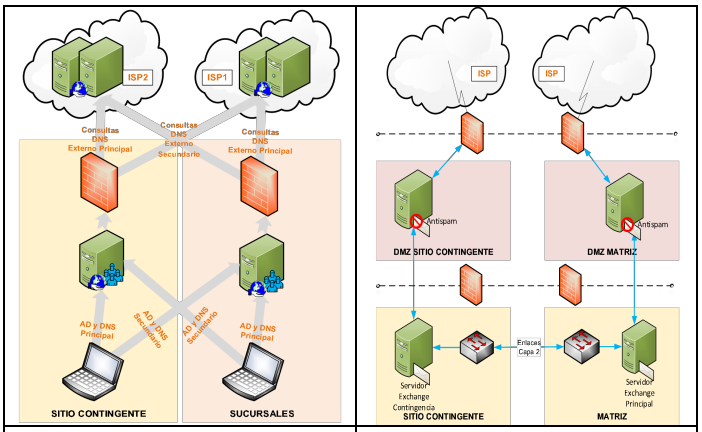
Figura 3. Estrategia de redes y enlaces de comunicación para sitio de contingencia [1].

Se tendrán dos enlaces que conectarán los centros de computación principales de Quito o las sucursales con el centro de cómputo de contingencia, que son: los de réplica y de datos. El servicio de réplica se realizará con dos enlaces de capa 2 entre los switches de distribución del sitio contingente y el principal; los enlaces serán redundantes en modo activo pasivo. Los enlaces de datos se configurarán entre las sucursales al sitio contingente (ver Figura 3). Las capacidades de los enlaces de réplica serán mayores a los de datos, puesto que se utilizarán para mantener la información de las aplicaciones sincronizadas entre el sitio principal y contingente.

Para la configuración de red propuesta, es necesario que se apunten a todos los servicios o servidores de aplicaciones por nombre de servidor y dominio (FQDN[5]); con esto, los servidores pueden tener dos direcciones IP por registro DNS: una de producción y otra de contingencia (Figura 4); al caerse una de ellas el DNS facilitará la IP disponible para el mismo FQDN que será la de contingencia [6] [7].

2) Autenticación de usuarios, correo electrónico y plataforma de telefonía.

La autenticación de usuarios se realiza a través de un controlador de dominio de Microsoft, también para el correo electrónico la compañía utiliza la solución de Microsoft, Exchange. La arquitectura de ambas aplicaciones permite la configuración de alta disponibilidad de sus servicios; es decir, si un controlador de dominio, o un servidor de correo, falla los clientes se conectan automáticamente a los servidores de contingencia que conforman la arquitectura y están disponibles y sincronizados. Por lo tanto, la estrategia es disponer de un servidor contingente en el centro de cómputo alternativo [6] [7], ver Figura 4.



a) Estrategia de contingencia para el servicio de DNS y Autenticación

b) Estrategia de contingencia para el correo electrónico

Figura 4. Estrategias de recuperación de los servicios de DNS y de correo electrónico [6] [7].

Para la arquitectura de alta disponibilidad del correo electrónico se debe configurar a los servidores de correo electrónico dentro de un mismo grupo de disponibilidad de base de datos (DAG[6]). La réplica de la información de las bases de los servidores utilizará el enlace de capa 2. En el sitio contingente existirá un antispam en clúster con el del sitio principal para el control del correo que se recibe o envía hacia fuera de la organización [7].

El servicio de comunicaciones unificadas (telefonía, centro de contacto telefónico, IVR, entre otros) también se cuenta con una arquitectura de alta disponibilidad, como se muestra en la Figura 5. Los enlaces de telefonía hacia la PSTN se gestionarán con un proveedor diferente al de la sede principal [8].

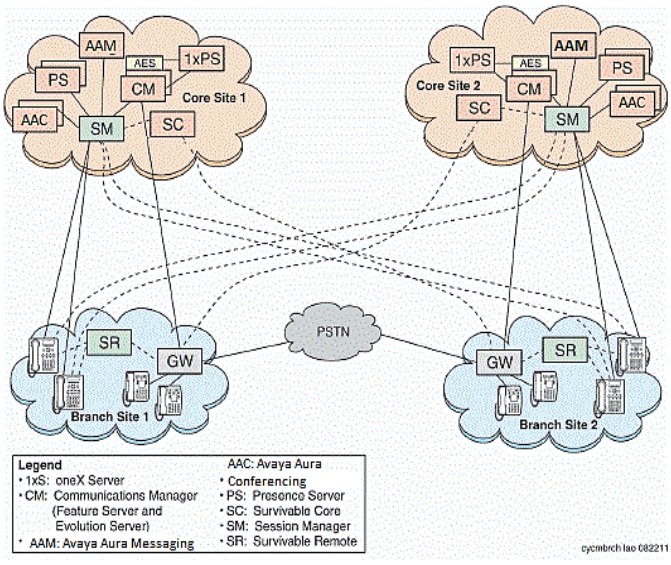


Figura 5. Estrategias de recuperación de los servicios de Comunicaciones Unificadas [8].

[5]El nombre completo de dominio de un host (FQDN, fully qualified domain name) es el registro que identifica a un computador o servidor único en un dominio, y está conformado por dos partes: nombre del host y nombre del dominio [13].

[6] "Un grupo de disponibilidad de base de datos (DAG) es un grupo de hasta 16 servidores de buzones de correo que aloja un conjunto de bases de datos y proporciona una recuperación automática a nivel de base de datos de fallas que afectan a servidores individuales o bases de datos" [14].

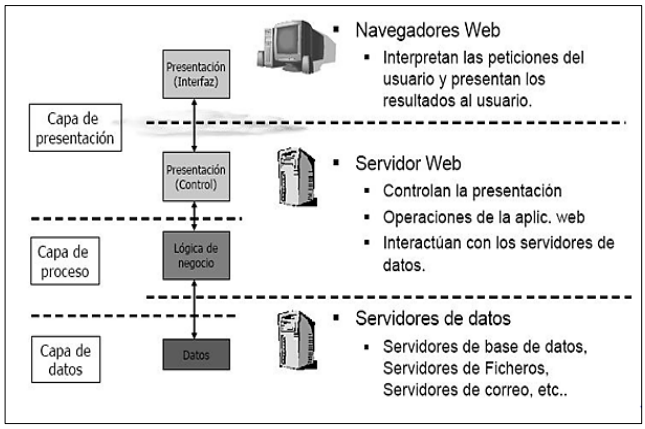


Figura 6. Arquitectura en capas de aplicativos críticos enlistados [9].

3) Estrategias para el resto de aplicativos de la compañía

Las aplicaciones del sistema del giro del negocio; la actualización de listas de información reservada y parametrización de búsquedas de clientes; cotización y emisión de productos; información e interacciones con los clientes (CRM); y, gestión documental y procesos (BPM), tienen la misma arquitectura de software (ver Figura 6), por lo cual se aplicó la misma estrategia para todos ellos.

La arquitectura consiste en tres capas (Figura 6): de presentación (servidores web), de proceso (servidores/servicios donde se aplican las reglas del negocio) y de datos (servidores de bases de datos).

Los elementos de cada capa sufren cambios con distinta frecuencia. La capa de datos de las aplicaciones, que corresponde a las bases de datos, sufre cambios en función de los datos ingresados o modificados, por lo que, se aplica la estrategia presentada en la sección 4 (más adelante), que es la réplica en línea, a fin de reducir la pérdida de información.

Las capas de presentación y procesos sufren cambios con menor frecuencia que la capa de datos. Por ejemplo, la herramienta de comercialización en línea sufre cambios en la capa de procesos o presentación, cada vez que se añade una regla de negocio[7] como la inclusión de un campo en el formulario de venta de un producto. Por ello la estrategia de recuperación los elementos de esta capa es la réplica de las imágenes de máquinas virtuales calendarizada.

Es importante destacar que, para que en el caso de las aplicaciones que tienen las tres capaz, éstas se deben recuperar en orden para que funcionen. Primero, las bases de datos, luego, la capa de procesos y, por último, los de la capa de presentación.

4) Servicio de base de datos y servicio de archivos de usuarios

Las bases de datos de las aplicaciones tienen una alta tasa de transacciones (de lectura y escritura). La estrategia de recuperación de las bases de datos consistirá en la réplica en línea de la información de las bases que corresponden a las aplicaciones críticas hacia el sitio contingente. La réplica en línea se realizará a través del enlace de capa 2. Las bases de datos del sitio contingente se configurarán en modo "clúster" con las bases de datos en el sitio principal, y estará en estado pasivo hasta que se deba activar el DRP.

item	DESCRIPCIÓN DEL APLICATIVO	HARDWARE			SOFTWARE		CAPA DE ARQ. DE SOFTWARE
		RAM (GIGAS)	vCPU	STORAGE (TERAS)	CANT.	TIPO DE LICENCIAMIENTO	
1	SERVIDORES DE ARCHIVO	72	9	20	5	WINDOWS SERVER STANDARD	ÚNICA
2	SISTEMA CORE	4	16	1	1	WINDOWS SERVER STANDARD	PROCESAMIENTO Y APLICACIÓN
3	SISTEMA CORE	384	18	42	3	WINDOWS SERVER STANDARD	BASE DE DATOS
4					3	MICROSOFT SQL SERVER	BASE DE DATOS
5	SISTEMA CORE	16	64	2	4	WINDOWS SERVER STANDARD	APLICACIÓN
6	BPM	24	4	0.46	1	WINDOWS SERVER STANDARD	APLICACIÓN
7	BPM	24	4	0.46	1	WINDOWS SERVER STANDARD	PROCESAMIENTO
8	BPM	128	5	5.3	1	WINDOWS SERVER STANDARD	BASE DE DATOS
					1	MICROSOFT SQL SERVER	BASE DE DATOS
9	Herramienta de CRM e Información del cliente	48	32	1.31	3	WINDOWS SERVER STANDARD	PROCESAMIENTO Y APLICACIÓN
10	Herramienta de Ventas móviles	32	8	1	2	WINDOWS SERVER STANDARD	PROCESAMIENTO Y APLICACIÓN
11	Plataforma de Contact Center, y gestión de grabaciones de llamadas	178	110	12	2	WINDOWS SERVER STANDARD	TODAS
					18	Red Hat Enterprise Linux	
12	Plataforma de entrega de aplicaciones remotas	52	36	1	7	WINDOWS SERVER STANDARD	TODAS
13	Correo electrónico	48	4	2	18	WINDOWS SERVER STANDARD	TODAS
14	Plataforma de Seguridad Perimetral: Firewall, Proxy y Antispam	36	58	1	3	Red Hat Enterprise Linux	TODAS
15	Plataforma de Autenticación de usuarios: Directorio Activo	8	4	0.5	1	WINDOWS SERVER STANDARD	NO APLICA
16	Plataforma de Administración de Redes LAN: DHCP, DNS	8	4	0.5	1	WINDOWS SERVER STANDARD	NO APLICA
17	Plataforma de virtualización y consolas de administración	8	4	0.5	1	WINDOWS SERVER STANDARD	TODAS
	TOTALES	1070	380	91.03			

Figura 7. Recursos totales para implementación de servicios/aplicativos críticos identificados. Nota: los nombres han modificados por los términos de confidencialidad del proyecto, dejando la descripción del aplicativo.

PROCESAMIENTO			
Cant.	Servidores	VCPU	RAM
9	ProLiant BL460c Gen9	408	2.2 TB
6	ProLiant BL460c Gen8	224	1.5 TB
Total		632	3.7 TB

ALMACENAMIENTO 3PAR			
Cant.	Discos	Capacidad unidad	Total RAW (TB)
48	Disk FC 10K SSF	1.8 TB	86,4
48	Disk NL 7K LFF	4 TB	192
TOTAL			278,4

Figura 8. Recursos totales de procesamiento y almacenamiento que se, por actualización de infraestructura tecnológica, serán trasladados al Centro de Cómputo alterno.

Una restricción que se identificó para la recuperación de las aplicaciones de CRM y BPM es que las bases deben levantarse en el mismo sitio geográfico, puesto que las latencias propias de los enlaces inhiben el funcionamiento de estas aplicaciones al conectarse con bases en diferentes sedes.

La misma herramienta y estrategia se utilizará para los servicios de archivos de usuarios en unidades compartidas, es decir, se replicará en línea de la información de los usuarios a un servidor de archivos en el sitio contingente y se direccionarán las unidades compartidas de los usuarios mediante DNS al sitio de contingencia.

[7] "Las reglas de negocios son instrucciones declarativas que rigen la conducta de los procesos empresariales. Una regla está formada por condiciones y acciones. La condición se evalúa, y si se evalúa como verdadera, se inician una o varias acciones." [15]

IV. Análisis del Hardware para el sitio de contingencia

La compañía optó actualizar la infraestructura del centro de cómputo principal y reutilizar el equipo reemplazado en el centro de cómputo alterno. La actualización consistió en migrar la infraestructura convergente de los centros de cómputo de Quito a nueva infraestructura hiperconvergente.

Tabla 3. Uso de Hardware Disponible de los Aplicativos Críticos

	Unidad	Disponible	Requerido	Uso %
RAM	GB	3700	1070	29%
vCPUs	cantidad	632	380	60%
Almace-namiento	TB	278.4	91.03	33%

Luego se validó la infraestructura convergente que aún contaba con soporte de fabricante para ser reutilizada en el centro de cómputo alterno. Se realizó el análisis de recursos disponibles para validar que dicha infraestructura cubra lo requerido para el DRP, los resultados se muestran en las Figura 7 y Figura 8, y Tabla 3. En conclusión, no se requiere comprar almacenamiento, ni procesamiento adicional para la implementación del DRP porque en todos los casos se utiliza menos del 60% de lo dispuesto.

Tabla 4 Costos anualizados de la implementación del DRP por tipo de gasto tecnológico

RESUMEN DE COSTOS POR TIPO DE RECURSOS				
TIPO DE GASTO TECNOLÓGICO	**MONTO POR CONCEPTO**		**% APORTE DE CADA COSTO AL TOTAL**	
	2019	**2020**	**2019**	**2020**
HARDWARE	$9,933.94	$0.00	3.1%	0.0%
SOFTWARE	$11,631.54	$0.00	3.6%	0.0%
LICENCIAMIENTO	$84,037.15	$60,140.68	26.2%	23.2%
SOPORTE DEL LICENCIAMIENTO	$7,791.91	$7,791.91	2.4%	3.0%
INSTALACIÓN	$48,316.52	$0.00	15.0%	0.0%
SERVICIO DE COMUNICACIÓN	$133,780.50	$160,536.60	41.6%	61.9%
SERVICIO DE HOUSING	$23,800.00	$28,560.00	7.4%	11.0%
SERVICIO DE SOPORTE	$2,000.00	$2,400.00	0.6%	0.9%
TOTAL	**$321,291.56**	**$259,429.19**	**100.0%**	**100.0%**

Tabla 5 Costos anualizados de la implementación del DRP por frecuencia de pago

Por frecuencia de pago	**2019**	**2020**
Una vez	29%	0%
Mensualmente	50%	74%
Anualmente	21%	26%
Total	100%	100%

V. Análisis de costos del diseño

El resumen de costos por cada tipo de gasto tecnológico y para los años 2019 y 2020 se muestran en las Tablas Tabla 4 y Tabla 5. Durante el año 2019 se pagarán costos únicos de instalación y configuración que elevarán el presupuesto necesario para mantener el DRP, y durante el año 2020 sólo se pagarán los costos del mantenimiento de la solución de DRP. Los rubros más significativos de la solución son los de enlaces de comunicaciones y de licenciamiento.

La mayoría de costos del proyecto para el año 2019 (considerando los meses de marzo a diciembre), que es el año de implementación, se deben pagar de forma mensual, representan el 49.6% de la inversión y corresponden principalmente a los enlaces de comunicaciones y arrendamiento del centro de datos. El segundo costo más importante es el de licenciamiento y su soporte, corresponde al 25.2% y tiene una frecuencia de pago anual. Los costos de implementación para el año 2019 representan el 15 % de la inversión y se pagan una vez.

VI. Análisis de riesgos del proyecto

Entre los riesgos principales que se pueden presentar para implementar las estrategias diseñadas están:

1. Que la infraestructura necesaria para el sitio contingente no esté instalada y configurada correctamente y de forma oportuna:
   - Esto podría generar retrasos en el proyecto o dificultades en la implementación de las estrategias. Para evitarlo se debe validar la infraestructura base antes de su entrega.
2. Fallas en los enlaces de comunicación WAN al Sitio Contingente.
   - Esto puede dificultar la réplica de datos entre el sitio principal y el contingente, ampliando el tiempo de recuperación de datos o incluso imposibilitando la recuperación de datos. Para evitarlo es importante realizar pruebas de los enlaces y destinar una ventana de prueba y puesta a producción adecuada para medir la transaccionalidad sobre los mismos y afinarlos.
3. Que algunos aplicativos no cuenten con soporte de fabricantes.
   - Esto puede dificultar tener la suficiente información sobre las restricciones del aplicativo al replicarlo o no contar con la ayuda oportuna para restablecer el aplicativo en caso de contingencia. Para evitarlo el área de tecnología debe garantizar de forma contractual el soporte de los aplicativos que se usan en procesos críticos.
4. Que exista demasiada información para la réplica inicial al sitio contingente
   - Esto puede causar que el DRP no se pueda manejar hasta que toda la información esté replicada. Este riesgo depende también de forma indirecta de los enlaces, sin embargo, para reducir el tiempo de la copia inicial lo óptimo es realizarla de forma local, en horarios de poca transaccionalidad o que puedan ser monitoreados y previo a trasladar los equipos al sitio contingente.

VII. Conclusiones y lecciones aprendidas del proyecto

La compañía, además de considerar el costo inicial para la implementación de un Plan de Recuperación ante Desastres del área de TI, debe proyectar y contemplar el costo de mantenimiento de dicha solución. En esta compañía el costo de mantenimiento representa un incremento del 33% del presupuesto anual asignado al área de TI, para un centro de cómputo alterno con una capacidad equivalente al 60% de la operación del centro de cómputo principal. Si ese presupuesto adicional no se reserva, se debería limitar el alcance del proyecto según lo que la compañía considere que debe o puede

invertir y sin descuidar las necesidades y escenarios planteados en el BIA.

El DRP es un plan que puede cambiar en función de las nuevas aplicaciones o necesidades del negocio, por lo que su presupuesto de mantenimiento también cambiará. Es por eso que se debe contrastar su costo con el de la pérdida causada por la materialización del riesgo para sensibilizar a las partes que aprueban el presupuesto del proyecto. Por lo tanto, es importante considerar la participación de las áreas de que tienen asignadas la evaluación de riesgos operativos y financieros y la administración de los procesos de la compañía para la promoción del proyecto.

El Plan de Continuidad del Negocio (PNC) de una compañía constituye la orquestación de varios planes: de comunicaciones, de operación, entre otros; y el de recuperación de la infraestructura tecnológica, durante una interrupción no esperada. Además de actualizar de forma constante el DRP, la compañía debe informar y entrenar a los colaboradores en sus roles y actividades dentro del PNC y otros planes que lo complementan. De lo contrario, el DRP no funcionará, si, a pesar de poner a disposición las herramientas tecnológicas, no se cuenta con el personal competente para acceder a ellas y utilizarlas.

Se recomienda que el BIA y el PNC sean levantados por un área que tenga conocimiento y gestión de los riesgos dentro de los procesos de la compañía. Primero, porque los procesos pueden requerir tareas manuales, no atadas a una herramienta y de criticidad alta, cuya estrategia de recuperación no correspondería al área de tecnología, sino a un área operativa. O bien, algunas estrategias de recuperación pueden no requerir una herramienta. Por ejemplo, para el caso actual, la comercialización puede realizarse mediante formularios pre-impresos (no por una herramienta en línea); en ese caso, provisionar de los formularios y entrenar al equipo en su uso no es tarea del área de TI.

Segundo, el área de tecnología destinada al desarrollo de aplicaciones, no es un área especialista en evaluación de riesgos. La responsabilidad de gestionar un plan con la complejidad del PNC debe ser de un área que cuente con las herramientas y competencias adecuadas, en caso de que no exista dicha área, debe ser generado como un proyecto de toda la compañía. En el caso de este proyecto, el escenario y procesos considerados críticos ya fueron establecidos por la Unidad de Riesgos de la compañía, la cual es la destinada a realizar dicho análisis según la normativa.

Si bien existen servicios de infraestructura en la nube, que pueden ser una alternativa para las estrategias de recuperación de la infraestructura, éstos deben ser analizados según el marco legal y operativo de cada compañía. Para el caso de las empresas de seguros del Ecuador, que manejan datos personales y sensibles de los usuarios, la legislación exige sigilo respecto a esa información, por lo que la compañía consideró un riesgo manejar la infraestructura como servicio en la nube.

En este diseño del proyecto se trabajó con miembros de distintas áreas de la compañía y proveedores. Entre las áreas que participaron están: el área de infraestructura y desarrollo tecnológico de aplicaciones, la Unidad de Riesgos y la oficina de procesos, la oficina de proyectos, y proveedores. Para coordinar el trabajo conjunto de las partes se realizaban reuniones de seguimiento semanales que permitían visualizar lo que se había hecho, lo que se debía hacer y los inconvenientes en que las distintas partes del proyecto requerían ayuda. Cada parte tenía un líder de proyecto, responsable de gestionar la comunicación, requerimientos y resultados de los compromisos en cada reunión, lo que facilitaba la coordinación de los esfuerzos.

VIII. Referencias bibliográficas

[1] NIST, Contingency Planning Guide for Information Technology Systems, Washintong: U.S. Goverment Printing Office, 2002.

[2] A. Cárdenas Pallo, Desarrollo del plan de Continuidad del negocio para la Empresa Equivida SA para el período 2012-2015, Sangolqui: Universidad de las Fuerzas Armadas ESPE, 2013.

[3] Seguros del Pichincha. Marzo, 2019. [En línea]. Disponible en: https://www.segurosdelpichincha.com/conoce-seguros-del-pichincha-aseguradora-lider-en-ecuador.html.

[4] F. d. V. y. S. Codificación de Resoluciones Monetarias, Junta Financiera Monetaria, Quito. Registro Oficial de la Asamblea Nacional, 2017, pp. 227-239.

[5] Project Management Institute. La guía de los fundamentos para la dirección de proyectos (Guía del PMBOK). Sexta ed., Newtown Square, Pennsylvania 19073-3299 EE.UU. Project Management Institute, Inc., 2017, pp. 23-25.

[6] Microsoft.Windows IP Pro Center - Use DNS policy for app load balancing. Microsoft. Mayo, 2019. [En línea]. Disponible en: https://docs.microsoft.com/en-us/windows-server/networking/dns/deploy/app-lb. [Último acceso: 10 Junio 2019].

[7] S. Branham.ExchangeITup. Stacey Branham, 6 Enero 2015. [En línea]. Disponible en: http://www.exchangeitup.net/2015/01/exchange-2013-planning-diagrams-part-1.html. [Último acceso: 10 Junio 2019].

[8] Avaya Inc. .AVAYA. Product Documentation. Redundancy and high availability. Avaya, 20 6 2018. [En línea]. Disponible en: https://documentation.avaya.com/bundle/AvayaAuraSessionManagerOverviewandSpecification_r7.1.3/page/RedundancyAndHighAvailability.html. [Último acceso: 10 Junio 2019].

[9] Instituto Tecnológico de Matehuala. 2.1 Arquitectura de las aplicaciones Web. Junio, 2015. [En línea]. Disponible en: https://programacionwebisc.wordpress.com/2-1-arquitectura-de-las-aplicaciones-web/.

[10] Universitat Oberta de Catalunya.Glosario. [En línea]. Disponible en: http://cv.uoc.edu/UOC/a/moduls/90/90_519/web/nwin/glossari/. [Último acceso: 2019].

[11] Superintendencia de Bancos.Superintendencia de Bancos. Libro I. Normas generales para instituciones del sistema financiero. Administración de Riesgos. 10 enero 2010. [En línea]. Disponible en: https://www.superbancos.gob.ec/bancos/wp-content/uploads/downloads/2017/06/L1_X_cap_I.pdf. [Último acceso: junio 2019].

[12] A. Guardiola Lozano, Manual de Introducción al Seguro, Madrid. Editorial MAPFRE, 1990.

[13] Indiana University.Knowledge Base. 2019. [En línea]. Disponible en: https://kb.iu.edu/d/aiuv. [Último acceso: Junio

2019].

[14] Microsoft.Microsoft Docs: Exchange Server - High availability - Database availability groups. Agosto, 2018. [En línea]. Disponible en: https://docs.microsoft.com/en-us/exchange/high-availability/database-availability-groups/database-availability-groups?view=exchserver-2019. [Último acceso: Junio 2019].

[15] Microsoft.Documentación principal de BizTalk Server. Microsoft. Junio, 2017. [En línea]. Disponible en: https://docs.microsoft.com/es-es/biztalk/core/rules. [Último acceso: Agosto 2019].

Karla S. Rivas P. Nacida en Quito, el 15 de abril de 1989. Obtuvo el título de Ingeniería en Electrónica y Telecomunicaciones en la Escuela Politécnica Nacional, Quito, en 2016. Estudió la Maestría en Gerencia de Sistemas Informáticos, en la Universidad de las Fuerzas Armadas ESPE, en 2016. Trabajó en el área de infraestructura tecnológica y de diseño de plataformas de comunicaciones unificadas con marcas como Cisco, Avaya, HP, Aruba, Checkpoint, McAfee, Veeam, entre otras, desde el 2014 al 2016. Actualmente, se realiza la gestión de proyectos tecnológicos en el sector de seguros.

Gustavo Salazar, Nacido en Quito, el 9 de septiembre de 1987. Es Ingeniero Electrónico graduado con honores de ESPE, Magister en Redes de Comunicaciones de PUCE, siendo el mejor graduado de todos los posgrados del año 2015. Doctorando en Ciencias Informáticas en la Universidad Nacional de La Plata - UNLP con investigación en Redes de Nueva Generación y basadas en programabilidad. Conferencista de Cisco Community Sopport en Español galardonado en el 2016/2017 y para Cisco Global Instructor Professional Development. Es Docente Universitario a nivel de Maestría en ESPE, PUCE, EPN, UPS y UNLP. Mejor instructor Cisco en Latinoamérica 2016/2017. Actualmente trabaja para Cisco Systems e Inlea en el desarrollo curricular de los programas Cisco Networking Academy y en la elección de futuros instructores a nivel mundial. Es instructor de instructores para programas CCNA R&S, CCNP R&S, CCNA Security, IT Essentials y CyberOPS en ESPE-Innovativa EP. Posee varias certificaciones Cisco, Microsoft e IPv6 Forum. Designado como Cisco Champion 2016 a 2019.