UNIVERSIDAD CENFOTEC

Maestría en Ciberseguridad

Documento final de Proyecto de Investigación Aplicada 2

“Construir una guía para la creación de un plan de recuperación de desastres seguro enfocado en la nube para la empresa Premier Soluciones”.

Realizado por:

Montero Corrales Jefry

Julio 2019

Derechos de autor

Dedicatoria

Esta tesis es la culminación de un sueño que tuve, de ser máster en temas que me apasionan y va dedicada a mi familia que siempre me ha apoyado en el cumplimiento de mis metas, quienes siempre están conmigo y a mi hija para mostrarle que, sin importar los obstáculos, siempre se puede salir adelante.

Agradecimientos

Agradezco a mi familia por el apoyo, a mis profesores de Cenfotec que han sido muy buenos y me han inducido de la forma correcta, a mi profesor tutor el máster Carlos Calvo, por la confianza que depositó en mí y por la guía que me dio para la creación del presente documento. Además, a los compañeros de trabajo de Premier Soluciones que siempre trataron de ayudarme en lo que pudieron.

TABLA DE CONTENIDOS

Figuras.

Tablas.

Abstract

El propósito de crear esta investigación es dar los lineamientos o pasos por seguir para la creación de un Plan de Recuperación de Desastres para la empresa Premier Soluciones, que va a proponer la estrategia y los procedimientos para mantener los procesos críticos de TI de la organización en operación ante un evento disruptivo, mientras camina paralelamente el proceso de recuperación total de los servicios.

Al no disponer de un plan de recuperación como tal, tampoco de normas, políticas, procedimientos o metodologías ágiles para la recuperación de servicios críticos en la continuidad de las aplicaciones y equipos de TI, se podrían producir cuantiosas pérdidas económicas, de imagen, de clientes, de información, entre otros aspectos que repercuten negativamente en la compañía en cuestión.

Esta investigación en su etapa final dará los procedimientos necesarios para que un grupo multidisciplinario interno pueda realizar el Plan de Recuperación de Desastres, enfocado en la nube y mantener un nivel de seguridad aceptable. Este plan permitirá de una forma transparente que los servicios analizados mantengan disponibilidad en caso de algún desastre que provoque una disrupción en alguno de ellos.

CAPÍTULO I

1 INTRODUCCIÓN

1.1 Generalidades

La actualidad en Costa Rica, en temas de ciberseguridad, no es muy alentadora, la cultura no existe, los puestos de trabajo no existen o son mínimos, todas las empresas trabajan bajo el pensamiento “a mí no me va a pasar” sin saber que es muy factible que esto ocurra. En los últimos años hemos visto una creciente oleada de ciberataques a compañías grandes, medianas y pequeñas; nadie está exento a sufrir un ataque. Premier Soluciones es una empresa de origen norteamericano enfocada en el desarrollo de software y consultoría internacional, específicamente de JD Edwards, su sede Costa Rica no escapa a la ciberseguridad. Se podría decir que en un modelo de madurez en ciberseguridad esta compañía quedaría con un gran 0 en muchos de los dominios. La inexistencia como mínimo de una política de ciberseguridad la alejan de un estándar en donde debería estar una empresa con clientes alrededor del mundo.

Este trabajo desarrolla un tema muy importante en la ciberseguridad, como lo es el tema de continuidad del negocio; se basa principalmente en uno de los tres pilares de la ciberseguridad como lo es la disponibilidad, sin perder de vista los dos restantes y no menos importantes como lo son la integridad y confidencialidad. Específicamente, se crean los procedimientos necesarios para realizar un “Plan de Recuperación de Desastres” para Premier Soluciones, que no puede permitir perder terreno ante sus competidores que lo llevan muy cercano. Una interrupción de los procesos críticos de TI podría traer consigo riesgos como atrasos en proyectos, demandas por incumplimiento de contratos, pérdida de clientes, daños de imagen, despido de personal, entre otros aspectos negativos. En general, este proyecto busca conocer las mejores prácticas en el mercado, alternativas viables dentro de los puntos de vista de líderes en el mercado en el tema de la continuidad del negocio. De ellos se aprenderá y será aplicable, funcional y seguro para una creación segura y a la medida de un plan de recuperación de desastres por aplicar dentro de la empresa Premier Soluciones, con el fin de dar una mayor resiliencia a sus procesos claves, ante un desastre.

1.2 Definición y descripción del problema

En la actualidad tan competitiva la continuidad del negocio es un tema clave para cualquier organización en donde la empresa en cuestión no se escapa. Es importante ser proactivo e ir por delante de la competencia en este tipo de temas, las amenazas que pudieren causar disrupciones en los procesos críticos de la organización son numerosas y van desde desastres naturales como huracanes, inundaciones, explosiones, incendios hasta eventos causados por el hombre sean o no intencionales como ataques de denegación de servicios, incendios, circuitos eléctricos, entre otros eventos. Es una ventaja competitiva tener los servicios mínimos en funcionamiento en caso de un desastre. Premier Soluciones no cuenta con este un plan de recuperación de desastres y es aquí en donde nace el principal problema que desencadena esta investigación. A falta de este plan, la organización en cuestión podría sufrir problemas económicos, de seguridad, de imagen, estratégicos y de funcionamiento. Una descripción básica de algunos de los riesgos asociados con no tener un plan de recuperación de desastres son los siguientes:

Problemas económicos

- Pérdida de clientes por falta de continuidad del negocio.
- Pérdida de reputación.
- Costos extra de recuperación ante desastres.
- Daño de hardware.
- Pago de salario al personal inactivo.
- Demandas por incumplimiento de contratos.
- Robo de hardware.

Problemas estratégicos

- Pérdida de oportunidades de negocios, nuevos contratos al tratar con organizaciones maduras que requieran un DRP, como requisito para realizar negocios
- Pérdida de participación en el mercado.
- Incumplimiento de contratos.

- Daños de imagen.
- Proceso normal de trabajo detenido.
- Problemas de expansión de operaciones.

Problemas de seguridad

- Explotación de vulnerabilidades en caso de desastres con las defensas abajo.
- Explotación de vulnerabilidades de día Zero.
- Fuga de información.
- Modificación no autorizada a la información.
- Robo de hardware.

Problema de funcionamiento

- Disrupción de los procesos claves de la organización.
- Incumplimiento de contratos.
- Reducción del desempeño/eficiencia operativa.

Como vimos anteriormente, los riesgos en los que puede incurrir una compañía enfocada en desarrollo de software y consultoría son bastante graves y pueden ocasionar pérdidas no solo económicas sino también daños de imagen.

1.3 Justificación

De acuerdo con la publicación (The Acronis Global Disaster Recovery Index: 2011, 2011), se reporta que la mayor cantidad de disrupciones en la continuidad del negocio se presentan por errores humanos con un 60%, con un 44% se encuentran los problemas en el centro de servidores, 56% por actualizaciones y parches, desastres en el sitio un 26%, desastres naturales un 10%, errores en hardware 14%, virus y malware un 18%; como vemos las causas de las disrupciones en la continuidad del negocio son muchas y son variadas y día a día surgirán más. Es aquí en donde se enfoca esta investigación, con la cual se dará un producto que propone un tratamiento a cada uno de estos riesgos y muchos más, por medio de un plan de recuperación de desastres.

Esta solución se enfocará cloud, para un control fácil, mayor flexibilidad, elasticidad de los servicios, la gran cantidad de controles en seguridad, las opciones de disponibilidad y redundancia, el monitoreo continuo, entre muchas características ofrecidas por la nube.

Como una justificación más estratégica, se pude decir que en la actualidad y con fines de evaluación, cuando un cliente desea adquirir o contratar un servicio, hay una ola que le indica que debe pedir a los ofertantes una prueba que indique que cuentan con un plan de recuperación de desastres. A pesar de no ser un requisito indispensable, este podría ser un factor que haga a este prospecto elegir alguna otra opción en el mercado, que le dé mayor confianza. Una organización madura desea tratar con organizaciones maduras también; en otras palabras, puede existir una pérdida de oportunidad de negocio.

1.4 Viabilidad

1.4.1 Punto de vista técnico

Técnicamente se está en la capacidad de realizar esta investigación y valorar las alternativas de implementación de este trabajo de creación. Se cuenta con los conocimientos para determinar los riegos en los cuales se está incurriendo actualmente. También se cuenta con la capacidad para evaluar las técnicas y estándares actuales que permitan la creación de los procedimientos necesarios para la creación del plan de recuperación de desastres. El trabajo se plantea ser enfocado en la nube, que hoy cuenta con muchas características que garantizan la continuidad del servicio, muchas características de seguridad y aspectos técnicos que nos van a permitir desarrollar nuestro trabajo.

1.4.2 Punto de vista operativo

Operativamente se cuenta con la facilidad de realizar este proyecto sin interrumpir las labores de la organización. Se cuenta con los accesos necesarios a la empresa, los contactos y permisos para realizar cualquier entrevista, análisis, solicitud de información y otras actividades que se requieran para esta investigación.

1.4.3 Punto de vista económico

Desde el punto de vista económico para esta investigación, la empresa facilitará lo necesario en cuanto a infraestructura y licencias para el desarrollo de la investigación. En cuanto al recurso humano, no hay costo alguno para la realización del trabajo, por lo que la empresa se ahorrará alrededor de cien dólares por hora laborada para el investigador de este trabajo. Al ser un trabajo enfocado en la nube, facilitará las pruebas de concepto en ella, ya que los proveedores más grandes como Azure y AWS cuentan con productos gratis para este tipo de actividades.

1.5 Objetivos

Se utiliza la taxonomía de Bloom, ya que permite atacar el problema, al clasificar el proceso en que se diseñan los objetivos de una manera secuencial, donde se parte de lo más básico a lo más específico. Igualmente es la taxonomía utilizada por la universidad; para este caso se trabaja con un objetivo general del nivel seis y tres objetivos específicos de los niveles inferiores.

1.5.1 Objetivo general

Construir una guía para la creación de un plan de recuperación de desastres seguro enfocado en la nube para la empresa Premier Soluciones.

1.5.2 Objetivos específicos

Identificar las áreas dentro de Premier Soluciones y sus dependencias de elementos de TI como hardware, software, redes y personas, mínimas, para su funcionamiento.

Conocer la situación actual de Premier Soluciones en términos de Ciberseguridad, según el ISO 27001 – 2014.

Crear un análisis de impacto de negocio (BIA, por sus siglas en inglés) que nos permita conocer los productos y servicios críticos y sus dependencias de TI en Premier Soluciones.

Crear un análisis de riesgos sobre los procesos y servicios críticos identificados en el BIA con el fin de conocer los riesgos que enfrentan dichos procesos.

Confeccionar una guía con las reglas que deberá seguir la empresa Premier Soluciones para lograr con éxito llevar a cabo la implementación de un plan de recuperación de desastres basado en sus reglas de negocio.

1.6 Alcances y limitaciones

1.6.1 Alcances

Como alcances para esta investigación se entregará una guía que propone la implementación de un plan de recuperación de desastres que permita una mayor resiliencia ante desastres, sean naturales o causados por el hombre para la empresa Premier Soluciones. Este plan permitirá la continuidad de las labores diarias mínimas principales, sin afectar su imagen, contratos, compromisos con clientes, planillas y administración de proyectos; en otras palabras, el núcleo fundamental del negocio. Los procesos críticos encontrados sobre los cuales se propone la continuidad son los siguientes:

Proceso de desarrollo de sistemas

Este es el proceso lucrativo principal de Premier Soluciones en donde se realizan desarrollos de sistemas; su cartera de aplicaciones es amplia pero destacan sus productos estrella como: ECOMMERCE, ECOMMERCE CMS, POS y MANAGEMENT CONSOLE; el trabajo día a día consiste en mejorar, depurar o analizar estos sistemas antes mencionados así como realizar modificaciones especiales para clientes sobre los mismos productos base; por ser el proceso lucrativo número uno y además brindar la mayor cantidad de empleo se va realizar el DRP para este proceso. Cabe mencionar que los sistemas que desarrolla Premier Soluciones están implementados con tecnología Microsoft como .net, C#, MVC; pero además existen desarrollos dentro del ERP JD *Edwards EnterpriseOne*, que permiten a sus funciones de negocio, realizar procesos más eficientes dentro del mismo núcleo del producto.

Procesos de aseguramiento de calidad (QA)

Por sus siglas en inglés QA (quality assurance), es un proceso que realiza un determinado departamento de Premier Soluciones, encargado de realizar las pruebas

pertinentes sobre los productos de software de la compañía y tiene como objetivo asegurar la calidad del producto en términos de funcionalidad, consistencia y seguridad. El QA se realiza en mayor proporción sobre el software, aunque hay procesos de QA que se realizan sobre consultorías y configuraciones específicas en un cliente.

Proceso de recursos humanos

Este proceso es el encargado de gestionar las necesidades, deberes y obligaciones de Premier Soluciones para con sus empleados. Los procesos principalmente son el pago de planillas a empleados, bonos, viáticos, recepción de pagos, gestionar vacaciones, entre otros.

Proceso de administración de proyectos

Es el proceso mediante el cual un Program Manager o Project Manager administra los diferentes proyectos en términos de recurso humano, tiempo y costos, con el fin de lograr alcanzar las diferentes metas trazadas estratégicamente.

Procesos de consultoría en JD Edwards

Proceso lucrativo de Premier Soluciones en donde su personal colabora con el cliente en temas estrictamente de JD Edwards como lo son instalaciones nuevas, modificación de instalaciones existentes, configuración de módulos, entre otras actividades. Cabe destacar que esas personas necesitan un ambiente interno de pruebas en caso de querer hacer configuraciones locales antes de llevarlas al cliente y es aquí en donde nace la necesidad.

Procesos de soporte técnico

Soporte técnico es un pequeño departamento en Costa Rica que se encarga de coordinar acciones técnicas sobre la infraestructura tecnología de Costa Rica y Miami ambas sedes cuentas con este departamento.

Comunicación

Es el proceso que permite la comunicación de los miembros de la organización, de forma normal, tanto interna como externa y de forma remota.

Service Plus

Proceso mediante el cual un cliente reporta un problema encontrado en su sistema miembro de la cartera de aplicaciones Premier Soluciones. Este departamento gestiona todo el proceso de atención del problema desde su recepción hasta su finalización.

Datos

Todos los procesos anteriores manejan datos y muchos de ellos son compartidos. El proceso de manejo de datos es de suma importancia en la actualidad y va a ser un logro grande para Premier Soluciones analizar los procedimientos involucrados en el manejo de estos y que sistemas informáticos de manejo de datos, deben ser incluidos en los procedimientos de creación del DRP.

1.6.2 Limitaciones

Como limitación para este proyecto, se identifica la falta de experiencia del autor e investigador en temas de continuidad del negocio, además del poco tiempo con que se cuenta para la conclusión de esta. La cantidad de servicios utilizados por Premier Soluciones para la operación normal del día a día, son numerosos, debido al nicho de negocio en el que se encuentra. La falta de cultura en ciberseguridad, dentro de esta organización, es otra limitante, debido a que no existen procesos previos en temas de ciberseguridad; se incluyen temas de continuidad del negocio, que pudieran colaborar como insumo para esta investigación.

La instalación y configuración de *JD Edwards EnterpriseOne,* es todo un proceso llevado a cabo por profesionales certificados en la materia, de los cuales Premier Soluciones goza del privilegio de tener muchos de ellos; la configuración del ERP queda fuera del alcance de este proyecto.

La Base de Datos IBM DB2 queda excluida de este proyecto, debido a que, según el análisis de realizado sobre su uso, en todos los clientes de Premier Soluciones, cada cliente provee acceso a una capa propia de negocios, para trabajar directamente conectado a sus bases de datos de desarrollo, sin necesitar recursos internos; por ello, queda fuera del alcance, al ser un ambiente de recuperación lo que se está creando.

Este trabajo da los procedimientos que deberá seguir un grupo multidisciplinario para la creación del DRP (disaster recovery plan) y no un DRP, como producto final, los costos de la implementación están fuera del alcance de esta investigación. Algunos factores que podrían inferir directamente en el precio final del producto son: elección del cloud, variación de precios en el tiempo, horas consultoría, elección del equipo multidisciplinario, tecnologías emergentes, entre otros.

CAPÍTULO II

2 MARCO TEÓRICO

2.1 Plan de recuperación de desastres

El producto estrella de este trabajo es la generación de los procedimientos necesarios para la implementación de un Plan de Recuperación de Desastres para la empresa Premier Soluciones; es por eso por lo que se debe conocer el término y para qué se utiliza. Este plan de recuperación de desastres es conocido, por sus siglas en inglés, como DRP, y se diseña para responder a incidentes no planificados que amenazan la infraestructura de TI y por consiguiente la continuidad del negocio; se debe comprender por infraestructura el hardware, software, redes, procesos y personas. Este plan a su vez pretende tomar las precauciones para minimizar los efectos de un desastre y sumar una alta resiliencia a la organización, para reanudar sus servicios críticos.

Todo DRP debe estar enfocado en software, hardware, personas, redes, procesos y personas críticos, para el proceso de negocio; además, es de suma importancia, principalmente para Premier Soluciones, el contar con un análisis de riesgos para lograr determinar cómo podrían impactar negativamente las operaciones normales de una organización. Generalmente el DRP es flexible a las necesidades de cada empresa y puede ser modular adaptándose a los requisitos en la organización.

Según (Toigo, 1996), la recuperación de desastres se está convirtiendo en un aspecto cada vez más importante de la informática empresarial. Como los dispositivos, sistemas y redes se vuelven cada vez más complejos, simplemente hay más cosas que pueden salir mal. Como consecuencia de ello, los planes de recuperación se han vuelto más complejos.

Según (Contingency Planning Guide for Federal Information Systems, 2010), de la NIST, por sus siglas en inglés National Institute for Standards and Technology de los Estados Unidos, lo que viene a continuación resume la estructura ideal de un plan de recuperación de desastres TI. Estos procedimientos describen los pasos por seguir para la creación de un DRP. Es un ejemplo expuesto para entenderlo y que podría ser su composición; no quiere decir que haya que utilizarlos en esta investigación.

- Elaboración de la declaración de políticas para el plan de contingencia. Contar con unas directivas formales que proporcionan la autoridad y orientación necesaria para elaborar un plan de contingencia efectivo.
- Realización del análisis de impacto sobre el negocio (BIA). El análisis del impacto sobre el negocio ayuda a identificar y priorizar los sistemas y componentes críticos de TI.
- Identificación de controles preventivos. Medidas que reducen los efectos de las disrupciones al sistema y pueden aumentar su disponibilidad y reducir los costos de contingencia del ciclo de vida.
- Desarrollo de estrategias de recuperación. Tener una estrategia integral garantiza que el sistema se recuperará de manera rápida y efectiva después de una disrupción.
- Desarrollo de un plan de contingencia TI. El plan de contingencia debería contener orientaciones y procedimientos detallados para la restauración del sistema dañado.
- Prueba, formación y ejecución del plan. La prueba del plan identifica lagunas en la planificación, mientras que la formación prepara al personal de recuperación para la activación del plan; ambas actividades mejoran la eficacia del plan y la preparación general de la entidad.
- Mantenimiento del plan. El plan debería ser un documento vivo que se actualiza regularmente para mantenerlo al día con mejoras al sistema.

2.2 Desastre

Uno de los objetivos de esta investigación, es brindar resiliencia robusta ante posibles desastres que puedan ocurrir dentro de la infraestructura interna o externa (subcontratada) de Premier Soluciones, que pueda afectar la continuidad de algún producto o servicio en específico. Dentro de un plan de recuperación de desastres, ¿a qué se le puede llamar un desastre? Un desastre en un DRP es cualquier evento que pueda causar una disrupción de alguno de los procesos críticos de TI; pueden ser o no, causados por el hombre. No causados por el hombre se puede mencionar que en una de las instalaciones físicas propias o subcontratadas, se imposibilite la continuidad de

algunos de los servicios críticos de Ti; como ejemplo, un malware que atacó parte de la infraestructura, ataque de denegación de servicios sobre un sistema crítico, proveedor externo de un sistema crítico fuera de línea, un corto circuito en hardware importante, caída del internet por más tiempo que el definido en el RTO o hackeo de uno de los sistemas críticos. Como desastres no causados por el hombre, se mencionan todos los desastres naturales como huracanes, inundaciones, terremotos, entre otros, que afecten el área de trabajo o la estancia de algún componente de TI, importante para la continuidad.

2.3 RTO, RPO y MTD

De la mano con la continuidad del negocio, en este caso el Plan de Recuperación de Desastres, se encuentran conceptos como RTO, por sus siglas en inglés *Recovery Time Objetive* y el concepto RPO, por sus siglas en inglés *Recovery Point Objetive*; ambos son conceptos claves en la recuperación, ya que darán un parámetro base para ajustar la estrategia de recuperación a dichos parámetros, como definición para el RTO, es el tiempo durante el cual una organización puede tolerar la falta de funcionamiento de sus aplicaciones y la caída de nivel de servicio asociada, sin afectar a la continuidad del negocio. Este concepto se recomienda aplicarlo a cada una de las aplicaciones por separado, puesto que cada una tiene su criticidad por encima de las demás. Otro aspecto por mencionar es que se recomienda que este tiempo se tome desde el instante que sucede el incidente, en lugar del momento en el que el equipo de TI comienza a trabajar, para solucionar y ver un escenario más realista.

El RPO es un concepto aplicable más a los datos y podría definirse como la cantidad máxima permitida de datos perdidos, medidos en el tiempo desde la ocurrencia de una falla hasta el último backup válido. Este valor se recomienda estar a cero, lo más cercano posible, pero el valor de los controles podría ser un poco costoso.

En la FIGURA 1, se observa sobre una línea de tiempo, cómo actúan el RPO y el RTO. Ambos son conceptos que miden cosas por separado, pero siempre se relacionan en algún punto. Por ejemplo: si para Premier Soluciones el que su servidor de base de datos *EnterpriseOne*, esté caído por una hora, tal vez no es un problema tan grave a nivel de tiempo, porque el atraso en los proyectos sería mínimo; por ello, un RTO

de una hora, estaría perfecto para comenzar. En cuanto al RPO, se pensaría que, al ser una empresa de desarrollo de software, un punto restauración de datos de no más día, no sería tan trágico, si se habla únicamente del desarrollo interno.

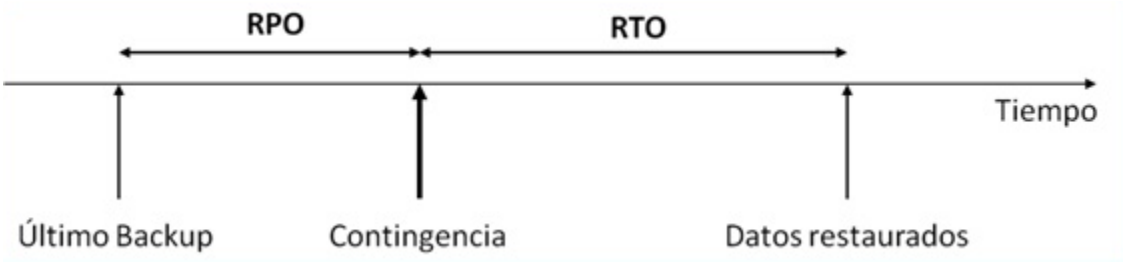


Figura 1. RPO y RTO

Otro tiempo que se debe conocer, es el Tiempo de inactividad máximo tolerable (MTD por sus siglas en inglés), y se refiere al tiempo máximo que la organización puede estar sin un producto o servicio, antes de entrar en crisis, que se produzcan efectos desastrosos en la compañía y repercuta en el negocio. Un ejemplo de esto sería, que el proceso de “Atención a incidentes internos”, no debe superar las 16 horas; para este caso el MTD sería de 16 horas.

2.4 JD Edwards EnterpriseOne

El negocio principal de Premier Soluciones es integrar su Suite de aplicaciones, como lo son el eCommerce (CMS), Punto de Venta (POS, por sus siglas en inglés) en tiempo real con el ERP (Enterprise Resource Planning) JD Edwards EnterpriseOne. Es por ello por lo que este concepto debe ser conocido en esta investigación de forma que dé al lector un conocimiento básico intermedio acerca de qué trata este componente. Como definición, por parte de su dueño Oracle, se puede decir que es una suite de aplicaciones integradas de software ERP que combina el valor comercial con la tecnología basada en estándares y una profunda experiencia sectorial en una solución empresarial de bajo coste total de propiedad. A su vez se puede decir que es una solución Global que se adapta a numerosas empresas en todo el globo terrestre, debido al gran número de configuraciones que posee y permite operar sin ningún problema como, por ejemplo: es multi-país, multi-compañía, multi-idioma y multi-moneda; esto da a entender que las barreras cultures, socio económicas, no son un problema para una compañía que decida optar por una solución de estas. Premier Soluciones cuenta con su instalación JD Edward EnterpriseOne en un servidor Windows

ubicado en el centro de datos de Telefónica en Miami Florida, que está disponible en la mayoría de los proveedores de servicios en la nube; esta información fue validada en AWS y Azure.

2.5 ERP (Enterprise Resource Planning)

ERP por sus siglas en inglés *Enterprise Resource Planning,* significa sistema de planificación de recursos empresariales. JD Edwards EnterpriseOne, como tal es un ERP y es uno de los actores principales dentro de este trabajo, del cual se crearán los procedimientos necesarios para dar una continuidad en un futuro DRP para Premier Soluciones. Como definición se puede decir que es un sistema integrado capaz de manejar diferentes operaciones de una compañía, como, por ejemplo: producción, inventario, envíos, contabilidad, facturación, logística o incluso recursos humanos, entre otros; todos los datos de las diferentes operaciones, dentro de una sola base de datos y encapsulados en módulos. JD Edward EnterpriseOne, en su página web, muestra un número grande de módulos (véase la FIGURA 2.)

Figura 2. Módulos JD Edwards EnterpriseOne

Los ERP-s funcionan en todo tipo de empresas y su selección depende de factores como el tamaño de la empresa, el tipo de empresa, procesos, recursos, entre otros. La principal desventaja de la utilización de este software es el precio, no solo de adquisición sino también de consultoría, para la instalación y adaptación a su empresa; sin embargo, también tiene ventajas y estas son algunas de las principales:

- Automatización de procesos de la empresa.
- Disponibilidad de la información de la empresa en una misma plataforma.

- Integración de las distintas bases de datos de una compañía en un solo programa.
- Ahorro de tiempo y costes.

Otra ventaja de algunos ERP-s es que ofrecen integración con soluciones de BI o Inteligencia Empresarial (BI, por sus siglas en inglés). Permite realizar informes sobre el estado de su empresa directamente con los datos del sistema ERP y JD Edwards EnterpriseOne, no es la excepción; estas herramientas ayudan a la toma de decisiones por la facilidad de tenerlos todos en una base de datos centralizada.

2.6 AS400

Como justificación de conocer este término, AS/400 es el servidor propietario de IBM que corre la base de datos de DB2/400; es una de las bases de datos, relacional, que soportan las soluciones que ofrece JD Edwards EnterpriseOne a sus usuarios. Las soluciones de software que ofrece Premier Soluciones abarcan DB2/400, como una de las bases de datos soportadas; es por esto que se debe conocer un poco de este término. Se puede decir que AS/400 es un sistema integrado muy complejo que incluye el hardware, el software, la seguridad, una base de datos y otros componentes propietarios. El AS/400 se diseña para separar el software y el hardware, así que los cambios en uno tienen poco efecto en el otro. Esto se logra a través del interfaz de la máquina (MI) que es un interfaz de la programación de software entre el uso, el sistema operativo y el hardware. El MI es un interfaz de programación de uso completo (API) fijo, que todos los usos deben utilizar para conseguir el hardware; este es cómo el AS400 alcanza la independencia del software. Su sistema operativo se llama OS/400; DB2/400 es la base de datos integrada, que es utilizada por Premier Soluciones. Esta base de datos es parte los componentes de software separados que residen encima del sistema operativo. En términos de continuidad del negocio, en una búsqueda inicial se determinó que IBM posee un cloud que ofrece tener una base de datos DB2. Por ello, la factibilidad de contar con esta característica dentro del proyecto, enfocado en la nube, continúa estando disponible; se encuentra evidencia que tanto Azure como AWS, tienen la

posibilidad de tener un DB2 en su nube. En la Figura 3 se puede observar la opción que brinda AWS dentro de su nube.

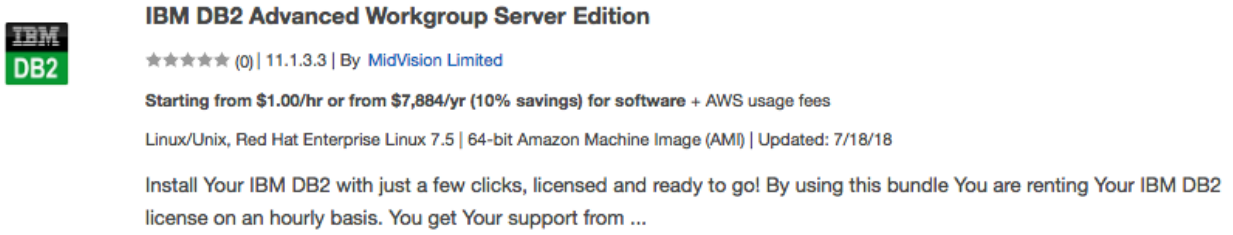


Figura 3. IBM DB2 AWS

2.7 Computación en la nube

Según (Sosinsky, 2010), el termino computación en la nube se refiere a las aplicaciones y servicios que se ejecutan sobre una red distribuida, al utilizar recursos virtualizados y accedidos mediante protocolos de red e Internet. Se distingue por la idea de que los recursos son virtuales y sin límites y que los detalles de los sistemas físicos sobre los que se ejecuta el software se abstraen del usuario. La idea, según lo leído anteriormente, consiste en tener servidores conectados entre sí, en donde se ofrecen servicios que son accedidos a través de internet; dicen ser recursos ilimitados porque cuentan con números y potentes servidores que comparten sus servicios de acuerdo con la demanda que así requiera cada cliente en particular.

Computación en nube es un nuevo paradigma de la computación que ha estado impactando a las organizaciones que hacen uso de los recursos de las tecnologías de la información y comunicación (TIC). Estas compañías están aprovechando este modelo de computación utilitaria, que consiste en contratar los servicios computacionales a un Proveedor de Servicios de Cloud Computing. Estos servicios incluyen procesamiento de datos, almacenaje, servidores virtuales, etc.

El plan de recuperación de desastres, para Premier Soluciones, buscar centrar su núcleo en la nube y aprovechar muchas de sus facilidades que esta da tales como:

- Baja inversión inicial.
- Eficiencia de costos.
- Elasticidad.

- Fácil uso y mantenimiento.
- Innovación.
- Continuidad del negocio fácil de ejecutar.

2.7.1 Tipos de nube

La computación en la nube cuenta con tres tipos básicos de entrega. En la FIGURA 4, se pueden observar los tipos de nubes básicas, entre ellas nube pública, nube privada y nube híbrida; a continuación, los tres tipos de nubes:

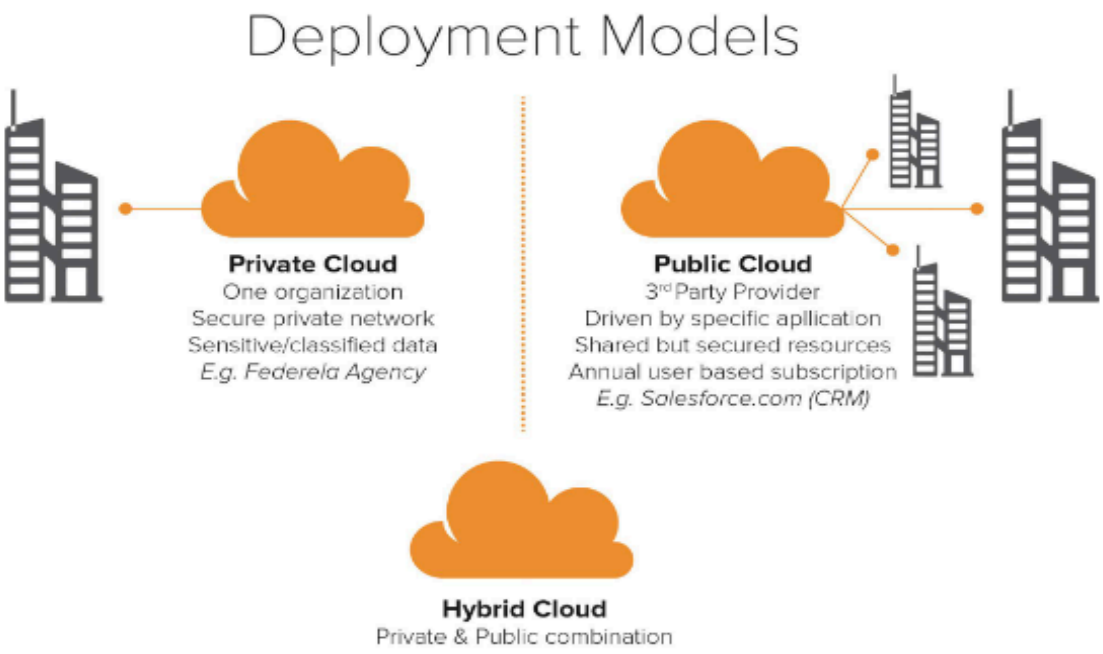


Figura 4. Tipos básicos de nube

2.7.1.1 Nube pública

Se define como infraestructura de nube compartida que es propiedad de un proveedor de nube, que se encarga de su mantenimiento y gestión, como Amazon Web Services o Microsoft Azure; entre sus principales beneficios se encuentran: su escalabilidad bajo demanda y sus precios de pago por uso.

2.7.1.2 Nube privada

Según Microsoft una nube privada es el conjunto de servicios informáticos que se ofrecen a través de Internet o de una red interna privada, solamente a algunos usuarios y no al público en general. Un inconveniente es que el departamento de TI de

la compañía es responsable de la administración de la nube privada y el costo que conlleva. Por tanto, las nubes privadas requieren el mismo gasto de personal, administración y mantenimiento que los centros de datos tradicionales en propiedad.

Las nubes privadas son productos *IaaS* dedicados a un solo cliente, lo que significa que, a diferencia de las nubes públicas, los usuarios no comparten recursos. Las nubes privadas incluyen infraestructura virtualizada, como el cómputo y el almacenamiento al que los usuarios pueden acceder en forma de autoservicio.

2.7.1.3 Nube híbrida

Según Microsoft, una nube híbrida es un entorno informático que combina una nube pública y una nube privada y permite que se compartan datos y aplicaciones entre ellas. Cuando la demanda de recursos informáticos y procesamiento fluctúa, la informática en nube híbrida permite a las empresas escalar sin problemas su infraestructura local en la nube pública, para poder administrar cualquier flujo de trabajo, sin necesidad de permitir que centros de datos de terceros accedan a todos sus datos. Las organizaciones obtienen la flexibilidad y la capacidad informática de la nube pública para tareas informáticas básicas y menos delicadas, mientras que mantienen las aplicaciones y los datos críticos para la empresa en la infraestructura local, a salvo detrás de un *firewall* de la compañía.

2.7.2 Servicios en la nube

La gran nube ofrece tres tipos de servicios, que se pueden utilizar y mezclar, cada uno, para realizar acciones específicas; en la FIGURA 5 se observan los tipos servicios que ofrece la nube.

Figura 5. Tipos de servicios en la nube

Infraestructura como un servicio (IaaS), es una forma básica de computación en la nube, que permite al usuario alquilar infraestructura de TI a un proveedor de servicios en la nube; esta infraestructura puede ser: servidores, máquinas virtuales, almacenamiento, redes y sistemas operativos.

Plataforma como un servicio (*PaaS*), es un servicio ofrecido a los desarrolladores que brindan las herramientas para crear y hospedar aplicaciones web de una manera sencilla; por medio de estos servicios, los encargados de TI no deberán preocuparse por configurar y administrar la infraestructura de servidores.

El siguiente servicio conocido es el Software como un servicio (*SaaS*), es un método de entrega de una aplicación de software a través de internet. En este tipo de servicio, los proveedores de servicios en la nube hospedan y administran las aplicaciones. Un ejemplo de este tipo de servicios es el office365; todo el software brindado por este se accede por medio de internet. SaaS son aplicaciones que se ejecutan en los servidores de la nube en lugar de los equipos o servidores del cliente. Esto permite al cliente ejecutar la aplicación en su navegador web sin necesidad de instalación (Leavitt, 2009). En este modelo, los usuarios disponen de acceso al aplicativo,

al estar incluido dentro de este modelo las infraestructuras y recursos necesarios para la entrega del servicio suscrito con base en ‘pago-por-uso’.

2.8 Resiliencia

La resiliencia es un término importante en la continuidad del negocio y consiste en sobreponerse o recuperarse a situaciones adversas; por otro lado, en una organización la resiliencia se da al superar los malos tiempos o adaptarse a ellos. Una organización altamente resiliente es aquella que es coherente, adaptable, competitiva, ágil y robusta (The British Standards Institution, 2014).

La resiliencia implica reestructurar nuestros recursos en función de las nuevas circunstancias y nuestras necesidades. De esta manera, las entidades resilientes, no solamente son capaces de sobreponerse a las adversidades, sino que van un paso más allá y utilizan esas situaciones para crecer y desarrollar al máximo su potencial. Este concepto es de gran importancia en el trabajo, ya que el objetivo del Plan de Recuperación de Desastres es lograr la resiliencia de Premier Soluciones.

2.9 eCommerce

eCommerce, es un producto de la suite de Premier Soluciones, es un método de compra de productos que se vale solamente de internet como medio de comercializar de manera online. La solución eCommerce de Premier Soluciones se conecta a las bases de JD Edwards EnterpriseOne, al trabajar directamente con los datos disponibles en el ERP; esto quiere decir que en tiempo real se actualizan los datos de las tablas. Uno de los éxitos de este producto es que llega a cada persona independientemente de su localización con solo contar con acceso a internet. De acuerdo con (Nielsen, 2017) se confirma un crecimiento a nivel mundial del comercio electrónico (conocido también por su sigla en inglés eCommerce) a ritmos del 23% cada año; esto hace el uso de eCommerce más popular entre las personas cada vez más. *“En Latinoamérica el promedio es del 10% de crecimiento, pero esos números pueden alcanzar hasta un 64%”*, (Nielsen, 2017); según el estudio, el uso de los eCommerce va en aumento cada vez más.

Los eCommerce en general cuentan con una serie de ventajas respecto al comercio tradicional, algunas de ellas son las siguientes:

- Disponibilidad 24 horas durante los 365 días del año para el cliente.
- No existen barreras geográficas para el cliente.
- Ventaja competitiva respecto al comercio tradicional.
- Posibilidad de segmentar a los clientes al trabajar online, mejorar la comunicación y lanzar campañas especializadas.
- Extender el alcance de tu negocio a nuevos usuarios, pero reducirlo respecto a otros.

Otro punto importante por destacar es que existen varios tipos de eCommerce dependiendo la naturaleza de sus transacciones y la forma que generan ingresos; a continuación, dos tipos utilizados hoy por los clientes de Premier Soluciones:

- B2B (Business-to-Business): empresas que comercian con otras empresas u organizaciones. Premier Soluciones cuenta con clientes que no venden a personas individuales, sino a compañías.
- B2C (Business-to-Consumer): empresas que comercian con consumidores. Es el más habitual y es el modelo en el que se le vende a personas individuales; este es el caso en el que tiene más clientes Premier Soluciones.

En la FIGURA 6, se observa un ejemplo con una arquitectura muy básica del flujo del eCommerce en donde existen tres actores: los usuarios finales, el eCommerce y un data center. En el data center, se encuentra el servidor JD Edwards EnterpriseOne, servidor de base de datos E1 y la capa de negocios; por el medio el eCommerce en la nube aplicación de Premier Soluciones y por último todos los usuarios finales que acceden el eCommerce. La petición la hace el usuario, el eCommerce la recibe y manda la petición al centro de datos en donde se encuentra la capa de negocios, la que a su vez se comunica con la base de datos de E1 y así actualiza en tiempo real de una forma amigable las tablas.

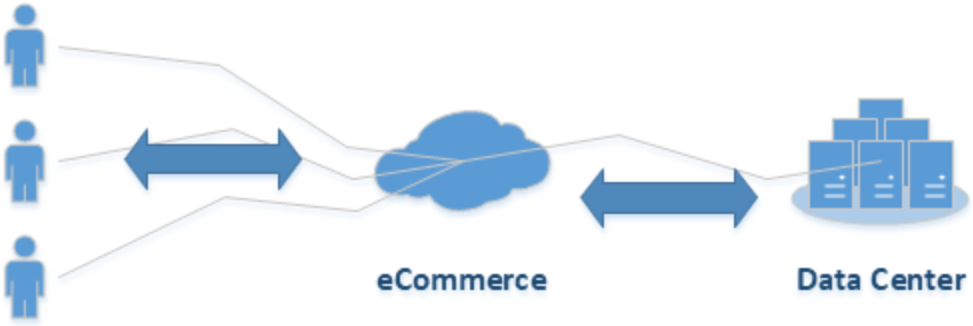


Figura 6. eCommerce arquitectura básica

2.10 Sitefinity CMS

Content Management System, por sus siglas en inglés, de acuerdo con el conocimiento adquirido durante años de trabajo para Premier Soluciones, un CMS es un software que permite crear y gestionar el contenido de un sitio web de una manera sencilla y rápida. De esta forma, la persona que lo adquiere podrá crear sus sitios web y páginas de contenido por medio del software, sin la necesidad de tener amplios conocimientos en alojamientos de sitios web o creación de páginas, debido a que el CMS, le permite, mediante plantillas, elegir diseños, subir imágenes, agregar contenido, entre otras facilidades; en muchos casos el proveedor del CMS permite el alojamiento del sitio. Premier Soluciones, por su parte, da este salto, años atrás de colocar su producto estrella **eCommerce,** en este tipo de software y ser pionero en el sector; de esa idea nace el **eCommerce CMS,** hoy producto estrella de la empresa, utilizado ya por empresas de renombre. El CMS elegido por Premier Soluciones, es Sitefinity el cual da la flexibilidad de hacer programación a la medida y permitir incluir la funcionalidad dentro del negocio, por medio de *.net* que es el lenguaje oficial de programación; este producto es adquirido por empresas que tienen contenidos dinámicos y que cambian constantemente.

CAPÍTULO III

3 ANÁLISIS DE LA SITUACIÓN ACTUAL

3.1 Historia de Premier Soluciones

Premier Soluciones tiene su sede principal en Miami, Florida, es un proveedor internacional líder de soluciones empresariales, se compone de software empresarial, servicios de consultoría de gestión y tecnología habilitadora. El enfoque de Premier, para brindar beneficios comerciales a sus clientes, es asociarse con proveedores de tecnología y desarrolladores de software empresarial, líderes en el mercado, como Oracle / JD Edwards y Microsoft, junto con la atracción de profesionales de consultoría altamente calificados, especializados en industrias, procesos y soluciones tecnológicas específicas.

Con la línea de productos *SmarterCommerce* de Premier, junto con soluciones de socios, Premier proporciona soluciones empresariales sólidas que abordan áreas como procesamiento de tarjetas de crédito, comercio electrónico B2C y B2B, aplicaciones de comercio móvil, punto de venta minorista (POS) y soluciones de centro de llamadas que están preintegrados con JD Edwards, así como con otras tecnologías de los clientes; se pueden implementar rápidamente en una base de tiempo y tarifa fijos.

Desde el inicio de la compañía, a principios de la década de 1990, el éxito de Premier, en el mercado, ha permitido un rápido crecimiento y expansión. Hasta la fecha, Premier ha brindado soluciones empresariales y servicios de consultoría, como JD Edwards y SmarterCommerce, a más de 250 sitios de clientes, en casi 20 países, incluidos los Estados Unidos y países de todo el Caribe, América Latina, Europa y Asia-Pacífico.

3.2 Identificación del negocio

Premier Soluciones, en su sede Costa Rica, cuenta con su centro de operaciones en donde se encuentra el personal necesario encargado de crear los productos de software, dar el mantenimiento y la atención a problemas en los clientes; además, brinda consultoría en el área de *JD Edwards*, principalmente.

El área operacional fuerte se encuentra en esta sede, todos y cada uno de los procesos que se realizan día a día en esta oficina es importantes, uno a uno,

independientemente de la posición en que se desempeña cada persona. Existen dentro de la compañía dos grandes divisiones: Desarrollo de Software y Consultoría en JD Edwards; adicional existen áreas un poco más pequeñas como el área administrativa y de administración de proyectos, cada área tiene sus procesos estándar de trabajo día a día, cada uno de estos procesos utiliza personas, hardware, software, comunicaciones, administración, experiencia, entre otros aspectos, para llevar a cabo las tareas día a día.

La identificación de estos procesos dentro de cada área de negocio dirige hacia la creación de los procedimientos adecuados y seguros para la creación de un futuro Plan de Recuperación de Desastres en Premier Soluciones.

3.3 Procesos por área

Después de un análisis en alto nivel de la actividad de Premier Soluciones, se han identificado áreas críticas que deben ser incluidas dentro del alcance de los procesos que debe cubrir el Plan de Recuperación de Desastres, para garantizar la continuidad del negocio. En la FIGURA 7 se pueden ver, de una forma gráfica, las áreas que componen el negocio de Premier Soluciones: desarrollo de software, consultoría en JD Edwards, recursos humanos, service plus y administración de proyectos; en dichas áreas hay procesos críticos compartidos, como la comunicación y datos.

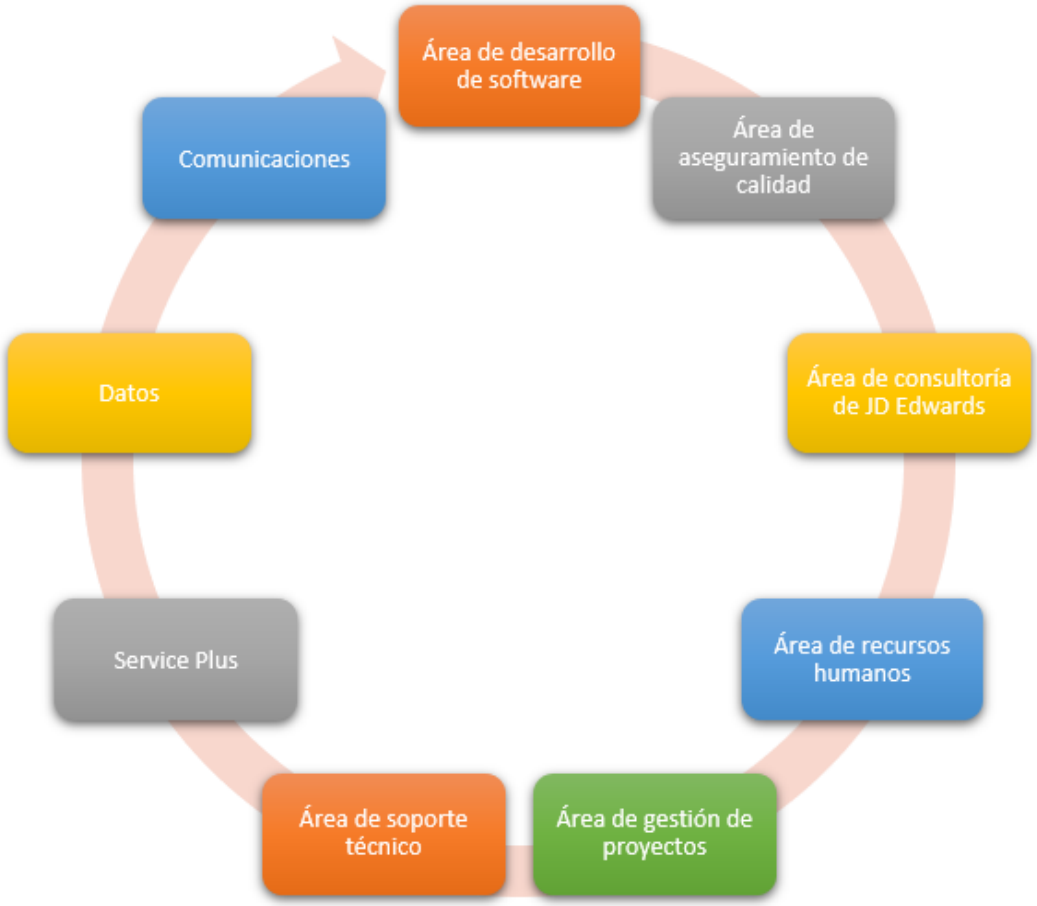


Figura 7. Áreas de Premier Soluciones

3.3.1 Área desarrollo de software

El desarrollo de software es el proceso más lucrativo de Premier Soluciones en él se encuentra depositada la confianza de decenas de clientes alrededor del mundo. Esta área crea el software que se integra con JD Edwards EnterpriseOne; esto significa que una persona de X puede consumir los productos que vende la empresa que posea el ERP de una forma amigable e intuitiva y utilizar las soluciones software de Premier Soluciones. Tal es el caso de la utilización del ECommerce, que, como ventaja competitiva sobre otros competidores del mercado, se integra a la perfección con los datos del ERP y todos estos procesos internos ocurren en tiempo real y de una forma transparente. En la FIGURA 8, se ve el producto final eCommerce que ofrece Premier Soluciones:

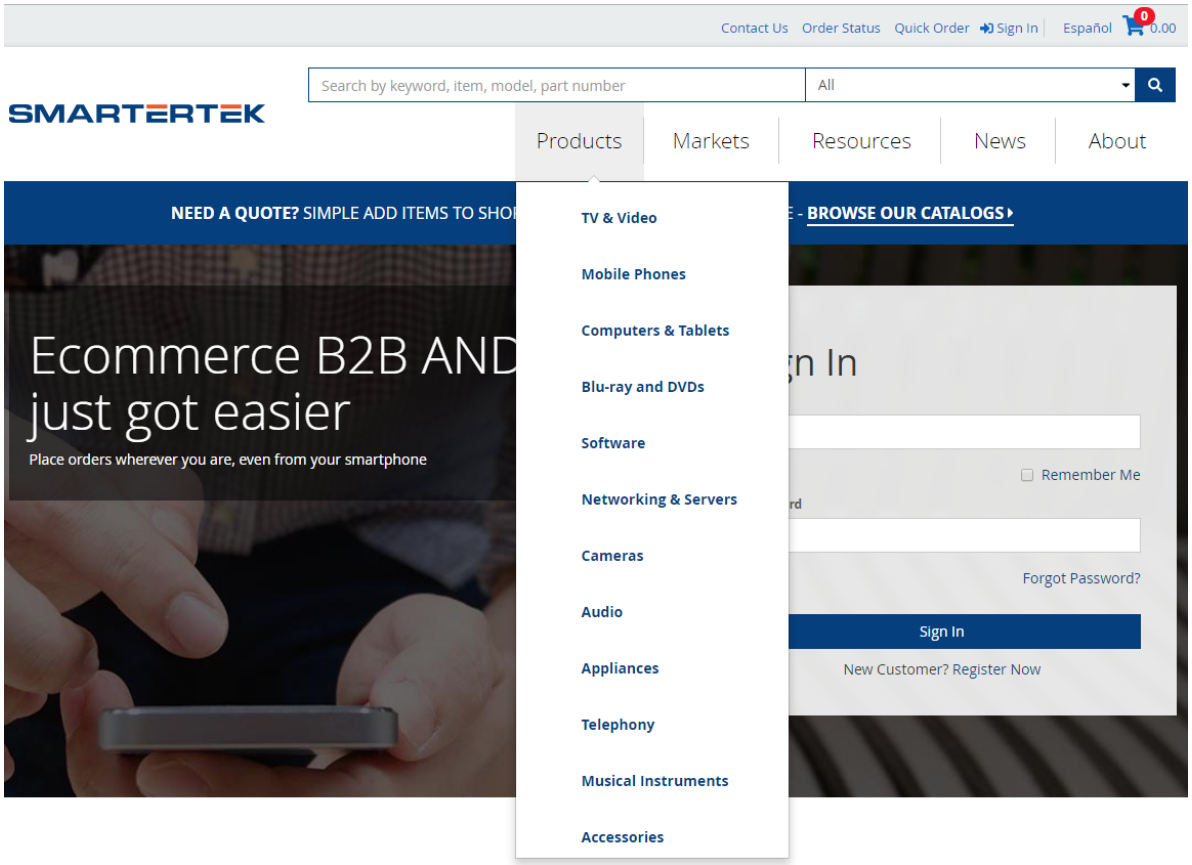


Figura 8. eCommerce Premier Soluciones

Otra de las soluciones de software estrella de Premier Soluciones es su POS (Point of Sale). Este software se integra, al igual que el eCommerce en JD Edwards EnterpriseOne, en tiempo real y es un software especializado en ventas en el sitio; esto quiere decir que se utiliza dentro de un local físico como supermercados, farmacias, entre otros comercios. En la FIGURA 9, se puede ver el POS que ofrece Premier Soluciones:

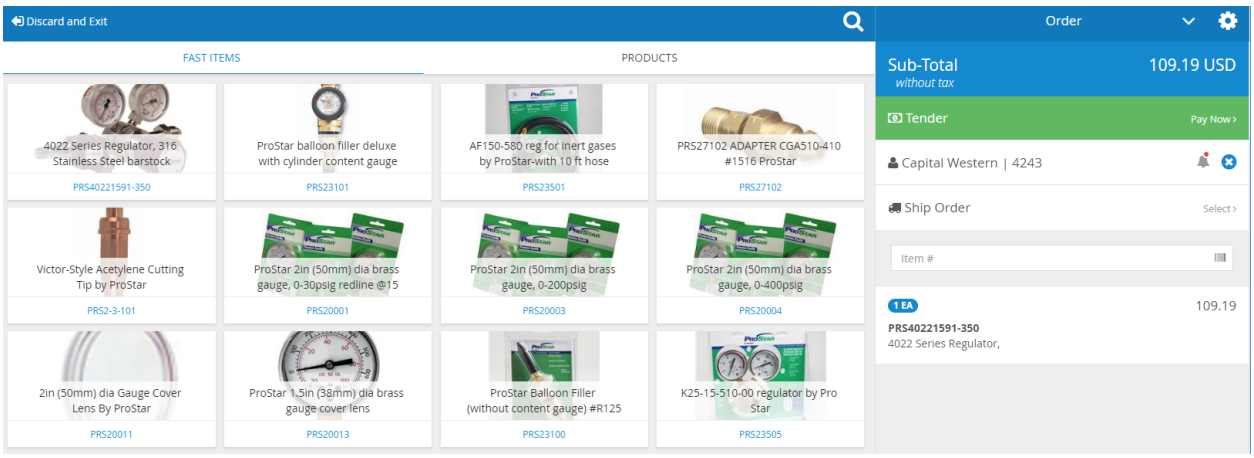


Figura 9. POS Premier Soluciones

Cada área tiene procesos y estos a su vez cuentan con subprocesos, que a su vez tienen sistemas asociados indispensables para realizar las tareas. Estos sistemas se mencionan, en forma general, en la siguiente tabla:

Hardware	
Servidor de JD Edwards EnterpriseOne	Ubicado en Telefónica data center en Miami.
Servidor de bases de Datos Oracle	Ubicado en Telefónica data center en Miami.
Servidor de bases de datos IBM/400	Ubicado en Telefónica data center en Miami.
Servidor de bases de datos SQL Server	Ubicado en Telefónica data center en Miami.
Máquina Windows i7, 16 GB RAM, 1TB Disco Duro	Máquina de uso personal para el trabajo.
Internet	
Servidor web - Desarrollo y pruebas	Máquina virtual utilizada como Web. Server. Ubicada en Telefónica para probar desarrollos y realizar los procesos de QA (SCWEBDV).
Servidor de aplicación - Desarrollo y pruebas	Máquina virtual utilizada como Application Server. Ubicada en Telefónica para probar desarrollos y

	realizar los procesos de QA (SCAPPDV).
Servidor de producción	Máquina virtual utilizada para realizar demostraciones a clientes o prospectos. Ubicado en Telefónica data center en Miami.
Software	
Visual Studio	Se cuenta con licencias para cada máquina utilizada. Actualmente cada usuario se autentica por medio del active directory de Premier Soluciones (TPGNET)
Team Foundation Server	Sirve como repositorio de Código Fuente, además manejo de proyectos de software. Actualmente cada usuario se autentica por medio del active directory de Premier Soluciones (TPGNET).
SQL Server Client, Oracle Client, iSeries client	Clientes gratuitos de conexión a base de datos.
Office 365(Word, Excel, Outlook, Power point, Teams)	El equipo ofimático lo utiliza cada miembro de la organización, el correo

	de la compañía es manejado mediante Office 365, al igual que la aplicación de comunicación como lo es TEAMS y Skype for Business. Actualmente cada usuario se autentica por medio del active directory de Premier Soluciones (TPGNET).
VPN	En la oficina existe un único VPN que conecta a Costa Rica con Telefónica Miami, en caso de trabajo en casa se necesita un usuario de VPN personal para utilizar Cisco AnyConnect.
JD Edwards EnterpriseOne	Es necesario para los desarrolladores la utilización de ese software ya que es el core de la funcionalidad y permite mostrar datos y funcionalidad base.

Tabla 1. Hardware y software área desarrollo de software

3.3.2 Área de aseguramiento de calidad

El área de aseguramiento de calidad es grande e importante dentro de cualquier empresa que desarrolle software, debido a la especialización de las personas que lo conforman, el software pasa por niveles básicos de pruebas durante el desarrollo. Estas pruebas abarcan aspectos más funcionales y desde hace unos años aspectos de seguridad con procesos muy informales, pero se da ese primer filtro. Seguidamente, todo desarrollo pasa por el filtro de este departamento; su función principal es asegurar la calidad del software en aspectos de funcionalidad, consistencia de datos, seguridad,

entre otros. Como todas las demás áreas el recurso humano, realiza estas funciones por medio de hardware, software, datos y comunicaciones, que se muestran en las siguientes tablas. El QA no solo se realiza sobre los productos de software, sino también para asegurar la calidad de los servicios de consultoría que se realizan en los clientes.

Hardware	
Servidor de JD Edwards EnterpriseOne	Ubicado en Telefónica data center en Miami.
Servidor de bases de Datos Oracle	Ubicado en Telefónica data center en Miami.
Servidor de bases de datos IBM/400	Ubicado en Telefónica data center en Miami.
Servidor de bases de datos SQL Server	Ubicado en Telefónica data center en Miami.
Máquina Windows i5, 16 GB RAM, 1TB Disco Duro	Máquina de uso personal para el trabajo.
Internet	Todo el acceso a las aplicaciones es por medio de internet.
Servidor web – QA	Máquina virtual utilizada como Web Server. Ubicada en Telefónica para realizar los procesos de QA (SCWEBDV).
Servidor de aplicación - QA	Máquina virtual utilizada como Application Server. Ubicada en

	Telefónica para probar desarrollos y realizar los procesos de QA (SCAPPDV).
Software	
Team Foundation Server	Sirve como repositorio de Código Fuente y manuales de funcionalidad, además manejo de proyectos de software. Actualmente cada usuario se autentica por medio del active directory de Premier Soluciones (TPGNET). En este repositorio además se encuentran los manuales de la funcionalidad del sistema.
Office 365(Word, Excel, Outlook, Power Point, Teams)	El equipo ofimático lo utiliza cada miembro de la organización, el correo de la compañía es manejado mediante Office 365, al igual que la aplicación de comunicación como lo es TEAMS y Skype for Business. Actualmente cada usuario se autentica por medio del active directory de Premier Soluciones (TPGNET).

VPN	En la oficina existe un único VPN que conecta a Costa Rica con Telefónica Miami, en caso de trabajo en casa se necesita un usuario de VPN personal para utilizar Cisco AnyConnect.
JD Edwards EnterpriseOne	Es necesario para QA la utilización de ese software ya que es el core de la funcionalidad y permite mostrar datos y funcionalidad base.

Tabla 2. Hardware y software área de QA

3.3.3 Área de soporte técnico

Esta es un área con poco personal, pero el recurso humano es muy importante, ya que una parte de este se encarga de verificación de equipos de red, comunicación del estado de la red, manejo de incidentes a nivel técnico, instalación de software en máquinas de los colaboradores y en los servidores en Telefónica, instalación de antivirus, configuración de la central telefónica, entro otras funciones. Otra parte del personal de esta área se encarga de la instalación de los productos de software de Premier Soluciones, adquiridos por los clientes; existen personas en Costa Rica y en Miami que básicamente comparten las mismas funciones. A continuación, las necesidades de hardware y software de una persona dentro de esta área.

Hardware	
Máquina Windows i5, 16 GB RAM, 1TB Disco Duro	Máquina de uso personal para el trabajo.
Internet	Todo el acceso a las aplicaciones es por medio de internet.

Software	
Team Foundation Server	Sirve como repositorio de Código Fuente, manuales de instalación e instaladores, además manejo de proyectos de software. Actualmente cada usuario se autentica por medio del active directory de Premier Soluciones (TPGNET). En este repositorio además se encuentran los manuales de la funcionalidad del sistema.
Office 365(Word, Excel, Outlook, Power point, Teams)	El equipo ofimático lo utiliza cada miembro de la organización, el correo de la compañía es manejado mediante Office 365, al igual que la aplicación de comunicación como lo es TEAMS y Skype for Business. Actualmente cada usuario se autentica por medio del active directory de Premier Soluciones (TPGNET).
VPN	En la oficina existe un único VPN que conecta a Costa Rica con Telefónica Miami, en caso de trabajo en casa se

	necesita un usuario de VPN personal para utilizar Cisco AnyConnect, en caso de trabajar en la infraestructura de algún cliente el VPN necesitara ser instalado en su máquina personal.

Tabla 3. Hardware y software área de soporte técnico

3.3.4 Área de recursos humanos

En Premier Soluciones el proceso de administración de personal es visto desde la sede en Miami; debido a que este proceso es uno de los críticos, se coloca dentro de los procesos a Disaster Recovery Plan. Entre las actividades que son gestionadas dentro del alcance, están las siguientes:

- Gestión de planillas a empleados.
- Gestión de bonos.
- Gestión de viáticos.
- Recepción de pagos.
- Gestión de vacaciones.

Recursos humanos, como las demás áreas, depende de ciertos elementos de hardware y software, para llevar a cabo su función. En la Tabla 4 se ven estos elementos.

Hardware	
Máquina Windows i5, 16 GB RAM, 1TB Disco Duro	Máquina de uso personal para el trabajo.
Internet	Todo el acceso a las aplicaciones es por medio de internet.
Software	
Servidor de JD Edwards EnterpriseOne	Ubicado en Telefónica data center en Miami.

Tabla 4. Hardware y software área recursos humanos

3.3.5 Área de administración de proyectos

Contempla el proceso en el que los administradores de proyectos se encargan de la gestión proyectos; cada proyecto puede ser visto de diferentes formas desde algo muy pequeño. Por ejemplo: una pequeña modificación dentro de alguno de los productos base o la creación de una nueva funcionalidad en los productos o bien un proyecto indefinido como la gestión de bugs dentro el producto base. Existen también proyectos grandes que pueden llevar el nombre de un cliente específico, que no solo incluyen áreas de desarrollo, sino también de consultoría o diseño. Conociendo el tipo de proyecto dentro de Premier Soluciones, su gestión es compleja, al tener que manejar tiempos, equipos de trabajo en muchos casos multidisciplinarios, la relación con los clientes, el análisis de procesos, la comunicación a los equipos de trabajo directamente, o líderes de área para su gestión y la gestión de los costos. Este proceso es vital para la continuidad del negocio de Premier Soluciones, por lo que será tomado en cuenta dentro de los procedimientos por crear para darle continuidad en caso de desastres.

Software	
Team Foundation servidor	Utilizado por Premier Soluciones como medio de gestión de proyectos de software. Actualmente cada usuario se autentica por medio del active directory de Premier Soluciones (TPGNET).
Microsoft Project	Herramienta utilizada para la gestión de los proyectos sean de software consultoría, entre otros.
@task	Software critico de gestión de proyectos en el cual el administrador del proyecto crear cada uno de los proyectos las

	tareas asociadas al mismo y las asigna a los recursos participantes, permite además la gestión de los tiempos, y la comunicación de estatus de tareas o casos. Cada miembro del proyecto va a reportar en este software el tiempo que estuvieron trabajando en cada uno de las tareas y el estatus de dicha tarea.

Tabla 5. Software área administración de proyectos

3.3.6 Área de consultoría en JD Edwards

El área de consultoría ha perdido terreno contra el desarrollo de software dentro de Premier Soluciones. Sin embargo, es un área importante encargada de dar consultoría a clientes en nuevas implementaciones de JD Edwards o sobre instalaciones ya realizadas, configuraciones de módulos, entre otras cosas. Según lo analizado, el área de consultoría tiene ciertas dependencias de hardware, software y comunicaciones.

Hardware	
Servidor de JD Edwards EnterpriseOne	Ubicado en Telefónica data center en Miami.
Servidor de bases de Datos Oracle	Ubicado en Telefónica data center en Miami.
Servidor de bases de datos IBM/400	Ubicado en Telefónica data center en Miami.
Servidor de bases de datos SQL Server	Ubicado en Telefónica data center en Miami.

Computadora laptop o desktop, con prestaciones básicas	Con esta computadora acceden máquinas virtuales localizadas en el data center en Miami.
Internet	
Máquinas virtuales de uso personal	Localizadas en el Data Center de Miami.
Software	
VPN	Para realizar sus pruebas trabajan conectados a un VPN que les permite la conectividad a los servicios necesarios localizados en Telefónica de Miami. Cuando trabajan con el cliente directamente el mismo va a proveer el VPN y las máquinas virtuales propias.
SQL Server Client, Oracle Client, iSeries client	Clientes gratuitos de conexión a base de datos.
Office 365(Word, Excel, Outlook, Power point, Teams, Skype for Business)	El equipo ofimático lo utiliza cada miembro de la organización, el correo de la compañía es manejado mediante Office 365, al igual que la aplicación de comunicación como lo es TEAMS y Skype For Business, Actualmente cada

	usuario se autentica por medio del active directory de Premier Soluciones (TPGNET).
JD Edwards EnterpriseOne	Es necesario para consultoría la utilización de ese software ya que es el core de la funcionalidad y permite mostrar datos y funcionalidad base..

Tabla 6. Hardware y software área consultoría JD Edwards

3.3.7 Procesos de comunicación

En el proceso de comunicación los miembros de la organización se comunican de forma interna o externa, con clientes proveedores, entre otros. La comunicación, dentro de cualquier organización, es importante y en Premier Soluciones no es la excepción; por ello, se categorizó como crítico y será tomado en cuenta dentro de los procedimientos que garanticen la resiliencia de este.

Software, Hardware	
Office 365: Microsoft Outlook, Microsoft Teams, Skype for Business	Actualmente cada usuario se autentica por medio del active directory de Premier Soluciones (TPGNET).
Red de Telefónica Avaya	Cada colaborador tiene su teléfono IP en la oficina para comunicación en caso de ser necesario.

Tabla 7. Hardware y software comunicaciones

3.3.8 Service Plus

Este es el procedimiento mediante el cual un cliente reporta un Ticket[1], y Premier Soluciones gestiona todo lo necesario para dar una solución al problema reportado por el cliente. El proceso de service plus se realiza por medio de *Salesforce,* en donde cada cliente, dependiendo de su contrato, recibe un usuario y contraseña del sistema, que permite al cliente hacer el reporte del caso sucedido. Este software se encuentra en línea en los servidores del proveedor. Una que vez que el cliente ingresa un caso, este es notificado a los correos del personal de service plus de Premier Soluciones, previamente configurados en el software. Dependiendo de los SLAs para el cliente, el caso será atendido en el tiempo prudente dentro de lo estipulado.

Premier Soluciones tiene un servidor intermedio dentro de Telefónica que por medio de una interfaz toma los datos del caso en Salesforce y crea las tareas en el software @task. Este es utilizado para la administración de los proyectos, una vez creada la tarea en @task; esta es asignada al recurso(s) para la resolución. Nótese en la Figura 10 el proceso descrito anteriormente.

Figura 10. Proceso de Service Plus

El hardware y software mínimo requerido por Service Plus para la continuidad del servicio, es el siguiente, encontrado en la Tabla 8.

Hardware

[1] Evento anómalo que sucede en uno de los servicios dados por Premier Soluciones.

Computadora laptop o desktop, con prestaciones básicas	Con esta computadora acceden máquinas virtuales localizadas en el data center en Miami.
Internet	
Máquinas virtuales de uso personal	Localizadas en el Data Center de Miami.
Software	
VPN	Para realizar sus pruebas trabajan conectados a un VPN que les permite la conectividad a los servicios necesarios localizados en Telefónica de Miami.
Office 365(Word, Excel, Outlook, Power point, Teams, Skype for Business)	El equipo ofimático lo utiliza cada miembro de la organización, el correo de la compañía es manejado mediante Office 365, al igual que la aplicación de comunicación como lo es TEAMS y Skype For Business, Actualmente cada usuario se autentica por medio del active directory de Premier Soluciones (TPGNET).

Tabla 8. Hardware y software service plus

Premier Soluciones, como cualquier empresa que presta servicios, maneja sus SLA, que son contratos para cada uno de sus clientes en los cuales determina el

nivel de servicio que el cliente quiere contratar. Puede ser para consultoría, acerca de las aplicaciones o sobre JD Edwards, dependiendo del servicio contratado por el cliente; así será el valor de este y los tiempos de respuesta del equipo de especialista de Premier Soluciones para la atención de casos.

3.3.9 Datos

Este activo es compartido por todas las áreas que comprende la organización. Como ya es conocido, la información es uno de los activos más importantes de la organización; es por ello por lo que es un proceso del cual se debe tomar precauciones en temas de continuidad y recuperación. Esta área se clasifica como un área común, debido a que los datos son manejados en todas las diferentes áreas, cada una según su rol de trabajo. Por ejemplo, el área de desarrollo se alimenta de las bases de datos provenientes de JD Edwards, para sus diferentes ambientes. Los ambientes utilizados en desarrollo de software son:

- Desarrollo.
- Pruebas.
- Producción.

El área de administración de proyectos utiliza la información ingresada en el software @task por cada uno de los miembros de los distintos proyectos, la información del Microsoft Project y la información del Team Foundation para hacer su gestión.

3.4 Estado de la cuestión

Esta investigación se orienta en la creación de los procedimientos para un futuro plan de recuperación de desastres para la empresa Premier Soluciones. Se elige esta orientación en particular, debido a que dicha empresa no cuenta con el plan que es muy importante en la actualidad si se quiere mantener como una empresa sólida y madura en su campo de aplicación.

El estado de la cuestión de esta investigación se basó en un sondeo realizado sobre Google Académico (scholar.google.com), en donde se aplicaron diversos criterios de búsqueda basados en continuidad del negocio, sobre artículos en inglés, debido a la existencia de más información valiosa en dicha lengua.

Los siguientes son los criterios buscados en dicha herramienta:

+ Disaster Recovery Plan.

En la siguiente imagen, la búsqueda arrojó 707000 resultados.

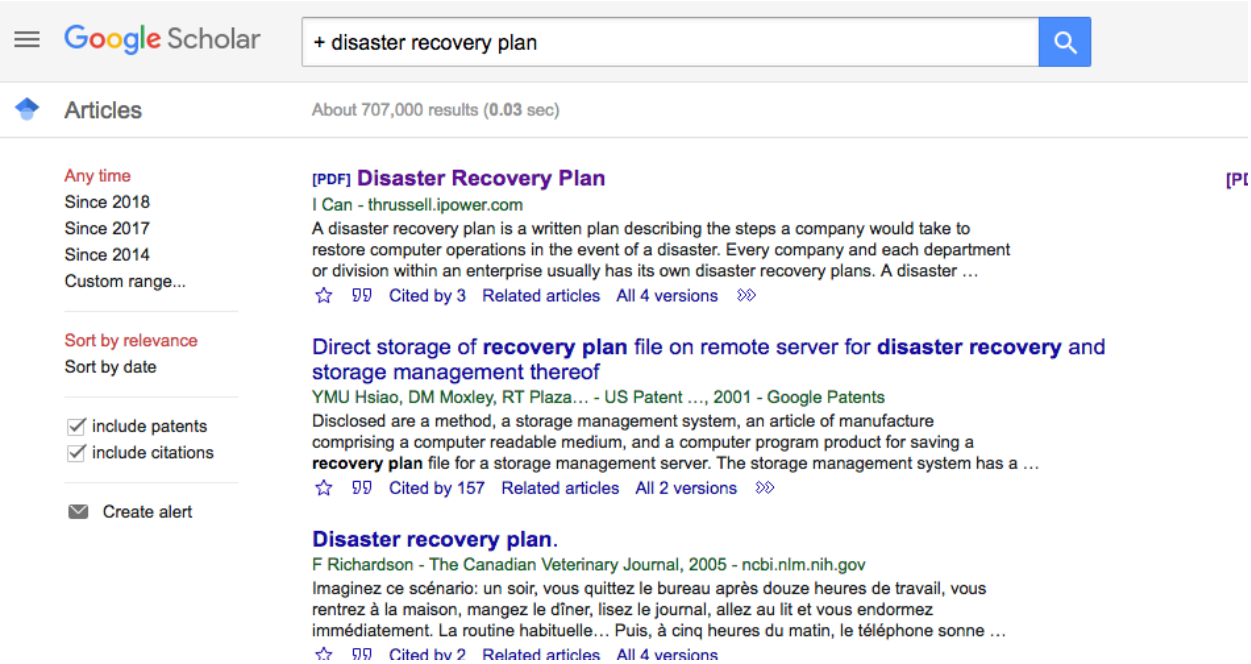


Figura 11. Scholar de Google

Existe mucha información sobre los DRP, pero cada uno es diferente para cada organización en que se implemente y esta no es la excepción. Premier Soluciones no cuenta con un plan de recuperación adecuado a sus procesos de negocio; esto deja la puerta abierta a su implementación, debido a que ningún DRP ha sido implementado sobre Premier Soluciones.

3.5 Políticas de ciberseguridad

Se realiza un análisis por áreas de las políticas existentes en Ciberseguridad, basado en (ISO 27001, 2014), como parte de la investigación y como insumo a la creación de los procedimientos para la confección del DRP y con el fin de tener un análisis de la situación actual de Premier Soluciones, en el campo de la Ciberseguridad,

Las Políticas de Ciberseguridad, en Premier Soluciones, son inexistentes en forma y papel, pero existe gran cantidad de procedimientos o acciones que se

ejecutan empíricamente que unidas pueden dar pie a la creación de una primera fase de políticas en ciberseguridad.

El siguiente análisis se basa sobre las áreas identificadas en (ISO 27001, 2014); a continuación, su enumeración:

- Políticas de seguridad de la información.
- Organización de la seguridad de la información.
- Seguridad ligada a los recursos humanos.
- Gestión de activos.
- Control de acceso.
- Criptografía.
- Seguridad física y ambiental.
- Seguridad de las operaciones.
- Seguridad de las comunicaciones.
- Adquisición, desarrollo y mantenimiento de sistemas.
- Relaciones con los proveedores.
- Gestión de incidentes de seguridad de la información.
- Aspectos de seguridad de la información en la gestión de la continuidad del negocio.
- Cumplimiento.

3.5.1 Políticas de seguridad de la información

3.5.1.1 Dirección de la gestión para la seguridad de la información

- No existe una política de ciberseguridad, debidamente documentada y aprobada por la gerencia.
- No hay encargados en ciberseguridad, por consiguiente, no hay roles y responsabilidades.

3.5.2 Organización de la seguridad de la información

3.5.2.1 Organización interna

- Roles y responsabilidades de seguridad de la información: no existen responsables, hay una persona encargada de muchas acciones que debieran ser segregadas.
- Segregación de funciones en seguridad de la información: no existe una segregación de funciones definida.
- Comunicaciones externas: no existen políticas, ni procedimientos definidos para las comunicaciones externas.
- Ciberseguridad en la gestión de proyectos: en los proyectos de software se intenta programar, basado en las mejores prácticas en ciberseguridad, pero temas como la disponibilidad pilar de la ciberseguridad quedan al descubierto por el tema de continuidad del negocio.

3.5.2.2 Dispositivos móviles y teletrabajo

- Política de dispositivo móvil: no existe una política definida en este tema, cualquier persona podría traer su dispositivo y solicitar la contraseña por medio de un correo o bien por medio de algún compañero; los controles para esto son inexistentes.
- Políticas de teletrabajo: las personas trabajan desde casa sin la existencia de controles para este tipo de actividad. A finales del año 2018, algunas personas toman iniciativa para dejar de utilizar TeamViewer y usar el Cisco AnyConnect VPN. Se creo una política interna de teletrabajo, sin embargo, no está firmada ni aprobada por la gerencia.

3.5.3 Seguridad ligada a los recursos humanos

3.5.3.1 Previo al empleo

- Investigación: no se realiza una investigación verificación de antecedentes, de acuerdo con las leyes y regulaciones actuales, a ninguno de los candidatos al puesto de trabajo.
- Términos y condiciones del empleo: se firma un contrato en el cual se habla de la relación del empleado y empleador con respecto al puesto de trabajo y

algunos temas de privacidad de la información muy superficiales. En este apartado existe por escrito un documento, pero no enfocado en seguridad de la información, por lo que podría mejorar en términos de ciberseguridad.

3.5.3.2 Durante el empleo

- Responsabilidades de la dirección: existen notificaciones verdales de crear desarrollos de manera segura y no divulgar información confidencial de clientes, el aspecto negativo es no contar con una política por escrito y no contar con procedimientos para su comprobación.
- Campañas de concientización en ciberseguridad: no se realizan campañas de concientización en ciberseguridad.
- Procesos disciplinarios: al no existir políticas definidas y aprobadas, no existen los procesos disciplinarios estipulados.

3.5.3.3 Finalización o cambio de empleo

Una vez que una persona es despedida o bien cambia de empleo, hay dos personas que se encargan de quitar los accesos físicos y virtuales, además de realizar la revisión de los activos que utilizaba la persona antes del último día de trabajo.

3.5.4 Gestión de activos

3.5.4.1 Responsabilidad por los activos

- Inventario de activos: existe una hoja de Excel en Google Drive “SmarterCommerce IT Equipment Workstations”, que cuenta con la descripción de los activos por persona. La hoja la actualiza cualquier persona con acceso y no se hace validación de autenticidad de la información, mediante ningún software.
- Uso aceptable de los activos: no existen políticas o reglas para el uso aceptable de la información o recursos de procesamiento.
- Devolución de activos: no existe ninguna regla o procedimiento estimulado ni comunicado de forma verbal.

3.5.4.2 Clasificación de la información

- La clasificación de la información: la información no es clasificada, el concepto no existe en la organización como tal, el manejo que se da en

cuanto a clasificación es dar a conocer la información a quien la necesite para su puesto de trabajo, pero procedimientos como tal no existen.

- Etiquetado de la información: no existe el etiquetado de la información.
- Manejo de activos en información: el manejo de activos, de acuerdo con un esquema de clasificación no existe.

3.5.4.3 Manejo de los medios

- Gestión de medios removibles: los medios removibles se encuentran en la organización sin el debido control; no existen procedimientos más allá que saber quién fue el último en utilizar el medio para conocer su localización.
- Eliminación de medios: no existen procedimientos para la destrucción segura de medios removibles.
- Traslado de medios físicos: no existen controles para el traslado de información en medios removibles que garanticen el acceso no autorizado a la información.

3.5.5 Control de acceso

3.5.5.1 Requisitos del negocio para el control de acceso

- Política de control de acceso: no existe una política de acceso a la información y a los recursos de procesamiento documentada y aprobada por la gerencia. Se intenta que cada persona tenga acceso a los recursos que necesita para su rol de trabajo, sin embargo, hay aspectos que no se controlan.
- Acceso a redes y servicios de red: en la organización solo hay dos redes, la que conecta a Costa Rica con Telefónica (data center), y una red con salida a internet solamente, a la que no todos los empleados tienen acceso; por ello, este control está bien aplicado, pero no documentado.

3.5.5.2 Gestión del acceso de usuarios

- Registro y cancelación de registro de usuarios: no existe un proceso formal, pero muchas veces el Program Manager es la persona encargada de conceder o revocar los accesos a las diferentes aplicaciones que los empleados necesitan.

- Gestión de derechos de acceso privilegiados: hay personas dentro de la organización que cuentan con todos los accesos sin ningún tipo de control o segregación.
- Revisión de los derechos de acceso de los usuarios: los propietarios de los activos rara vez realizan una revisión de los derechos de acceso, no existe un proceso formal para este caso.

3.5.5.3 Responsabilidades de los usuarios

No existen procedimientos o campañas de concientización para educar a los usuarios acerca de salvaguardar la información secreta de acceso, tanto interna como externa (activos en los clientes).

3.5.5.4 Control de acceso a sistemas y aplicaciones

- Restricción de acceso a la información: no existe una política de control de acceso documentado y aprobado; sin embargo, la mayoría de los sistemas cuentan con la restricción de acceso a usuarios que no lo necesitan, como parte de sus funciones.
- Procedimientos de accesos seguros: las aplicaciones que manejan información cuentan con procesos de autenticación, seguros.
- Sistema de gestión de contraseñas: existe una aplicación “Management Console” que es la encargada de aplicar el Password Policy, para los sistemas desarrollados por Premier Soluciones; sin embargo, software externo utilizado dentro, cuenta con sus propias políticas de contraseñas que no siempre son bien configuradas.
- Uso de programas utilitarios privilegiados: no existen programas con tal nivel de privilegio; sin embargo, uno de ellos podría ser una base de datos que con la modificación de alguno de sus datos permitirá la manipulación de la funcionalidad de la aplicación. Para el acceso a bases de datos, no existe una segregación de usuarios, todos los desarrolladores trabajan con un usuario genérico con privilegios de “arman”.
- Control de acceso al código fuente: el código fuente tiene su control de acceso por medio del active directory, se encuentra en TFS y cada persona tiene acceso a lo que necesita para trabajar en su puesto de trabajo. Sin

embargo, no existen controles que prevengan el descargar dicho código fuente, subirlo en alguna nube personal o bien copiarlo en un USB.

3.5.6 Criptografía

3.5.6.1 Controles de criptografía

- Política sobre el uso de controles criptográficos: existe una política documentada que surge como requisito de certificación para PCI Compliance DSS.
- Gestión de llaves: existe una política física y aprobada sobre el uso, protección y el tiempo de vida útil de las llaves criptográficas; en ellas se describe, entre otras cosas, cómo las aplicaciones cuentan con procedimientos para hacer cambio de estas llaves, basados en PCI Compliance DSS.

3.5.7 Seguridad física y ambiental

3.5.7.1 Áreas seguras

- Perímetro de la seguridad física: las áreas están debidamente separadas y los accesos físicos distribuidos a cada trabajador.
- Controles de entrada física: cada área tiene sus propios controles de acceso, algunas con doble factor de autenticación.
- Aseguramiento de oficinas, salas e instalaciones: existe seguridad física en cada una de las áreas.
- Protección contra amenazas externas y ambientales: equipos contra incendios y alarmas debidamente colocadas.
- Áreas de entrega y carga: solo existe un acceso; sin embargo, las áreas de donde reside el personal y centro de datos están aisladas de los visitantes, por medio de controles físicos y lógicos.

3.5.7.2 Equipo

Los equipos cuentan con buena ubicación, el cableado perfectamente bien ubicado, ups por cada equipo, los activos no se sacan de la oficina sin previa autorización.

Recomendación: asegurar los equipos por medio de la adquisición de un seguro, dar mantenimiento a los equipos, validación de los equipos para reutilizarlos en términos de privacidad de la información, equipo desatendido con seguridad, adoptar política de pantalla y escritorios limpios.

3.5.8 Seguridad de las operaciones

3.5.9 Procedimientos y responsabilidades operacionales

- **Gestión de cambios**: no existe gestión de cambios en los procesos del negocio, los procesos se cambian verbalmente, sin ningún documento que respalde tal decisión.
- **Separación de ambientes de desarrollo, pruebas y operación**: existe una separación bien definida de ambientes, para todo el ciclo de desarrollo.

3.5.9.1 Protección contra código malicioso

Este objetivo se cumple en un 40%. Premier Soluciones cuenta con protección del *endpoint* empresarial, en todas las máquinas de la compañía; sin embargo, no realiza campañas de concientización acerca de las amenazas de un programa maligno, ni tiene procedimientos de recuperación definidos en caso de un desastre provocado por este riesgo.

3.5.9.2 Respaldo

Los datos se encuentran en Telefónica y las copias de seguridad se realizan según lo estipulado en el contrato. Se cuenta con una red de almacenamiento SAN, aunque no existe una política interna escrita y aprobada; estas copias de seguridad son analizadas para detección de programa maligno.

3.5.9.3 Registro y seguimiento

Todas las aplicaciones cuentan con logs; sin embargo, los usuarios que se utilizan generalmente son genéricos, por lo que es difícil determinar quién realizó cada acción. No existe una persona encargada de revisar logs del sistema periódicamente, ni una política que lo requiera; técnicamente los relojes de todos los servidores están sincronizados.

3.5.9.4 Control de software operativo

No existen procedimientos, ni una política establecida que garanticen el control del software que se instala en cada una de las máquinas.

3.5.10 Gestión de vulnerabilidades técnicas

No existen procedimientos para la gestión de vulnerabilidades técnicas dentro de la infraestructura o software de Premier Soluciones, ni procedimientos o reglas sobre el software que se instala en cada una de las máquinas o servidores.

3.5.10.1 Consideraciones de auditoría en los sistemas de información

Todos los sistemas desarrollados en Premier Soluciones cuentan con módulos de auditoria. Sin embargo, por lo general estas opciones se encuentran apagadas y se encienden únicamente para intentar reproducir errores.

3.5.11 Seguridad de las comunicaciones

3.5.11.1 Gestión de seguridad de la red

En Premier soluciones hay una correcta segregación de las redes y cada usuario trabaja conectado a la red necesaria para su puesto de trabajo. Los servicios de red externos cuentan con niveles de servicio y la seguridad de estos es verificada.

3.5.11.2 Transferencia de información

La información es transferida por medio de Outlook y no se envía encriptada, solamente el canal que es https. La transferencia de información interna, por medio de dispositivos físicos, no tiene controles que garanticen la seguridad de la información incluida; se recomienda la creación de una política para la transferencia segura de información.

3.5.12 Adquisición, desarrollo y mantenimiento de sistemas

3.5.12.1 Requisitos de seguridad de los sistemas de información

Cada nuevo módulo que se crea o cada porción de código que se realiza, va de la mano con un análisis previo de seguridad, basado en las mejores prácticas para garantizar la seguridad de la información. Algunas de las prácticas realizadas, son el cifrado de datos, verificación de integridad de datos, denegación a servicios, entre otros.

3.5.12.2 Seguridad en los procesos de desarrollo y soporte

Premier soluciones cuenta con una guía de desarrollo de sistemas que se debe seguir para cualquier desarrollo. Los cambios al producto base son ampliamente documentados y controlados; sin embargo, mejoras a productos ya instalados en clientes, no son 100% documentados y se han encontrado inconsistencias entre los documentos de requerimientos del sistema. Cada cambio realizado al software es probado en términos de funcionalidad por el equipo de QA. Sin embargo, en términos de seguridad, hay una brecha amplia en el departamento, debido, en gran medida, a la carencia de procedimientos de pruebas en seguridad de los sistemas; las pruebas de aceptación son parte del ciclo de desarrollo del software.

Recomendaciones

- Crear una política de desarrollo seguro analizada y aprobada.
- Realizar entrenamientos o capacitación de pruebas de software, enfocado en seguridad.
- Capacitar al equipo de desarrollo en programación segura.
- Documentar un procedimiento dentro de la política de ciberseguridad, sobre el manejo de cambios en el software para clientes.
- Realizar análisis de vulnerabilidades en los ambientes de desarrollo, con el fin de garantizar que son seguros.

3.5.12.3 Pruebas de datos

Los datos en los ambientes de QA o pruebas, cuentan con su acceso limitado y su plan de respaldo; son cambiados solo para realizar pruebas específicas.

3.5.13 Gestión de incidentes de seguridad de la información

En Premier Soluciones no existen procedimientos documentados acerca del tratamiento que debería darse a un incidente de seguridad de la información. Sin embargo, cada incidente de seguridad encontrado es comunicado al Program Manager, quien intenta ubicar la persona más idónea para darle una gestión apropiada pero improvisada. De los incidentes que se reportan, ninguno se analiza para clasificado, tampoco es documentado, queda del conocimiento de los involucrados por medio de correos electrónicos solamente. No existe un proceso que involucre a toda la

organización a reportar posibles incidentes de seguridad de la información, en alguna área extra al producto en desarrollo.

Se recomienda la creación de un plan de gestión de incidentes dentro de Premier Soluciones que establezca responsabilidades y procedimientos para una respuesta rápida, efectiva y ordenada a incidentes de seguridad de la información, así como involucrar más a cada trabajador para que puedan identificar y conozcan el procedimiento de cómo reportar un posible incidente de seguridad de la información.

3.5.14 Aspectos de seguridad de la información en la gestión de la continuidad del negocio

En premier Soluciones no existen procesos, procedimientos, ni controles establecidos, ni documentados, que garanticen el nivel necesario de continuidad para la seguridad de la información, durante una situación adversa. Como recomendación, primero se debe crear un plan de continuidad del negocio y en su desarrollo los procedimientos para la continuidad de la seguridad de la información, en cada proceso.

3.5.15 Cumplimiento

3.5.15.1 Cumplimiento de los requisitos legales y contractuales

Premier Soluciones, en términos de tratamiento de datos, no se rige por ninguna regulación, en términos legales se encuentra muy desprotegida en esta área. En el caso de propiedad intelectual siempre trata de estar en orden con todas las regulaciones, desde un libro electrónico hasta el software utilizado para la creación de sus productos o utilizado dentro de sus productos. Por otro lado, en términos contractuales, se rige por el código de trabajo de Costa Rica por lo que cuenta con todos los requisitos legales.

3.5.15.2 Revisión de seguridad de la información

En este apartado, Premier Soluciones está lejos del objetivo, ya que no cuenta con políticas y procedimientos de seguridad de la información; por ello, las revisiones en este apartado no se dan. Se recomienda comenzar con la creación de una primera versión de las políticas de ciberseguridad.

CAPÍTULO IV

4 Elaboración del BIA

4.1 Introducción

El análisis de impacto en el negocio es un insumo en el desarrollo del Plan de Recuperación de Desastres (DRP). El BIA permite identificar los recursos y procesos críticos para determinar el impacto operacional y financiero, conocer el tiempo de interrupción y prioridades de recuperación en el negocio; en otras palabras, identifica las actividades de Premier Soluciones, que son claves para su supervivencia.

El propósito del Análisis de Impacto en el Negocio (BIA), es relacionar los recursos específicos con los procesos críticos de los sistemas. Con base en esta información, se determinan las consecuencias que se presentan, en caso de producirse una interrupción en los recursos del Área IT, producido, ya sea por el hombre o por desastres naturales. Los resultados del BIA deben incorporarse apropiadamente en el desarrollo de estrategias de recuperación que forman parte del Plan de Recuperación de Desastres (DPR).

4.2 Objetivo

El BIA se constituye en el pilar sobre el que se va a construir el Plan de Recuperación de Desastres; es la guía que determina qué necesita ser recuperado y el tiempo requerido para recuperación.

4.3 Beneficios

- Será utilizado como una de las fases iniciales para el desarrollo del DRP para Premier Soluciones.
- Identificar los recursos más importantes de una organización y el impacto que podría representar en caso de algún incidente o interrupción mayor.
- Contribuye a mejorar el entendimiento sobre las afectaciones a la organización y cómo responder a estas.
- Proporciona los datos necesarios para presentar a la gerencia y poder justificar el presupuesto destinado a la recuperación de desastres.

4.4 Fases

Basado en (ISO 22301, 2012), los elementos que van a componer este Análisis de Impacto de Negocio (BIA), se encuentran en la Figura 12.

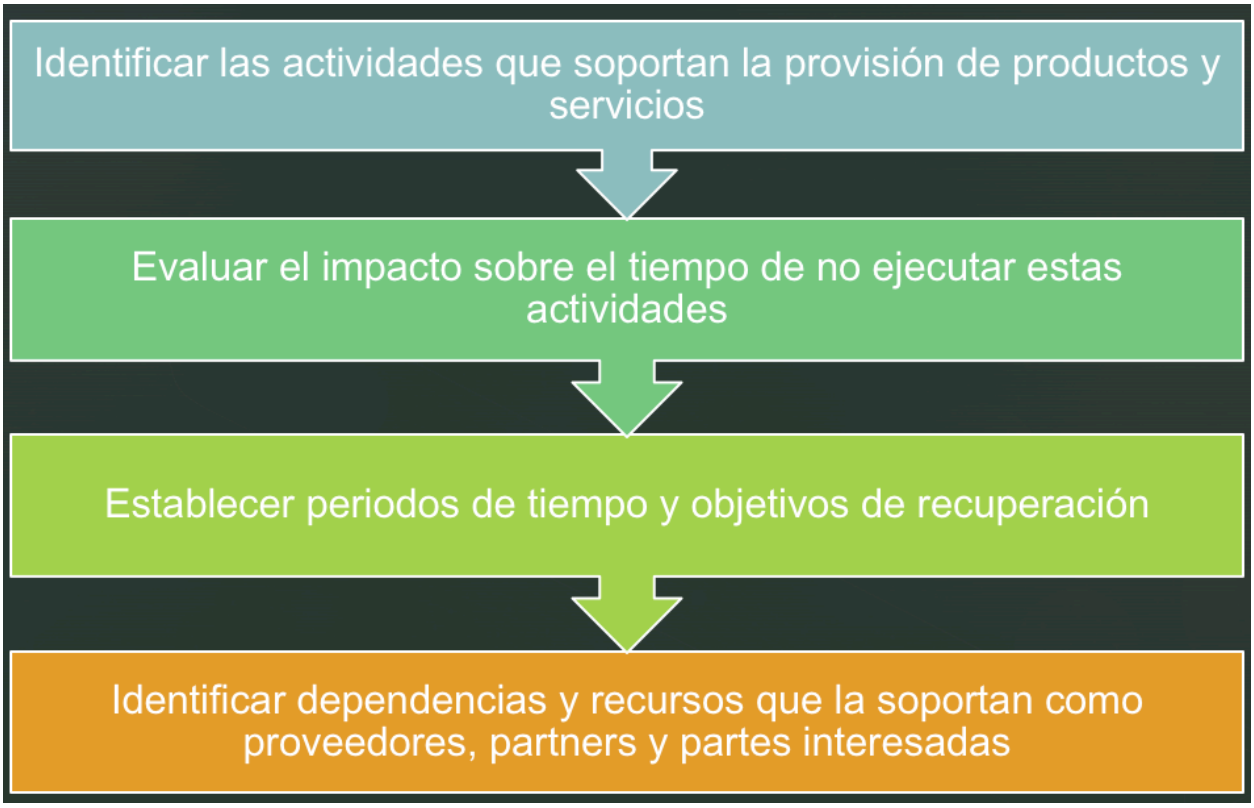


Figura 12. Elementos del BIA

4.5 Metodología

Todos los procedimientos de las áreas identificadas en Premier Soluciones, así como los recursos tecnológicos en los que se soportan tales actividades, deben ser clasificados de acuerdo con su prioridad de recuperación. Para ello se mide el tiempo que puede dejar de realizar tal actividad, sin que ello cause pérdidas financieras, daño de imagen, y/o penalizaciones legales o contractuales. En caso de continuidad todo gira alrededor del impacto, buscando sostener las operaciones críticas de la compañía. El modelo está basado en el conocimiento adquirido en cursos de la maestría en Ciberseguridad de la Universidad Cenfotec y en el documento publicado (MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, 2012), pero principalmente, en (ISO 22301, 2012).

4.6 Parámetros de análisis y evaluación

Impactos. Basado en los campos de interés de la compañía, se identificaron dos áreas de impacto sobre las cuales se basa este análisis: el impacto financiero y el impacto operacional; este último, divido en: impacto a la marca e impacto legal y regulatorio. A continuación, el detalle de cada una:

- **Impacto financiero**: incluye pérdida de ingresos, pérdida de ingresos por ventas no realizadas, penalizaciones por no cumplir compromisos contractuales o niveles de servicio y oportunidades, pérdidas durante la disrupción del proceso.
- **Impacto legal y regulatorio**: representa todas aquellas acciones acordes con el cumplimiento de la ley, obligaciones estatutarias, reglamentarias, contractuales o cualquier requisito legal. Incluye pérdidas por no presentar reportes financieros o de impuestos en las fechas indicadas, demandas o penalizaciones por incumplir requerimientos obligatorios en las actividades lucrativas de Premier Soluciones.
- **Impacto a la marca**: incluye la pérdida de confianza por parte de los clientes y del mercado, reclamaciones de responsabilidad, clientes insatisfechos por el servicio, apariciones en las noticias por quejas de los clientes, pérdida de reputación y pérdidas de ventajas competitivas.

Para analizar de una forma cuantitativa o cualitativa, se deben definir valores, para Premier Soluciones y, después de una reunión con las personas involucradas en proyectos, se define que el impacto tendrá una escala comprendida en el rango de (1) a (5), en la Tabla 9 se especifican los valores y su descripción.

Valor	Calificación	Descripción
1	Insignificante	Si el proceso sufre algún tipo de disrupción, esto no genera mayor impacto en la continuidad de la empresa.
2	Bajo	Si el proceso sufre algún tipo de disrupción, tiene algún impacto en la organización, el cual no sería significativo y no impactaría la rentabilidad de la empresa.

3	Medio	Si el proceso sufre algún tipo de disrupción, tiene un impacto moderado en los ingresos, podría afectar de forma moderada la rentabilidad generada por clientes, podría impactar su imagen y/o podría tener problemas legales.
4	Significativo	Si el proceso sufre algún tipo de disrupción, tiene un impacto significativo, y afecta la rentabilidad de la empresa, pero no la sostenibilidad del negocio además impactaría su imagen y/o podría tener problemas legales serios.
5	Critico	Si el proceso sufre algún tipo de disrupción, tiene un impacto severo generado por pérdidas financieras que afectan la rentabilidad e ingresos de la compañía y su continuidad en el mercado.

Tabla 9. Definición de valores de impacto

Seguidamente se definen los tiempos contra los cuales se va a evaluar el impacto expresado en horas categorizado en seis tractos analizados previamente en una reunión con algunos miembros de Premier Soluciones. Este tiempo significa la cantidad de horas que el proceso o servicio se encuentra fuera de producción y nos permitirá evaluar el impacto contra el tiempo de ausencia.

- 4 horas
- 4 a 8 horas
- 8 a 24 horas
- 24 a 48 horas
- 48 a 72 horas
- > 72 horas

4.7 Identificar las actividades que soportan la provisión de productos y servicios

En el capítulo anterior y, gracias a los colaboradores de Premier Soluciones, se lograron identificar y limitar previamente las áreas de alcance para la investigación. En la Figura 7, se encuentran las áreas dentro de Premier Soluciones, que serán tomadas en cuenta para la realización, no solo del DRP, sino también de este BIA; dichas áreas son las expuestas en la Figura 13.

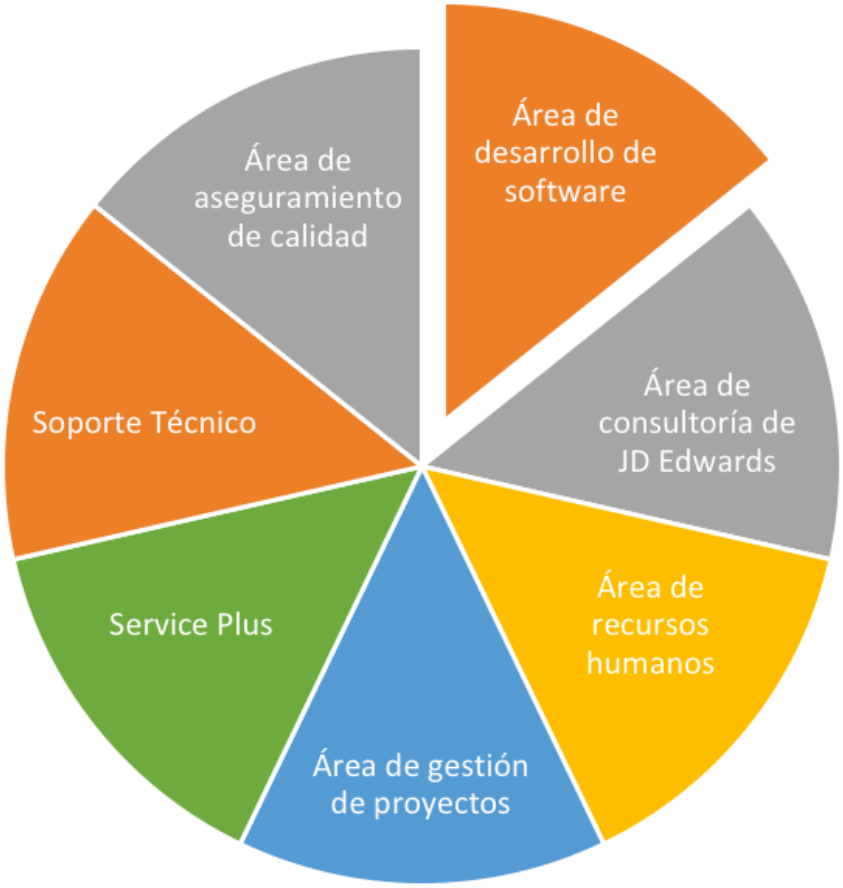


Figura 13. Áreas Premier Soluciones

Dentro de cada una de estas áreas existen procesos o servicios que se deben identificar para su posterior evaluación. En la Tabla 10, se encuentran los procesos identificados para cada una de las áreas; estos procesos o servicios serán filtrados posteriormente para identificar los de mayor criticidad y analizar su impacto en la organización, en caso de que este fuera de servicio.

Código	Procesos críticos
	Área de desarrollo de sistemas
1	Proceso de desarrollo de Software .net.
2	Proceso de desarrollo de Software en JD Edwards EnterpriseOne.
3	Pruebas del software desarrollado.
4	Análisis de requerimientos sobre mejoras en el software.
5	Solicitar aprobación para cambio de software (mejoras, nuevos módulos).
6	Enviar paquetes de actualización de software a clientes.
7	Reporte de problemas en software base.

8	Ingreso de tiempo laborado en @task.
9	Comunicación con el área de gestión de proyectos, miembros de proyectos (desarrolladores, consultores).
10	Análisis de adquisición de nuevo software para uso en las aplicaciones.
11	Procesos de revisión de código.
	Área consultoría JD Edwards EnterpriseOne
12	Análisis de requerimientos sobre cambios o mejoras sobre objetos de JD Edwards EnterpriseOne.
13	Solicitar aprobación de cambios en objetos de JD Edwards EnterpriseOne.
14	Publicar paquetes de JD Edwards EnterpriseOne para el producto base.
15	Comunicación con el Cliente-Consultoría.
	Área de recursos humanos
16	Gestión de planillas (pagos).
17	Gestión de viáticos.
18	Recepción de pagos.
19	Gestión de vacaciones.
20	Pagos a proveedores.
	Área de gestión de proyectos
21	Asignar personal al proyecto.
22	Recepción y atención de casos Service Plus - Gestión de Proyectos.
23	Recepción de nuevos requerimientos (mejoras, nuevas características).
24	Comunicación con la alta gerencia (llamadas, correos, estatus de proyectos).
	Service Plus
25	Recepción y atención de casos cliente-service plus.
26	Seguimiento a casos (comunicación, llamadas, correo).
27	Comunicación service plus-cliente.
	Soporte Técnico
28	Instalación de productos SmarterCommerce en el cliente.
29	Instalación de paquetes de actualización en los clientes.

30	Instalación de nuevas versiones de los productos SmarterCommerce en ambientes de desarrollo y pruebas.
31	Gestión de las telecomunicaciones.
32	Atención de incidentes internos.
33	Instalación y configuración de software en máquinas personales y servidores.
34	Instalación de parches en máquinas personales y servidores.
35	Mantenimiento de la central Telefónica.
36	Gestión del Active Directory.
	Área de aseguramiento de calidad
37	Pruebas sobre desarrollos en producto base.
38	Pruebas sobre desarrollos de mejoras y problemas para el cliente.
39	Pruebas sobre trabajos de consultoría.
40	Comunicación constante entre QA - Gestión de Proyectos.

Tabla 10. Procesos críticos de Premier Soluciones

4.8 Evaluar el impacto sobre el tiempo de no ejecutar estas actividades

Después de identificar los procesos críticos dentro de cada una de las áreas dentro de Premier Soluciones, se procede a evaluar el impacto en dichos procesos. En esta sección se muestra el impacto que tendría cada una de las actividades en caso de una disrupción con el paso del tiempo. Comienza desde las 4 horas y hasta más de 72 horas, analizados desde el punto de vista del impacto financiero, impacto a la marca e impacto legal y regulatorio. Las siguientes tablas no contienen todas las actividades definidas en la Tabla 10. Procesos críticos de Premier Soluciones, debido a que la estrategia es filtrar los procesos y servicios, de acuerdo con su criticidad. Después de realizada una reunión con personal de Premier Soluciones, se descartaron varios de ellos, fácilmente identificables, debido a que su código es consecutivo.

4.8.1.1 Calificación impacto financiero

		Horas					
Código	**Procesos críticos**	**4**	**4 a 8**	**8 a 24**	**24 a 48**	**48 a 72**	**>72**
	Área de desarrollo de sistemas						
1	Proceso de desarrollo de Software .net.	2	3	3	3	4	4
2	Proceso de desarrollo de Software en JD Edwards EnterpriseOne.	2	2	3	3	3	3
3	Pruebas del software desarrollado.	2	2	2	2	2	3
6	Enviar paquetes de actualización de software a clientes.	2	2	3	3	3	3
8	Ingreso de tiempo laborado en @task.	1	1	1	1	1	2
9	Comunicación con el área de gestión de proyectos, miembros de proyectos (desarrolladores, consultores).	2	2	3	3	4	4
11	Procesos de revisión de código.	2	2	2	2	2	3
	Área consultoría JD Edwards EnterpriseOne						
12	Análisis de requerimientos sobre cambios o mejoras sobre objetos de JD Edwards EnterpriseOne.	1	1	1	1	1	2
13	Solicitar aprobación de cambios en objetos de JD Edwards EnterpriseOne.	1	1	1	1	1	2
14	Publicar paquetes de JD Edwards EnterpriseOne para el producto base.	2	2	2	2	3	3
15	Comunicación con el Cliente-Consultoría.	2	2	3	3	3	4
	Área de recursos humanos						
16	Gestión de planillas (pagos).	1	1	2	3	3	3
17	Gestión de viáticos.	1	1	2	2	3	3

18	Recepción de pagos.	1	1	2	2	2	2
20	Pagos a proveedores.	1	1	1	1	2	2
	Área de gestión de proyectos						
21	Asignar personal al proyecto.	1	2	3	3	4	4
22	Recepción y atención de casos Service Plus - Gestión de Proyectos.	1	2	3	3	4	4
23	Recepción de nuevos requerimientos (mejoras, nuevas características).	1	2	2	2	2	2
24	Comunicación con la alta gerencia (llamadas, correos, estatus de proyectos).	1	2	2	2	3	3
	Service Plus						
25	Recepción y atención de casos cliente-service plus.	2	2	3	3	4	4
26	Seguimiento a casos (comunicación, llamadas, correo).	1	2	2	2	3	4
27	Comunicación service plus-cliente.	1	1	3	3	3	4
	Soporte Técnico						
28	Instalación de productos SmarterCommerce en el cliente.	1	1	1	2	3	4
29	Instalación de paquetes de actualización en los clientes.	2	2	3	3	3	4
30	Instalación de nuevas versiones de los productos SmarterCommerce en ambientes de desarrollo y pruebas.	1	1	1	1	1	2
31	Gestión de las telecomunicaciones	2	3	3	4	4	**5**
32	Atención de incidentes internos.	2	3	3	3	4	4
34	Instalación de parches en máquinas personales y servidores	1	1	1	3	3	4
36	Gestión del Active Directory.	1	2	3	3	3	3
	Área de aseguramiento de calidad						

38	Pruebas sobre desarrollos de mejoras y problemas para el cliente.	2	2	2	3	3	4
39	Pruebas sobre trabajos de consultoría en el cliente.	2	2	2	2	3	4
40	Comunicación constante entre QA - Gestión de Proyectos.	2	2	3	3	3	3

Tabla 11. Impacto Financiero

En la Tabla 11. Impacto Financiero, se observa que las actividades más críticas en el rango definido de 1 a 5, son aquellas que involucran directamente procesos de la relación con el cliente. Estos son los procesos con mayor impacto en menos horas y deberán tener mayor precedencia a la hora de definir el MTD en estas actividades. Actividades del core de la compañía y actividades internas, tienen un alto impacto financiero en un mayor tiempo, por lo tanto, deben ser tomadas en cuanta con su respectiva precedencia a la hora de definir los tiempos de recuperación.

Según el análisis anterior, las siguientes actividades son las de mayor impacto en un menor tiempo de horas fuera de servicio:

- 1 - Proceso de desarrollo de Software .net.
- 2 - Proceso de desarrollo de Software en JD Edwards EnterpriseOne.
- 6 - Enviar paquetes de actualización de software a clientes.
- 9 - Comunicación con el área de gestión de proyectos, miembros de proyectos (desarrolladores, consultores).
- 15 - Comunicación con el Cliente-Consultoría.
- 21 - Asignar personal al proyecto.
- 22 - Recepción y atención de casos Service Plus - Gestión de Proyectos.
- 25 - Recepción y atención de casos cliente-service plus.
- 27 - Comunicación service plus-cliente.
- 31 - Gestión de las telecomunicaciones.
- 32 - Atención de incidentes internos.

- 36 - Gestión del Active Directory.
- 40 - Comunicación constante entre QA - Gestión de Proyectos.

4.8.1.1 Calificación impacto legal y regulatorio

En la Tabla 12 se analiza el impacto legal y regulatorio de los procesos o servicios de Premier Soluciones, a través de las horas que se encuentren fuera de servicio.

		Horas					
Código	**Procesos críticos**	**4**	**4 a 8**	**8 a 24**	**24 a 48**	**48 a 72**	**>72**
	Área de desarrollo de sistemas						
1	Proceso de desarrollo de Software .net.	1	2	3	3	3	4
2	Proceso de desarrollo de Software en JD Edwards EnterpriseOne.	1	2	3	3	3	4
3	Pruebas del software desarrollado.	1	1	2	2	2	3
6	Enviar paquetes de actualización de software a clientes.	2	3	4	4	4	4
8	Ingreso de tiempo laborado en @task.	1	1	1	1	1	1
9	Comunicación con el área de gestión de proyectos, miembros de proyectos (desarrolladores, consultores).	1	2	3	3	3	4
11	Procesos de revisión de código.	1	1	1	2	2	2
	Área consultoría JD Edwards EnterpriseOne						
12	Análisis de requerimientos sobre cambios o mejoras sobre objetos de JD Edwards EnterpriseOne.	1	2	2	2	3	3
13	Solicitar aprobación de cambios en objetos de JD Edwards EnterpriseOne.	1	2	2	2	3	3

14	Publicar paquetes de JD Edwards EnterpriseOne para el producto base.	1	1	1	1	2	2
15	Comunicación con el Cliente-Consultoría.	1	1	3	3	4	4
	Área de recursos humanos						
16	Gestión de planillas (pagos).	2	2	2	3	4	4
17	Gestión de viáticos.	2	2	2	2	3	3
18	Recepción de pagos.	2	2	2	2	2	2
20	Pagos a proveedores.	2	2	2	2	2	3
	Área de gestión de proyectos						
21	Asignar personal al proyecto.	1	2	3	3	3	4
22	Recepción y atención de casos Service Plus - Gestión de Proyectos.	2	2	3	3	4	**5**
23	Recepción de nuevos requerimientos (mejoras, nuevas características).	1	1	2	2	2	3
24	Comunicación con la alta gerencia (llamadas, correos, estatus de proyectos).	1	2	2	2	3	3
	Service Plus						
25	Recepción y atención de casos cliente-service plus.	2	3	3	3	4	**5**
26	Seguimiento a casos (comunicación, llamadas, correo).	1	2	2	3	3	4
27	Comunicación service plus-cliente.	1	2	2	2	3	4
	Soporte Técnico						
28	Instalación de productos SmarterCommerce en el cliente.	1	1	2	3	3	4
29	Instalación de paquetes de actualización en los clientes.	2	2	3	3	3	4

30	Instalación de nuevas versiones de los productos SmarterCommerce en ambientes de desarrollo y pruebas.	1	1	1	1	2	2
31	Gestión de las telecomunicaciones.	2	3	3	3	4	**5**
32	Atención de incidentes internos.	2	3	3	3	3	4
34	Instalación de parches en máquinas personales y servidores.	1	1	2	3	3	4
36	Gestión del Active Directory.	1	2	2	2	2	2
	Área de aseguramiento de calidad						
38	Pruebas sobre desarrollos de mejoras y problemas para el cliente.	2	2	3	3	4	4
39	Pruebas sobre trabajos de consultoría	2	2	2	3	4	4
40	Comunicación constante entre QA - Gestión de Proyectos.	2	2	3	3	3	3

Tabla 12. Impacto Legal y regulatorio

En la Tabla 12, se puede observar que las actividades más críticas en el rango definido anteriormente de 1 a 5, son aquellas que involucran directamente procesos de la relación con el cliente y los procesos del Core de la compañía.

Según el análisis anterior, las siguientes actividades son las de mayor impacto en un menor tiempo:

- 1. Proceso de desarrollo de Software .net.
- 2. Proceso de desarrollo de Software en JD Edwards EnterpriseOne.
- 6. Enviar paquetes de actualización de software a clientes.
- 16. Gestión de planillas (pagos).
- 22. Recepción y atención de casos por parte de Service Plus.
- 25. Recepción y atención de casos.
- 26. Seguimiento a casos (comunicación, llamadas, correo).
- 27. Comunicación con el cliente.

- 28. Instalación de productos SmarterCommerce en el cliente.
- 29. Instalación de paquetes de actualización en los clientes.
- 32. Atención de incidentes internos.
- 34. Instalación de parches en máquinas personales y servidores.
- 38. Pruebas sobre desarrollos de mejoras y problemas para el cliente.
- 39. Pruebas sobre trabajos de consultoría.

4.8.1.1 Calificación impacto a la marca

En la Tabla 13 se analiza el impacto a la marca de los procesos o servicios de Premier Soluciones, a través de las horas que se encuentren fuera de servicio.

		Horas					
Código	**Procesos críticos**	**4**	**4 a 8**	**8 a 24**	**24 a 48**	**48 a 72**	**>72**
	Área de desarrollo de sistemas						
1	Proceso de desarrollo de Software .net.	2	2	3	4	4	4
2	Proceso de desarrollo de Software en JD Edwards EnterpriseOne.	1	2	3	4	3	4
3	Pruebas del software desarrollado.	1	1	2	2	3	4
6	Enviar paquetes de actualización de software a clientes.	1	2	3	3	4	**5**
8	Ingreso de tiempo laborado en @task.	1	1	1	1	1	1
9	Comunicación con el área de gestión de proyectos, miembros de proyectos (desarrolladores, consultores).	1	2	3	3	3	4
11	Procesos de revisión de código.	1	1	1	2	2	3
	Área consultoría JD Edwards EnterpriseOne						

12	Análisis de requerimientos sobre cambios o mejoras sobre objetos de JD Edwards EnterpriseOne.	1	2	2	2	2	3
13	Solicitar aprobación de cambios en objetos de JD Edwards EnterpriseOne.	1	2	2	2	2	3
14	Publicar paquetes de JD Edwards EnterpriseOne para el producto base.	1	1	1	1	2	2
15	Comunicación con el Cliente-Consultoría.	1	1	3	4	4	4
	Área de recursos humanos						
16	Gestión de planillas (pagos).	1	1	2	3	3	3
17	Gestión de viáticos.	1	1	2	2	3	3
18	Recepción de pagos.	1	1	2	2	2	2
20	Pagos a proveedores.	1	1	2	2	2	3
	Área de gestión de proyectos						
21	Asignar personal al proyecto.	1	2	3	3	3	4
22	Recepción y atención de casos Service Plus - Gestión de Proyectos.	1	2	3	3	4	4
23	Recepción de nuevos requerimientos (mejoras, nuevas características).	1	1	2	2	2	3
24	Comunicación con la alta gerencia (llamadas, correos, estatus de proyectos)	2	2	2	2	3	4
	Service Plus						
25	Recepción y atención de casos cliente-service plus.	2	2	3	3	4	**5**
26	Seguimiento a casos (comunicación, llamadas, correo).	1	2	2	2	3	4
27	Comunicación service plus-cliente.	1	2	4	4	4	4

	Soporte técnico						
28	Instalación de productos SmarterCommerce en el cliente.	1	1	2	3	3	3
29	Instalación de paquetes de actualización en los clientes.	2	2	3	3	3	3
30	Instalación de nuevas versiones de los productos SmarterCommerce en ambientes de desarrollo y pruebas.	1	1	1	1	2	2
31	Gestión de las telecomunicaciones.	2	3	3	3	4	**5**
32	Atención de incidentes internos.	2	3	3	3	3	4
34	Instalación de parches en máquinas personales y servidores.	1	1	2	3	3	4
36	Gestión del Active Directory.	1	3	4	4	4	4
	Área de aseguramiento de calidad						
38	Pruebas sobre desarrollos de mejoras y problemas para el cliente.	2	2	3	3	4	4
39	Pruebas sobre trabajos de consultoría.	2	2	3	3	4	4
40	Comunicación constante entre QA - Gestión de Proyectos.	2	2	3	3	3	3

Tabla 13. Impacto a la marca

En la Tabla 13, se observa que las actividades más críticas en el rango definido de 1 a 5, son aquellas que involucran directamente los procesos del Core de la compañía, procesos de la relación con el cliente y algunos procesos técnicos internos.

Según el análisis anterior, las siguientes actividades son las de mayor impacto:

- 1. Proceso de desarrollo de Software .net.
- 2. Proceso de desarrollo de Software en JD Edwards EnterpriseOne.
- 3. Pruebas del software desarrollado.
- 6. Enviar paquetes de actualización de software a clientes.

- 22. Recepción y atención de casos por parte de Service Plus.
- 25. Recepción y atención de casos.
- 26. Seguimiento a casos (comunicación, llamadas, correo).
- 31. Gestión de las telecomunicaciones.
- 32. Atención de incidentes internos.
- 34. Instalación de parches en máquinas personales y servidores.
- 38. Pruebas sobre desarrollos de mejoras y problemas para el cliente.
- 39. Pruebas sobre trabajos de consultoría.

4.9 Periodos de tiempo y objetivos de recuperación

Basado en el impacto financiero y el impacto operativo (imagen, legal y regulatorio) analizados anteriormente, se definen los tiempos de recuperación para cada uno de los procesos ordenados por prioridad. En la Tabla 14, se ve el promedio del impacto de cada uno de los procesos, desde el punto de vista financiero, de imagen y legal. Estos valores se obtuvieron sumando cada valor del impacto y su resultado se dividió entre el número de factores. Por medio del mapa de calor, se identifican fácilmente cuáles son los procesos más críticos basados en el promedio de los impactos antes analizados y ordenados por los impactos más altos en los tiempos más bajos, con el fin de priorizarlos.

		Horas					
Código	**Procesos críticos**	**4**	**4 a 8**	**8 a 24**	**24 a 48**	**48 a 72**	**>72**
31	Gestión de las telecomunicaciones.	2	3	3	3.33	4	**5**
32	Atención de incidentes internos.	2	3	3	3	3.33	4
6	Enviar paquetes de actualización de software a clientes.	1.66	2.33	3.33	3.33	3.66	4
1	Proceso de desarrollo de Software .net.	1.66	2.33	3	3.33	3.66	4
25	Recepción y atención de casos cliente-service plus.	2	2.33	3	3	4	4.67

36	Gestión del Active Directory.	1	2.33	3	3	3	3
2	Proceso de desarrollo de Software en JD Edwards EnterpriseOne.	1.33	2	3	3.33	3	3.67
22	Recepción y atención de casos Service Plus - Gestión de Proyectos.	1.33	2	3	3	4	4.33
21	Asignar personal al proyecto.	1	2	3	3	3.33	4
9	Comunicación con el área de gestión de proyectos, miembros de proyectos (desarrolladores, consultores).	1.33	2	3	3	3.33	4
29	Instalación de paquetes de actualización en los clientes.	2	2	3	3	3	3.67
40	Comunicación constante entre QA - Gestión de Proyectos.	2	2	3	3	3	3
38	Pruebas sobre desarrollos de mejoras y problemas para el cliente.	2	2	2.66	3	3.66	4
39	Pruebas sobre trabajos de consultoría en el cliente.	2	2	2.33	2.66	3.66	4
26	Seguimiento a casos (comunicación, llamadas, correo).	1	2	2	2.33	3	4
24	Comunicación con la alta gerencia (llamadas, correos, estatus de proyectos).	1.33	2	2	2	3	3.33
27	Comunicación service plus-cliente.	1	1.66	3	3	3.33	4
12	Análisis de requerimientos sobre cambios o mejoras sobre objetos de JD Edwards EnterpriseOne.	1	1.66	1.66	1.66	2	2.67
13	Solicitar aprobación de cambios en objetos de JD Edwards EnterpriseOne.	1	1.66	1.66	1.66	2	2.67
15	Comunicación con el Cliente-Consultoría.	1.33	1.33	3	3.33	3.66	4
16	Gestión de planillas (pagos).	1.33	1.33	2	3	3.33	3.33
17	Gestión de viáticos.	1.33	1.33	2	2	3	3
3	Pruebas del software desarrollado.	1.33	1.33	2	2	2.33	3.33
18	Recepción de pagos.	1.33	1.33	2	2	2	2
23	Recepción de nuevos requerimientos (mejoras, nuevas características).	1	1.33	2	2	2	2.67
20	Pagos a proveedores.	1.33	1.33	1.66	1.66	2	2.67
11	Procesos de revisión de código.	1.33	1.33	1.33	2	2	2.67

14	Publicar paquetes de JD Edwards EnterpriseOne para el producto base.	1.33	1.33	1.33	1.33	2.33	2.33
34	Instalación de parches en máquinas personales y servidores.	1	1	1.66	3	3	4
28	Instalación de productos SmarterCommerce en el cliente.	1	1	1.66	2.66	3	3.67
30	Instalación de nuevas versiones de los productos SmarterCommerce en ambientes de desarrollo y pruebas.	1	1	1	1	1.66	2
8	Ingreso de tiempo laborado en @task.	1	1	1	1	1	1.33

Tabla 14. Promedio de Impacto

4.9.1 Determinar el MTD de los procesos

Una vez identificados los procesos críticos del negocio, por medio del mapa de calor en la Tabla 14, se procede a identificar el MTD, que corresponde al tiempo máximo de inactividad de un proceso o servicio que puede tolerar una organización antes de colapsar y se hace la clasificación a fin de priorizar la recuperación del proceso o servicio. En el siguiente cuadro se definió para la columna de “Prioridad”, que entre menor sea el número, la prioridad es mayor, por ejemplo, prioridad 1 va a requerir mayor atención inmediata que prioridad 2.

		Horas	
Código	**Procesos críticos**	**MTD**	**Prioridad**
31	Gestión de las telecomunicaciones.	8	1
32	Atención de incidentes internos.	8	1
15	Comunicación con el Cliente-Consultoría.	12	2
25	Recepción y atención de casos cliente-service plus.	12	2
22	Recepción y atención de casos Service Plus - Gestión de Proyectos.	12	2
9	Comunicación con el área de gestión de proyectos, miembros de proyectos (desarrolladores, consultores).	18	3

21	Asignar personal al proyecto.	18	3
6	Enviar paquetes de actualización de software a clientes.	18	3
1	Proceso de desarrollo de Software .net.	20	4
2	Proceso de desarrollo de Software en JD Edwards EnterpriseOne.	20	4
29	Instalación de paquetes de actualización en los clientes.	20	4
36	Gestión del Active Directory.	20	4
27	Comunicación service plus-cliente.	20	4
38	Pruebas sobre desarrollos de mejoras y problemas para el cliente.	20	4
34	Instalación de parches en máquinas personales y servidores.	20	4
40	Comunicación constante entre QA - Gestión de Proyectos.	24	5
16	Gestión de planillas (pagos).	24	5
39	Pruebas sobre trabajos de consultoría en el cliente.	48	6
28	Instalación de productos SmarterCommerce en el cliente.	48	6
26	Seguimiento a casos (comunicación, llamadas, correo).	48	6
24	Comunicación con la alta gerencia (llamadas, correos, estatus de proyectos).	48	6
17	Gestión de viáticos.	56	7
3	Pruebas del software desarrollado.	72	8
18	Recepción de pagos.	74	9
23	Recepción de nuevos requerimientos (mejoras, nuevas características).	74	9
11	Procesos de revisión de código.	74	9
12	Análisis de requerimientos sobre cambios o mejoras sobre objetos de JD Edwards EnterpriseOne.	80	10
13	Solicitar aprobación de cambios en objetos de JD Edwards EnterpriseOne.	80	10
20	Pagos a proveedores.	80	10
14	Publicar paquetes de JD Edwards EnterpriseOne para el producto base.	80	10
30	Instalación de nuevas versiones de los productos SmarterCommerce en ambientes de desarrollo y pruebas.	80	10
8	Ingreso de tiempo laborado en @task.	80	10

Tabla 15. MTD y Prioridad de procesos críticos

En la Tabla 15, los procesos ya cuentan con su MTD y priorización, basado en su MTD; entre más bajo sea el MTD mayor será la prioridad. Un ejemplo de cómo interpretar la tabla es el siguiente: el proceso con el código 31 - “Gestión de las telecomunicaciones”, cuenta con un MTD de 8 horas. Esto quiere decir que ese proceso debe ser restaurado en menos de 8 horas para no afectar la organización; como su MTD es el menor, entonces su prioridad va a ser prioridad 1.

4.10 Identificar dependencias

Según (ISO 22301, 2012), esta es la última etapa del BIA, después de varias reuniones con personas involucradas en los proyectos día a día, en cada una de las áreas en Premier Soluciones. Se ha decidido identificar las dependencias de los procesos con prioridad de 1 a 5 solamente; con esto se enumeran cada una de las dependencias en relación con el recurso humano, recursos tecnológicos como hardware y software, proveedores, instalaciones y datos para cada uno de los procesos en el rango de prioridad antes mencionado.

Procesos críticos		Recursos críticos de TI	RTO	RPO
31 - Gestión de las telecomunicaciones.	Externo	Internet	4	
		VPN Telefónica (Miami, USA) - CR - CR-Telefónica (Miami, USA).	8	
		Router Cisco 1900 Series.	8	
32 - Atención de incidentes internos.		Recurso humano de soporte #1 Costa Rica.	8	
		Recurso humano de soporte #1 Miami.	8	
		Laptop personal para el recurso.	8	
15 - Comunicación con el Cliente-Consultoría.		Laptop personal para el recurso.	10	
	Externo	Correo electrónico office 365.	10	

	Externo	Skype for business.	10	
	Externo	Zoom Conference.	10	
	Externo	Internet.	8	
25 - Recepción y atención de casos cliente - service plus.	Externo	Salesforce.	10	
	Externo	Outlook - Office 365.	10	
	Externo	Software @task.	10	
	Externo	Internet.	8	
22 - Recepción y atención de casos Service Plus - Gestión de Proyectos.		Laptop personal para el recurso.	8	
	Externo	Outlook - Office 365.	10	
	Externo	Software @task.	10	
9 - Comunicación con el área de gestión de proyectos, miembros de proyectos. (desarrolladores, consultores).		Laptop personal para el recurso gestión de proyectos.	12	
	Externo	Outlook - Office 365.	12	
	Externo	Software @task.	18	
	Externo	Microsoft Teams.	18	
	Externo	Zoom Conference.	18	

21 - Asignar personal al proyecto.	Externo	Outlook - Office 365.	18	
	Externo	Software @task.	18	
	Externo	Teams.	18	
	Externo	Zoom Conference.	18	
6 - Enviar paquetes de actualización de software a clientes.		FTP - Repositorio de paquetes de actualización - en Telefónica.	12	
		Recurso humano de soporte #1 Miami.	8	
	Externo	Outlook - Office 365.	18	
	Externo	Acceso al TFS Source Code	18	
1 - Proceso de desarrollo de Software .net.		Servidor de JD Edwards EnterpriseOne.	12	
		Servidor de bases de Datos Oracle.	12	
		Servidor de bases de datos IBM/400.	12	
		Servidor de bases de datos SQL Server.	12	
		VPN Telefónica (Miami, USA) - CR / CR-Telefónica (Miami, USA).	16	
		Licencia de Visual Studio.	12	
		Router Cisco 1900 Series.	10	
		Máquina de desarrollo.	12	
		JD Edwards EnterpriseOne.	12	
		Bases de Datos JD Edwards EnterpriseOne (SQL, IBM, Oracle).	12	24
	Externo	Team Foundation Server (TFS).	12	
	Externo	Internet	8	

2 - Proceso de desarrollo de Software en JD Edwards EnterpriseOne.		VPN Telefónica (Miami, USA) - CR / CR - Telefónica (Miami, USA).	16	
		Servidor de JD Edwards EnterpriseOne.	12	
		SmarterCommerceDB - SQL Server.	12	24
		Bases de Datos JD Edwards EnterpriseOne (SQL, IBM, Oracle).	12	24
		Máquina de desarrollo.	12	
	Externo	Internet.		
29 - Instalación de paquetes de actualización en los clientes.		FTP - Repositorio de paquetes de actualización – Telefónica.	16	
		VPN al cliente.	12	
		Laptop personal para el recurso.	12	
	Externo	Team Foundation Server (TFS).	12	
36 - Gestión del Active Directory.		VPN Telefónica (Miami, USA) - CR - CR-Telefónica (Miami, USA).	18	
		Windows server - Active Directory – Telefonica.	12	
27 - Comunicación service plus-cliente.	Externo	Teams.	12	
	Externo	Zoom Conference.	12	
	Externo	Office 365.	12	
	Externo	Internet.	12	
		Servidor Web con aplicaciones para pruebas.	18	

38 - Pruebas sobre desarrollos de mejoras y problemas para el cliente.		Servidor de bases de datos IBM/400 o Oracle o SQL Sever.	16	
		Servidor de JD Edwards EnterpriseOne.	14	
		Servidor capas del negocio.	16	
		SmarterCommerceDB - SQL Server.	16	24
		Bases de Datos JD Edwards EnterpriseOne (SQL, IBM, Oracle).	16	24
		VPN Telefónica (Miami, USA) - CR - CR-Telefónica (Miami, USA).	10	
	Externo	Internet.	8	
34 - Instalación de parches en máquinas personales y servidores.		Recurso humano de soporte #1 Costa Rica.	18	
40 - Comunicación constante entre QA - Gestión de Proyectos.	Externo	Teams.	20	
	Externo	Zoom Conference.	20	
	Externo	Outlook - Office 365.	20	
16 - Gestión de planillas (pagos).		Servidor de JD Edwards EnterpriseOne.	20	
	Externo	Software @task.		

Tabla 16. RTO – RPO de procesos críticos

En la tabla anterior. se observa que cada uno de los procesos o servicios analizados cuentan con dependencias de sistemas, personas, hardware, software, proveedores entre otros que deben ser evaluados para lograr dar continuidad al proceso o servicio. Los servicios comparten muchas de las dependencias; por ello hay que prestar especial atención sobre ellas, para dar una resiliencia mayor a la organización.

4.11 Identificación de controles preventivos

Premier Soluciones cuenta con algunos controles preventivos, con el fin de mantener la continuidad de sus operaciones; ayuda a minimizar la probabilidad de ocurrencia de muchos riesgos asociados a sus activos. Esto permite, en menor medida, evitar algunas de las amenazas identificadas en el análisis de riesgos, realizado. Algunos de los controles aplicados hoy, tanto para la seguridad física como seguridad lógica de la información, se encuentran en la Tabla 17.

Físicos
Uso de UPS para máquinas personales.
Extintores.
Aire acondicionado.
Alarma contra incendios.
Áreas físicas definidas con accesos separados
Uso de UPS en cuarto de máquinas (servidores).
Uso de un SAN.
Lógicos
Antivirus corporativo.
Backup del software de cada una de las máquinas de los colaboradores.
Backup semanal de los servidores de bases de datos en Telefónica.
Políticas generales aplicadas por active directory, a los usuarios y maquinas.
Segmentación de red.
Red desmilitarizada.
Transferencia de datos por VPN.

Tabla 17. Controles preventivos

4.12 Gestión de riegos

Como parte de apoyo al desarrollo del BIA, para Premier Soluciones, es importante realizar una adecuada gestión de riesgos que le permita determinar cuáles son los principales riesgos de sus procesos u actividades y las dependencias en relación con el recurso humano, recursos tecnológicos como hardware y software, proveedores, instalaciones y datos de ellos. La correcta gestión de riesgos permite el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables.

4.12.1 Metodología

Es importante aclarar que para este trabajo y basados en la metodología de gestión de riesgos impulsadas por (ISO 31000, 2018), llamamos activos a las actividades y procesos, y sus dependencias identificadas en el BIA realizado anteriormente para Premier Soluciones. La gestión de los riesgos está estructurada de forma metódica en las normas ISO (ver Figura 14).

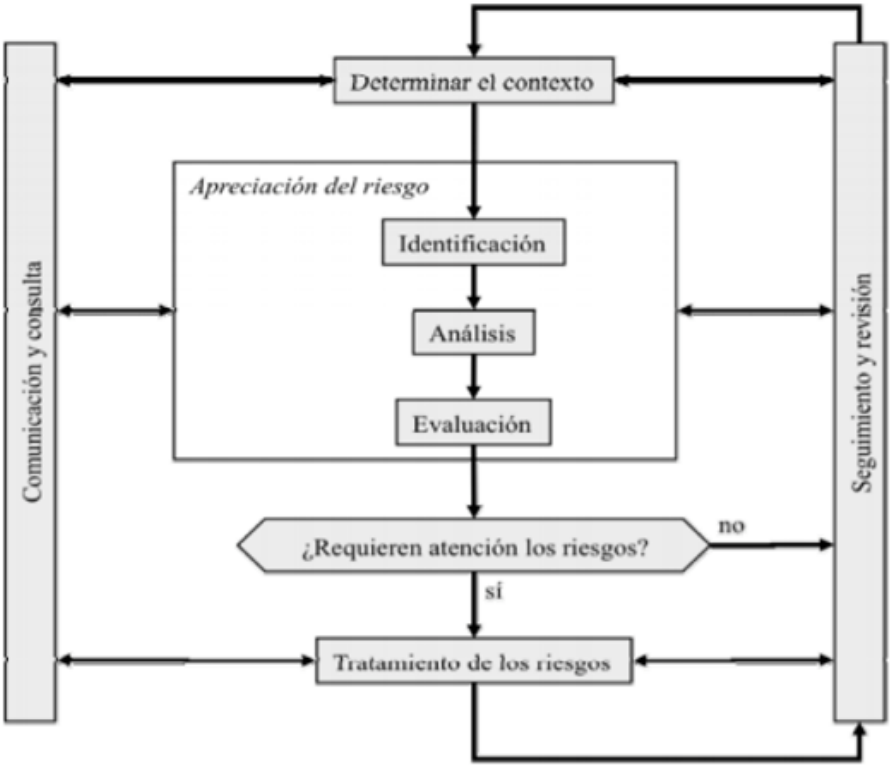


Figura 14. Proceso de gestión de riesgos (ISO 31000)

4.12.1.1 Proceso de gestión de riesgos

Según (ISO 31000, 2018), los elementos a en la Figura 15, son los que deben estar presentes en la correcta gestión de riesgos.

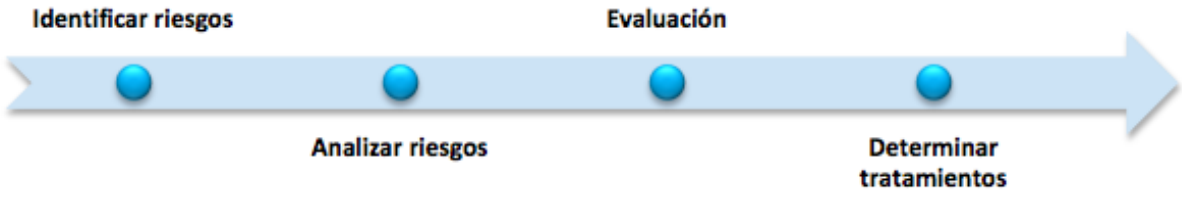


Figura 15. Gestión de riesgos

La determinación del contexto: consiste en determinar los parámetros y condicionantes externos e internos que permiten encuadrar la política que se seguirá para gestionar los riesgos; un ejemplo de sus elementos es el alcance del análisis, incluyendo obligaciones propias y obligaciones contraídas.

- La identificación de los riesgos: encuentra una relación de los posibles puntos de vulnerables. Lo que se identifica será analizado en la una etapa posterior y lo que no se identifique quedará como riesgo oculto o ignorado.
- El análisis de los riesgos: busca calificar los riesgos identificados de forma que con el resultado del análisis se tendrá una visión estructurada que permita centrarse en lo más importante.
- La evaluación de los riesgos: traduce las consecuencias a términos de negocio. En este punto, los encargados de tomar decisiones en Premier Soluciones deberán elegir qué riesgos se aceptan y cuáles no, así como de en qué circunstancias aceptar un riesgo, trabajar en su tratamiento o heredarlo.
- Identificación de amenazas.
- El tratamiento de los riesgos: recopila las actividades encaminadas a modificar la situación de riesgo, como por ejemplo mitigar, eliminar o evitar, compartir o transferir y financiar o aceptar.

4.12.2 Desarrollo

4.12.2.1 Establecimiento del contexto

Los procesos y actividades que aplican para este análisis son los determinados en la última parte del BIA de Premier Soluciones, que van desde prioridad de un 1 y hasta prioridad 5, definido de esta forma por los miembros que participan activamente en proyectos en Premier Soluciones y la gerencia esto mediante correos electrónicos.

En la Tabla 18 se encuentra la lista de todos los servicios, procesos y sus dependencias antes mencionados, sobre los cuales va a trabajar la gestión de los riesgos asociados.

Procesos críticos		Recursos críticos de TI
31 - Gestión de las telecomunicaciones	Externo	Internet.
		VPN Telefónica (Miami, USA) - CR - CR- Telefónica (Miami, USA).
		Router Cisco 1900 Series.
32 - Atención de incidentes internos		Recurso humano de soporte #1 Costa Rica.
		Recurso humano de soporte #1 Miami.
		Laptop personal para el recurso.
15 - Comunicación con el Cliente-Consultoría		Laptop personal para el recurso.
	Externo	Correo electrónico office 365.
	Externo	Skype for business.
	Externo	Zoom Conference.
	Externo	Internet.
25 - Recepción y atención de casos cliente - service plus	Externo	Salesforce.
	Externo	Outlook - Office 365.
	Externo	Software @task.
	Externo	Internet.
22 - Recepción y atención de casos Service Plus - Gestión de Proyectos		Laptop personal para el recurso.
	Externo	Outlook - Office 365.

	Externo	Software @task.
9 - Comunicación con el área de gestión de proyectos, miembros de proyectos (desarrolladores, consultores)		Laptop personal para el recurso gestión de proyectos.
	Externo	Outlook - Office 365.
	Externo	Software @task.
	Externo	Microsoft Teams.
	Externo	Zoom Conference.
21 - Asignar personal al proyecto	Externo	Outlook - Office 365.
	Externo	Software @task.
	Externo	Teams.
	Externo	Zoom Conference.
6 - Enviar paquetes de actualización de software a clientes		FTP - Repositorio de paquetes de actualización - en Telefónica.
		Recurso humano de soporte #1 Miami.
	Externo	Outlook - Office 365.
	Externo	Acceso al TFS Source Code.
1 - Proceso de desarrollo de Software .net		Servidor de JD Edwards EnterpriseOne.

		Servidor de bases de Datos Oracle
		Servidor de bases de datos IBM/400.
		Servidor de bases de datos SQL Server.
		VPN Telefónica (Miami, USA) - CR - CR- Telefónica (Miami, USA).
		Licencia de Visual Studio.
		Router Cisco 1900 Series.
		Máquina de desarrollo.
		JD Edwards EnterpriseOne.
		Bases de Datos JD Edwards EnterpriseOne (SQL, IBM, Oracle).
	Externo	Team Foundation Server (TFS).
	Externo	Internet.
2 - Proceso de desarrollo de Software en JD Edwards EnterpriseOne		VPN Telefónica (Miami, USA) - CR - CR- Telefónica (Miami, USA).
		Servidor de JD Edwards EnterpriseOne.
		SmarterCommerceDB - SQL Server.
		Bases de Datos JD Edwards EnterpriseOne (SQL, IBM, Oracle).
		Máquina de desarrollo.
	Externo	Internet.
29 - Instalación de paquetes de actualización en los clientes		FTP - Repositorio de paquetes de actualización – Telefónica.
		VPN al cliente.
		Laptop personal para el recurso.
	Externo	Team Foundation Server (TFS).
36 - Gestión del Active Directory		VPN Telefónica (Miami, USA) - CR - CR- Telefónica (Miami, USA).
		Windows server - Active Directory – Telefonica.

27 - Comunicación service plus-cliente	Externo	Teams.
	Externo	Zoom Conference.
	Externo	Office 365.
	Externo	Internet.
38 - Pruebas sobre desarrollos de mejoras y problemas para el cliente		Servidor Web con aplicaciones para pruebas.
		Servidor de bases de datos IBM/400 o Oracle o SQL Sever.
		Servidor de JD Edwards EnterpriseOne.
		Servidor capas del negocio.
		SmarterCommerceDB - SQL Server.
		Bases de Datos JD Edwards EnterpriseOne (SQL, IBM, Oracle).
		VPN Telefónica (Miami, USA) - CR - CR- Telefónica (Miami, USA).
	Externo	Internet.
34 - Instalación de parches en máquinas personales y servidores		Recurso humano de soporte #1 Costa Rica.
40 - Comunicación constante entre QA - Gestión de Proyectos	Externo	Teams.
	Externo	Zoom Conference.
	Externo	Outlook - Office 365.

16 - Gestión de planillas(pagos)		Servidor de JD Edwards EnterpriseOne.
	Externo	Software @task.

Tabla 18. Procesos y servicios Premier Soluciones

4.12.2.2 Identificación de los riesgos

En esta etapa para Premier Soluciones después de reuniones entre involucrados en los proyectos y miembros de la alta gerencia, se decide contemplar las siguientes actividades:

- Procesos y servicios críticos de Premier Soluciones.
- Dependencias en TI para los procesos y servicios.
- Riesgo identificado, para cada procesos, servicio o dependencia se propone analizar la naturaleza del riesgo.
- Identificar las amenazas para cada producto o servicio.

Estimación del riesgo

Para este proyecto de Premier Soluciones, como metodología de análisis de riegos, se va a utilizar la forma cualitativa debido a que interesa saber el impacto contra la probabilidad que una vulnerabilidad sea explotada por una amenaza y no el impacto económico. Para esta estimación cualitativa se tienen los siguientes valores.

Impacto		Probabilidad	
5	Severo	5	Muy alta
4	Mayor	4	Alta
3	Menor	3	Medio
2	Bajo	2	Baja
1	Insignificante	1	Muy baja

Tabla 19. Estimación cualitativa el riesgo

En la Tabla 19 se pueden observar los valores numéricos asignados, tanto al impacto de los riesgos como a su probabilidad de ocurrencia; en ambos casos, es 5 el valor más alto, por consiguiente, el más significativo y 1 el valor más bajo; en otras palabras, el de menor peso.

4.12.3 Análisis de los riesgos

En la Tabla 20. Análisis de riesgos, se puede observar cada uno de los riesgos identificados para los procesos y servicios críticos previamente identificados en el BIA. En conjunto con los riesgos, se pueden observar el impacto y la probabilidad, asignados a cada uno de ellos después de varios análisis, con las diferentes áreas dentro de Premier Soluciones.

Proceso o servicio	Código	Riesgos	Impacto	Probabilidad
31 - Gestión de las telecomunicaciones	31-R01	Pérdida de comunicación con Telefónica.	5	4
	31-R02	Retrasos en proyectos.	5	4
	31-R03	Personas sin laborar.	3	4
	31-R04	Daño de imagen por retrasos en proyectos.	4	3
	31-R05	Pérdida de clientes.	4	2
	31-R06	Explotación de vulnerabilidades sobre la infraestructura.	5	2
	31-R07	Explotación de vulnerabilidades de día cero.	5	2
	31-R08	Disrupción del enlace a internet.	5	4
	31-R09	Daño de equipo de telecomunicaciones (Router, switch, vpn).	5	4
32 - Atención de incidentes internos	32-R01	Daño de imagen por incidentes en seguridad de la información.	5	4
	32-R02	Pérdida de comunicación con Telefónica.	5	4
	32-R03	Robo de datos sensibles.	5	3
	32-R04	Acceso no autorizado a la información.	4	3
	32-R05	Retrasos en proyectos.	5	3
15 - Comunica	15-R01	Daño de imagen por incumplimiento de contratos.	5	2

ción con el Cliente-Consultoría	15-R02	Pérdida de clientes.	4	2
25 - Recepción y atención de casos cliente - service plus	25-R01	Daño de imagen por incumplimiento de contratos.	5	3
	25-R02	Pérdida de clientes.	4	2
	25-R03	Demandas judiciales por incumplimiento de contratos.	4	2
22 - Recepción y atención de casos Service Plus - Gestión de Proyectos	22-R01	Daño de imagen por incumplimiento de contratos.	5	2
	22-R02	Pérdida de clientes.	4	2
	22-R03	Retrasos en proyectos.	4	2
9 - Comunicación con el área de gestión de proyectos, miembros de proyectos (desarrolladores, consultores)	9-R01	Retrasos en proyectos.	4	3
	9-R02	Personas sin laborar.	3	2
	9-R03	Tareas con brechas entre lo que quiere y lo que se realizó (ambigüedad de los requerimientos).	4	4
21 - Asignar personal al proyecto	21-R01	Retrasos en proyectos.	4	2
	21-R02	Personas sin laborar.	3	2
	21-R03	Daño de imagen por retrasos en proyectos.	4	2
6 - Enviar paquetes de actualizaci	6-R01	Pérdida de clientes.	4	2
	6-R02	Demandas judiciales por retrasos en proyectos.	5	2

ón de software a clientes				
1 - Proceso de desarrollo de Software .net	1-R01	Retrasos en proyectos.	4	4
	1-R02	Pérdida de clientes.	4	4
	1-R03	Personas sin laborar.	3	3
	1-R04	Daño de equipo de PC para el trabajo.	4	4
	1-R05	Daño de imagen por retrasos en proyectos.	5	4
2 - Proceso de desarrollo de Software en JD Edwards Enterprise One	2-R01	Retrasos en proyectos.	4	4
	2-R02	Pérdida de clientes.	4	4
	2-R03	Personas sin laborar.	3	3
	2-R04	Daño de imagen por retrasos en proyectos.	5	4
29 - Instalación de paquetes de actualización en los clientes	29-R01	Pérdidas económicas por penalizaciones del contrato al incumplir con los tiempos estipulados.	4	2
	29-R02	Daño de imagen por incumplimiento de contratos.	4	2
36 - Gestión del Active Directory	36-R01	Acceso no autorizado a la información.	5	4
	36-R02	Fuga de información.	5	4
	36-R03	Explotación de vulnerabilidades sobre la infraestructura.	5	5
27 - Comunicación service plus-cliente	27-R01	Daño de imagen por retrasos en proyectos.	4	3
	27-R02	Entregas con errores en productos o servicios por requerimientos ambiguos.	4	5

38 - Pruebas sobre desarrollos de mejoras y problemas para el cliente	38-R01	Daño de imagen por productos o servicios de baja calidad.	4	4
	38-R02	Brechas de seguridad en el producto entregado al cliente.	4	3
34 - Instalación de parches en máquinas personales y servidores	34-R01	Explotación de vulnerabilidades sobre la infraestructura.	4	2
	34-R02	Explotación de vulnerabilidades de día cero.	4	2
40 - Comunicación constante entre QA - Gestión de Proyectos	40-R01	Daño de imagen por productos o servicios de baja calidad.	4	2
	40-R02	Brechas de seguridad en el producto entregado al cliente.	4	3
16 - Gestión de planillas(pagos)	16-R01	Demandas por parte de colaboradores por el no pago de sus servicios.	4	2
	16-R02	Retrasos en proyectos por renuncias del capital humano.	4	1

Tabla 20. Análisis de riesgos

4.12.4 Evaluación de los riesgos

En esta etapa, por medio de gráficos, se pretende interpretar los datos analizados, de manera que se pueda ver con claridad cuáles son los riesgos con una alta probabilidad de ocurrencia y con un impacto considerable para la organización. En la Tabla 21 se puede encontrar la representación del mapa de calor, asociado a ese análisis de riesgos. En este se pueden observar cuáles son los riesgos que tienen mayor impacto en la organización y cuál es la probabilidad de que se materialice. Los que cumplan con ese criterio, deben ser tratados con prioridad, para minimizar el impacto en caso de que

una vulnerabilidad de este sea explotada. Los procesos críticos tratados, identificados en el mapa de calor por el color rojo, son los siguientes:

- 32-R01 - Daño de imagen por incidentes en seguridad de la información.
- 32-R02 - Pérdida de comunicación con Telefónica.
- 32-R03 - Robo de datos sensibles.
- 32-R05 - Retrasos en proyectos.
- 25-R01 - Daño de imagen por incumplimiento de contratos.
- 31-R01 - Pérdida de comunicación con Telefónica.
- 31-R02 - Retrasos en proyectos.
- 31-R03 - Personas sin laborar.
- 31-R08 - Disrupción del enlace a internet.
- 31-R09 - Daño de equipo de telecomunicaciones (router, switch, vpn).
- 36-R01 - Acceso no autorizado a la información.
- 36-R02 - Fuga de información.
- 36-R03 - Explotación de vulnerabilidades sobre la infraestructura.
- 9-R03 - Tareas con brechas entre lo que quiere y lo que se realizó (ambigüedad de los requerimientos).
- 1-R01 - Retrasos en proyectos.
- 1-R02 - Pérdida de clientes.
- 1-R04 - Daño de imagen por retrasos en proyectos.
- 2-R01 - Retrasos en proyectos.
- 2-R02 - Pérdida de clientes.
- 2-R04 - Daño de imagen por retrasos en proyectos.
- 38-R01 - Daño de imagen por productos o servicios de baja calidad.
- 27-R02 – Errores en entrega de productos o servicios por requerimientos ambiguos.

Impacto	Severo		31-R06 \ 31-R07 \ 15-R01\ 22-R01 \ 6-R02	32-R03 \ 32-R05 \ 25-R01	31-R01 \ 31-R02 \ 32-R01 \ 32-R02 \ 1-R05 \ 2-R04 \ 36-R01 \ 36-R02 \ 31-R08 \ 31-R09	36-R03
	Mayor	16-R02	31-R05 \ 15-R02 \ 25-R02 \ 25-R03 \ 22-R02 \ 22-R03 \ 21-R01 \ 21-R03 \ 6-R01 \ 29-R01 \ 29-R02 \ 34-R01 \ 34-R02 \ 40-R01 \ 16-R01	31-R04 \ 32-R04 \ 9-R01 \ 27-R01 \ 38-R02 \ 40-R02	9-R03 \ 1-R01 \ 1-R02 \ 2-R01 \ 2-R02 \ 38-R01 \ 1-R04	27-R02
	Menor		9-R02 \ 21-R02	1-R03 \ 2-R03	31-R03	
	Bajo					
	Insignificante					
		Muy bajo	Bajo	Medio	Alta	Muy alta
		Probabilidad				

Tabla 21. Probabilidad vs Impacto

4.12.5 Identificación de amenazas

Para los procesos y servicios identificados podemos clasificar las amenazas en las siguientes categorías:

Amenazas naturales

- Desastres naturales.

Amenazas ambientales

- Fuego.
- Daños por agua.
- Cortocircuito.
- Corte del suministro eléctrico.
- Condiciones inadecuadas de temperatura y/o humedad.
- Fallo de hardware.
- Fallo de software.
- Degradación de los soportes de almacenamiento de información.

Amenazas humanas

- Error humano.
- Robo de hardware/software/datos.
- Ataque de hacker.
- Incumplimiento de documentación.
- Accesos no autorizados.
- Programa maligno.
- Manipulación de la información.
- Ataque por hacker.

Para este análisis se identificaron las posibles amenazas que podrían afectar los procesos o servicios de Premier Soluciones. Para una mejor comprensión, en la Tabla 22, se encuentra el nombre del proceso o servicio y visualmente, para cada uno de los riesgos, las amenazas asociadas. Por ejemplo, el proceso “31 - Gestión de las

telecomunicaciones” cuenta con el riesgo *“Pérdida de comunicación con Telefónica por daño de hardware”*, este riesgo se puede materializar por las siguientes amenazas:

- Fuego.
- Daños por agua.
- Cortocircuito.
- Fallo de hardware.
- Fallo de software.
- Corte del suministro eléctrico.
- Condiciones inadecuadas de temperatura y/o humedad.
- Error humano.
- Robo de hardware/software/datos.
- Desastres naturales.
- Ataque de hacker.

De esta forma, Premier Soluciones puede fácilmente crear mecanismos que le ayuden a mitigar, evitar, transferir o aceptar muchos de los riesgos, al atacar sus amenazas.

Proceso o servicio	Riesgos	Fuego	Daños por agua	Cortocircuito	Fallo de hardware	Fallo de software	Corte del suministro eléctrico	Condiciones inadecuadas de temperatura y/o humedad	Degradación de los soportes de almacenamiento	Error Humano	Incumplimiento de documentación	Accesos no autorizados	Malware	Manipulación de la información	Robo hardware/software/datos	Desastres naturales	Ataque por hacker
31 - Gestión de las telecomunicaciones	Pérdida de comunicación con Telefónica por daño de hardware.	X	X	X	X	X	X	X		X					X	X	X
	Retrasos en proyectos.	X	X	X	X	X	X		X	X	X	X	X	X		X	
	Personas sin laborar.	X	X	X	X	X	X		X	X	X	X	X	X	X	X	
	Daño de imagen por retrasos en proyectos.	X	X	X	X	X	X		X	X	X	X	X	X	X	X	
	Pérdida de clientes.	X	X	X	X	X	X		X	X	X	X	X	X	X	X	
	Explotación de vulnerabilidades sobre la infraestructura.				X	X				X	X	X	X	X			X
	Explotación de vulnerabilidades de día cero.				X	X				X	X	X	X	X			X
	Disrupción del enlace a internet.			X			X	X		X						X	
	Daño de equipo de telecomunicaciones (router, switch, vpn).	X	X	X	X	X	X	X		X		X			X	X	
32 - Atención de incidentes internos	Daño de imagen por incidentes en seguridad de la información.								X	X	X	X	X	X			X
	Pérdida de comunicación con Telefónica.	X	X	X	X	X	X	X		X		X	X	X	X	X	
	Robo de datos sensibles.									X	X	X	X	X	X		X
	Acceso no autorizado a la información.									X	X	X	X	X	X		X
	Retrasos en proyectos.	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
15 - Comunicación con el Cliente-Consultoría	Daño de imagen por incumplimiento de contratos.	X	X	X	X	X	X			X	X				X	X	
	Pérdida de clientes.	X	X	X	X	X	X		X	X	X	X	X	X	X	X	

25 - Recepción y atención de casos cliente - service plus	Daño de imagen por incumplimiento de contratos.	X	X	X	X	X	X			X	X				X		
	Pérdida de clientes.	X	X	X	X	X	X		X	X	X	X	X	X	X		
	Demandas judiciales por incumplimiento de contratos.	X	X	X	X	X	X			X	X	X	X	X	X	X	
22 - Recepción y atención de casos Service Plus - Gestión de Proyectos	Daño de imagen por incumplimiento de contratos.	X	X	X	X	X	X			X	X				X		
	Pérdida de clientes.	X	X	X	X	X	X		X	X	X	X	X	X	X		
	Retrasos en proyectos.	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
9 - Comunicación con el área de gestión de proyectos, miembros de proyectos (desarrolladores, consultores)	Retrasos en proyectos.	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
	Personas sin laborar.	X	X	X	X	X	X	X	X	X					X	X	
	Tareas con brechas entre lo que quiere y lo que se realizó (ambigüedad de los requerimientos).									X	X						
21 - Asignar personal al proyecto	Retrasos en proyectos.	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
	Personas sin laborar.	X	X	X	X	X	X	X	X	X					X	X	
	Daño de imagen por retrasos en proyectos.	X	X	X	X	X	X			X		X	X	X	X	X	
6 - Enviar paquetes de actualización de software a clientes	Pérdida de clientes.				X	X				X		X	X	X	X	X	
	Demandas judiciales por retrasos en proyectos.	X	X	X	X	X	X			X	X	X	X	X	X	X	
1 - Proceso de desarrollo de Software .net	Retrasos en proyectos.	X	X	X	X	X	X	X		X		X	X	X	X	X	
	Pérdida de clientes.										X						
	Personas sin laborar.	X	X	X	X	X	X			X			X		X	X	
	Daño de equipo de PC para el trabajo.	X	X	X	X	X	X	X		X			X		X	X	
	Daño de imagen por retrasos en proyectos.	X	X	X	X	X	X			X	X		X			X	
2 - Proceso de desarrollo	Retrasos en proyectos.	X	X	X	X	X	X	X		X		X	X	X	X	X	
	Pérdida de clientes.										X						

de Software en JD Edwards EnterpriseOne	Personas sin laborar.	X	X	X	X	X	X			X			X		X	X	
	Daño de imagen por retrasos en proyectos.	X	X	X	X	X	X			X	X		X		X	X	
29 - Instalación de paquetes de actualización en los clientes	Pérdidas económicas por penalizaciones del contrato al incumplir con los tiempos estipulados.				X	X					X				X	X	
	Daño de imagen por incumplimiento de contratos.				X	X					X				X	X	
36 - Gestión del Active Directory	Acceso no autorizado a la información									X	X	X	X	X	X		X
	Fuga de información.									X	X	X	X	X	X		X
	Explotación de vulnerabilidades sobre la infraestructura.									X	X	X	X	X	X		X
27 - Comunicación service plus-cliente	Daño de imagen por retrasos en proyectos.	X	X	X	X	X	X			X		X	X	X	X	X	
	Entregas errores de productos o servicios por requerimientos ambiguos.									X	X						
38 - Pruebas sobre desarrollos de mejoras y problemas para el cliente	Daño de imagen por productos o servicios de baja calidad.									X	X						
	Brechas de seguridad en el producto entregado al cliente.									X	X						X
34 - Instalación de parches en máquinas personales y servidores	Explotación de vulnerabilidades sobre la infraestructura.									X	X	X	X	X	X		
	Explotación de vulnerabilidades de día cero.									X	X	X	X	X	X		
40 - Comunicación constante entre QA - Gestión de Proyectos	Daño de imagen por productos o servicios de baja calidad.									X	X						
	Brechas de seguridad en el producto entregado al cliente.									X	X						

16 - Gestión de planillas(pagos)	Demandas por parte de colaboradores por el no pago de sus servicios.										X						
	Retrasos en proyectos por renuncias del capital humano.	X	X	X	X	X	X			X			X		X	X	

Tabla 22. Amenazas

4.12.6 Tratamiento de los riesgos

Según reuniones con personas involucradas en proyectos dentro de Premier Soluciones y algunos otros colaboradores, se ha tomado la decisión de dar un tratamiento a los riesgos críticos identificados en el mapa de calor (Tabla 21) con el color rojo, que vienen a ser los riesgos con mayor privacidad de materialización y con un impacto fuerte dentro de esta.

Proceso o servicio	Código	Riesgos	Estatus de Riesgo	Justificación
31 - Gestión de las telecomunicaciones	31-R01	Pérdida de comunicación con Telefónica.	Mitigar	Se recomienda la creación de un DRP que migre la infraestructura a la nube que permita eliminar la dependencia absoluta con Telefónica.
	31-R02	Retrasos en proyectos.	Mitigar	Se recomienda la creación de un DRP que migre la infraestructura a la nube que permita eliminar la dependencia absoluta con Telefónica.
	31-R03	Personas sin laborar.	Mitigar	Se recomienda la creación de un DRP que migre la infraestructura a la nube que permita eliminar la dependencia absoluta con Telefónica.
	31-R08	Disrupción del enlace a internet.	Mitigar	Contar con diferentes proveedores de internet, contar con políticas de “Working From Home” para poder aplicarlo

	31-R09	Daño de equipo de telecomunicaciones (router, switch, vpn.	Mitigar	Contar con duplicidad de hardware o con contratos con proveedores de cercanos o bien migración de la infraestructura a la nube
32 - Atención de incidentes internos	32-R01	Daño de imagen por incidentes en seguridad de la información.	Mitigar	Crecer el área encargada y capacitar en temas de atención de incidentes
	32-R02	Pérdida de comunicación con Telefónica.	Mitigar	Se recomienda la creación de un DRP que migre la infraestructura a la nube que permita eliminar la dependencia absoluta con Telefónica.
	32-R03	Robo de datos sensibles.	Mitigar	Crear una política de ciberseguridad que contribuya a la seguridad de la información
	32-R04	Acceso no autorizado a la información.		
	32-R05	Retrasos en proyectos.	Aceptar	Se acepta el riesgo debido a que teniendo un buen grupo de atención a incidentes y una infraestructura en la nube permitirá la una resiliencia mayor ante un incidente
15 - Comunicación con el Cliente-Consultoría	15-R01	Daño de imagen por incumplimiento de contratos.	Mitigar	Contar con diferentes canales de comunicación y tener una buena forma de comunicar al cliente sobre algún tipo de disrupción
	15-R02	Pérdida de clientes.	Mitigar	Se puede mitigar fortaleciendo la comunicación con el cliente y comunicando de forma clara sobre posibles atrasos en proyectos

25 - Recepción y atención de casos cliente - service plus	25-R01	Daño de imagen por incumplimiento de contratos.	Mitigar	Contar con diferentes canales de comunicación y tener una buena forma de comunicar al cliente sobre algún tipo de disrupción
	9-R03	Tareas con brechas entre lo que quiere y lo que se realizó (ambigüedad de los requerimientos).	Mitigar	Creación de Política de Working From Home, fomentar medios alternos de comunicación
1 - Proceso de desarrollo de Software .net	1-R01	Retrasos en proyectos.	Mitigar	Creación de Política de Working From Home, fomentar medios alternos de comunicación
	1-R02	Pérdida de clientes.	Mitigar	Creación de Política de Working From Home, fomentar medios alternos de comunicación
	1-R04	Daño de equipo de PC para el trabajo.	Transferir	Asegurar PC's contra robo, asegurar el menaje de la oficina contra daños
	1-R05	Daño de imagen por retrasos en proyectos.	Mitigar	Creación de Política de “Working From Home”, fomentar medios alternos de comunicación, mejorar los contratos legales para proteger de mejor forma a la empresa
2 - Proceso de desarrollo de Software en JD	2-R01	Retrasos en proyectos.	Mitigar	Creación de Política de Working From Home, fomentar medios alternos de comunicación
	2-R02	Pérdida de clientes.	Mitigar	Creación de Política de Working From Home, fomentar medios alternos de comunicación

Edwards EnterpriseOne	2-R04	Daño de imagen por retrasos en proyectos.	Mitigar	Creación de Política de Working From Home, fomentar medios alternos de comunicación, mejorar los contratos legales para proteger de mejor forma a la empresa
36 - Gestión del Active Directory	36-R01	Acceso no autorizado a la información.	Mitigar	Crear una política de ciberseguridad que contribuya a la seguridad de la información
	36-R02	Fuga de información.	Mitigar	Crear una política de ciberseguridad que contribuya a la seguridad de la información
	36-R03	Explotación de vulnerabilidades sobre la infraestructura.	Mitigar	Crear una política de ciberseguridad que contribuya a la seguridad de la información, conformar un pequeño grupo encargado de la Ciberseguridad
27 - Comunicación service plus-cliente	27-R02	Entregas de errores de productos o servicios por requerimientos ambiguos.	Mitigar	Contar con diferentes canales de comunicación y tener una buena forma de comunicar al cliente sobre algún tipo de disrupción
38 - Pruebas sobre desarrollos de mejoras y problemas para el cliente	38-R01	Daño de imagen por productos o servicios de baja calidad.	Mitigar	Se recomienda la creación de un DRP que migre la infraestructura a la nube que permita eliminar la dependencia absoluta con Telefónica y poder tener servidores para pruebas en todo momento

Tabla 23. Tratamiento de los riesgos

Según la Tabla 23, podemos decir que la mayoría de los riesgos encontrados pueden mitigarse de tal forma que se reduzca el riesgo a un nivel aceptable o manejable; se nota que Premier Soluciones y, como cualquier otra empresa que ofrece productos y servicios, depende de sus clientes; este análisis deja entrevisto los posibles riesgos con el fallo de alguno de sus productos o servicios más críticos. Se puede ver que muchos de los riesgos se comparten entre varios servicios, como, por ejemplo: Pérdida de comunicación con Telefónica; es aquí donde nace como opción para su mitigación, la elaboración de un DRP, basado en la nube con el cual muchos de los riesgos van a ser mitigados.

CAPÍTULO V

5 Elaboración de procedimientos DRP

Un desastre resultará en pérdidas reales, tanto para los sistemas de información como para la mayoría de los datos almacenados. Como mínimo, el tiempo, el dinero y la capacidad operativa se perderán. Un desastre físico (huracán, inundación, explosión, etc.) llevaría a la pérdida de al menos algunos datos y software. Un plan de recuperación de desastres es un elemento esencial de un programa de recuperación de negocios integral.

El plan de recuperación de desastres para Premier Soluciones, como se describió en los objetivos, es una guía para su implementación y no un producto terminado. El diseño del prototipo del Plan de Recuperación de Desastres (DPR), permite desarrollar una guía que facilita la recuperación de elementos como equipos y aplicaciones que soportan los procesos críticos en el Área IT de Premier Soluciones. La implementación de este prototipo permitirá mantener la continuidad de las operaciones y minimizar el tiempo de interrupción de los procesos críticos, ocasionados por la presencia de amenazas naturales, humanas o ambientales.

5.1 Metodología

La metodología recomendada para el desarrollo del plan de recuperación de desastres para los sistemas de información críticos de TI de Premier Soluciones se moldea desde el inicio de este proyecto en donde se tomaron en cuenta insumos para el DRP como la implementación del BIA y la realización del análisis de riesgos. A falta solamente de definir las estrategias de recuperación y la definición de roles y responsabilidades. Basada en las recomendaciones del NIST (National Institute of Standards and Technology), DRII (Disaster Recovery Institute International) y el BCI (Business Continuity Institute), en la Figura 16 se define la siguiente estructura del futuro DRP.

Figura 16. Fases del prototipo DRP

5.2 Inicio del proyecto Plan de Recuperación ante desastres

Cabe resaltar que para el inicio del proyecto se necesita el apoyo de la gerencia, puesto que este proyecto devenga gastos en horas de personas y recursos de TI fuera de la organización, además su validez necesita de estas firmas. En esta fase es donde se definen aspectos administrativos para iniciar con el proyecto, como por ejemplo documentar la razón de ser del DRP y los beneficios que obtiene la organización con su realización, elegir las personas que estarán en el proyecto, con consiguiente tendrán algún tipo de responsabilidad. Puntualmente algunas de las actividades que se deben realizar son las siguientes:

- Revisión de los procesos y servicios críticos de Premier Soluciones; este paso no va a comenzar desde 0, debido a que el BIA realizado en este documento, ya identificó los servicios y procesos críticos de Premier Soluciones.
- Entendimiento de TI, en dónde estamos y hacia a dónde queremos ir.

- Valoración de los riesgos, es un proceso que ya se realizó en este documento, sobre los procesos y servicios críticos de Premier Soluciones.
- Evaluación del nivel en el que se encuentra la organización y propuestas de acciones por seguir para mejorar los niveles de respuesta ante eventos que afecten la entrega de servicios.
- Establecer los objetivos de continuidad como por ejemplo procesos validos adecuados, para comunicación de crisis, determinar qué eventos son catalogados como una crisis, evaluación de incidentes, respuesta a ciber-incidentes, recuperación de desastres, entre otros aspectos.
- Acordar el compromiso con la gerencia para la realización del proyecto por escrito y con sus debidas firmas y confirmar la existencia de recursos financieros, humanos y logísticos.
- Conformar el equipo del DRP. En este paso se debe elegir a los responsables de la realización de cada una de las actividades; se recomienda un grupo multidisciplinario para obtener diferentes puntos de vista. Es requerido que las personas, dentro de Premier Soluciones, estén enteradas de este proyecto, en caso de tener que colaborar con algún tipo de dato.
- Refinar el alcance del proyecto; en este punto se debe revisar y aprobar el alcance del proyecto tomando en cuenta el objetivo de continuidad establecido.

5.3 Análisis de impacto sobre el negocio (BIA)

El BIA es un insumo para la creación del DRP, con el que se logran identificar los procesos y servicios críticos y sus dependencias para cada una de las áreas de Premier Soluciones; a estos procesos identificados se le asignaron los valores de RTO, RPO y MTD, con el fin de conocer cuál es la prioridad de recuperación de cada uno.

5.4 Análisis de riesgos

El análisis de riesgos permite conocer cuáles son los riesgos asociados a los procesos y servicios definidos en el BIA y con esta información conocer, mediante un mapa de calor, cuál es la probabilidad de ocurrencia contra el impacto para la organización y así identificar a cuáles riesgos son los que se les debe dar mayor tratamiento prioritario, para evitar o disminuir la interrupción de los productos o servicios. Además de esto, se conoció cuáles son

las amenazas que pueden afectar a cada uno de los productos y servicios de Premier Soluciones.

5.5 Identificación de los controles preventivos

En el desarrollo del BIA se identificaron cuáles son los controles preventivos que utiliza actualmente Premier Soluciones, para proteger sus activos, reducir los efectos de las disrupciones a los productos y servicios y aumentar su disponibilidad con el fin de reducir los costos de contingencia del ciclo de vida.

5.6 Estrategias de recuperación

Las estrategias de recuperación están basadas en los resultados obtenidos en el BIA. La Tabla 24 muestra los procesos y servicios críticos y sus dependencias de TI; estos se encuentran ordenados por prioridad de recepción, basados en su tiempo RTO y MTD.

Procesos críticos		Recursos críticos de TI	RTO
31 - Gestión de las telecomunicaciones	Externo	Internet.	4
		VPN Telefónica (Miami, USA) - CR - CR- Telefónica (Miami, USA).	8
		Router Cisco 1900 Series.	8
32 - Atención de incidentes internos		Recurso humano de soporte #1 Costa Rica.	8
		Recurso humano de soporte #1 Miami.	8
		Laptop personal para el recurso.	8
15 - Comunicación con el Cliente-Consultoría		Laptop personal para el recurso.	10
	Externo	Correo electrónico office 365.	10
	Externo	Skype for business.	10
	Externo	Zoom Conference.	10

	Externo	Internet.	8
25 - Recepción y atención de casos cliente - service plus	Externo	Salesforce.	10
	Externo	Outlook - Office 365.	10
	Externo	Software @task.	10
	Externo	Internet.	8
22 - Recepción y atención de casos Service Plus - Gestión de Proyectos		Laptop personal para el recurso.	8
	Externo	Outlook - Office 365.	10
	Externo	Software @task.	10
9 - Comunicación con el área de gestión de proyectos, miembros de proyectos (desarrolladores, consultores)		Laptop personal para el recurso gestión de proyectos.	12
	Externo	Outlook - Office 365.	12
	Externo	Software @task.	18
	Externo	Microsoft Teams.	18
	Externo	Zoom Conference.	18
21 - Asignar personal al proyecto	Externo	Outlook - Office 365.	18

	Externo	Software @task.	18
	Externo	Teams.	18
	Externo	Zoom Conference.	18
6 - Enviar paquetes de actualización de software a clientes		FTP - Repositorio de paquetes de actualización - en Telefónica.	12
		Recurso humano de soporte #1 Miami.	8
	Externo	Outlook - Office 365.	18
	Externo	Acceso al TFS Source Code.	18
1 - Proceso de desarrollo de Software .net		Servidor de JD Edwards EnterpriseOne.	12
		Servidor de bases de Datos Oracle.	12
		Servidor de bases de datos IBM/400.	12
		Servidor de bases de datos SQL Server.	12
		VPN Telefónica (Miami, USA) - CR - CR- Telefónica (Miami, USA).	16
		Licencia de Visual Studio.	12
		Router Cisco 1900 Series.	10
		Máquina de desarrollo.	12
		JD Edwards EnterpriseOne.	12
		Bases de Datos JD Edwards EnterpriseOne (SQL, IBM, Oracle).	12
	Externo	Team Foundation Server (TFS).	12
	Externo	Internet.	8
2 - Proceso de desarrollo de Software en JD Edwards EnterpriseOne		VPN Telefónica (Miami, USA) - CR - CR- Telefónica (Miami, USA).	16

		Servidor de JD Edwards EnterpriseOne.	12
		SmarterCommerceDB - SQL Server.	12
		Bases de datos JD Edwards EnterpriseOne (SQL, IBM, Oracle).	12
		Máquina de desarrollo.	12
	Externo	Internet.	
29 - Instalación de paquetes de actualización en los clientes		FTP - Repositorio de paquetes de actualización – Telefónica.	16
		VPN al cliente.	12
		Laptop personal para el recurso.	12
	Externo	Team Foundation Server (TFS).	12
36 - Gestión del Active Directory		VPN Telefónica (Miami, USA) - CR - CR- Telefónica (Miami, USA).	18
		Windows server - Active Directory – Telefónica.	12
27 - Comunicación service plus-cliente	Externo	Teams.	12
	Externo	Zoom Conference.	12
	Externo	Office 365.	12
	Externo	Internet.	12
38 - Pruebas sobre desarrollos de mejoras y problemas para el cliente		Servidor Web con aplicaciones para pruebas.	18
		Servidor de bases de datos IBM/400 o Oracle o SQL Server.	16
		Servidor de JD Edwards EnterpriseOne.	14
		Servidor capas del negocio.	16

		SmarterCommerceDB - SQL Server.	16
		Bases de datos JD Edwards EnterpriseOne (SQL, IBM, Oracle).	16
		VPN Telefónica (Miami, USA) - CR - CR- Telefónica (Miami, USA).	10
	Externo	Internet.	8
34 - Instalación de parches en máquinas personales y servidores		Recurso humano de soporte #1 Costa Rica.	18
40 - Comunicación constante entre QA - Gestión de Proyectos	Externo	Teams.	20
	Externo	Zoom Conference.	20
	Externo	Outlook - Office 365.	20
16 - Gestión de planillas(pagos)		Servidor de JD Edwards EnterpriseOne.	20
	Externo	Software @task.	

Tabla 24. Procesos y servicios ordenados por MTD/RTO

Con el fin de identificar únicamente los servicios de TI, se crea la Tabla 25, en donde se encuentra, de forma final, cada uno de los elementos de TI, utilizados por Premier Soluciones, para dar soporte a sus procesos y servicios críticos.

Hardware	
Servidor de JD Edwards EnterpriseOne.	Ubicado en Telefónica data center en Miami.
Servidor de base de datos Oracle.	Ubicado en Telefónica data center en Miami.
Servidor de base de datos IBM/400.	Ubicado en Telefónica data center en Miami.
Servidor de base de datos SQL Server.	Ubicado en Telefónica data center en Miami.

Máquina Windows i7, 16 GB RAM, 1TB Disco Duro.	Máquina de uso personal para el trabajo.
Servidor web - Desarrollo y pruebas.	Máquina utilizada como Web Server. Ubicada en Telefónica para probar desarrollos y realizar los procesos de QA (SCWEBDV).
Servidor de aplicación - Desarrollo y pruebas.	Máquina utilizada como Application Server. Ubicada en Telefónica para probar desarrollos y realizar los procesos de QA (SCAPPDV).
Servidor de producción.	Máquina utilizada para realizar demostraciones a clientes o prospectos. Ubicado en Telefónica data center en Miami.
Software	
Visual Studio – Licencias	Se cuenta con licencias para cada máquina utilizada. Actualmente cada usuario se autentica por medio del active directory de Premier Soluciones (TPGNET).
Team Foundation Server	Sirve como repositorio de Código Fuente, además manejo de proyectos de software. Actualmente cada usuario se autentica por medio del active directory de Premier Soluciones (TPGNET).
SQL Server Client, Oracle Client, iSeries client	Clientes gratuitos de conexión a servidores de base de datos.
Office 365(Word, Excel, Outlook, Power point, Teams).	El equipo ofimático lo utiliza cada miembro de la organización, el correo de la compañía es manejado mediante Office 365, al igual que la aplicación de comunicación como lo es TEAMS y Skype for Business. Actualmente cada usuario se autentica por medio del active directory de Premier Soluciones (TPGNET).
VPN	En la oficina existe un único VPN que conecta a Costa Rica con Telefónica Miami, en caso de trabajo en casa se necesita un usuario de VPN personal para utilizar Cisco AnyConnect.
JD Edwards EnterpriseOne.	Es necesario para los desarrolladores la utilización de ese software ya que es el core de la funcionalidad.
Telecomunicaciones	

Router Cisco 1900 Series.	Router encargado de la comunicación entre la oficina de Miami y Telefónica en Miami, US. Además, este router trabaja como VPN el cual crea una comunicación por un canal privado. Existe uno de estos en CR y otro en Telefónica.
Internet.	En Costa Rica se cuentan con dos enlaces de internet con la compañía American Data, cada enlace en una localización geográfica diferente, además entrando y saliendo de Costa Rica también por lugares diferentes.
Switch 3COM	Encargado de distribuir el enlace de internet dentro de la oficina de Premier Soluciones

Tabla 25. Elementos de TI que soportan los procesos críticos de Premier Soluciones

En caso de un desastre, sea natural o causado por el hombre, que afecte la continuidad del servicio de Premier Soluciones por alguno de sus elementos de TI, se debe seguir el siguiente esquema de recuperación.

5.6.1 Azure active directory

Premier Soluciones con la licencia de Microsoft Azure de Office 365 ya cuenta con el Active Directory completamente sincronizado en la nube, tal y como lo está on-Premises. Con esto se facilita la gestión de usuarios, roles y permisos y va a permitir, además, acceder la infraestructura virtual de Azure de una forma segura, para cada uno de los colaboradores de Premier Soluciones. La Figura 17 es la solución de arquitectura propuesta en este trabajo, para manejar la autenticación a los recursos de Azure; esto, por medio del ya migrado Active Directory con el fin de utilizar los mismos usuarios del dominio premierway.com, para conducir los accesos.

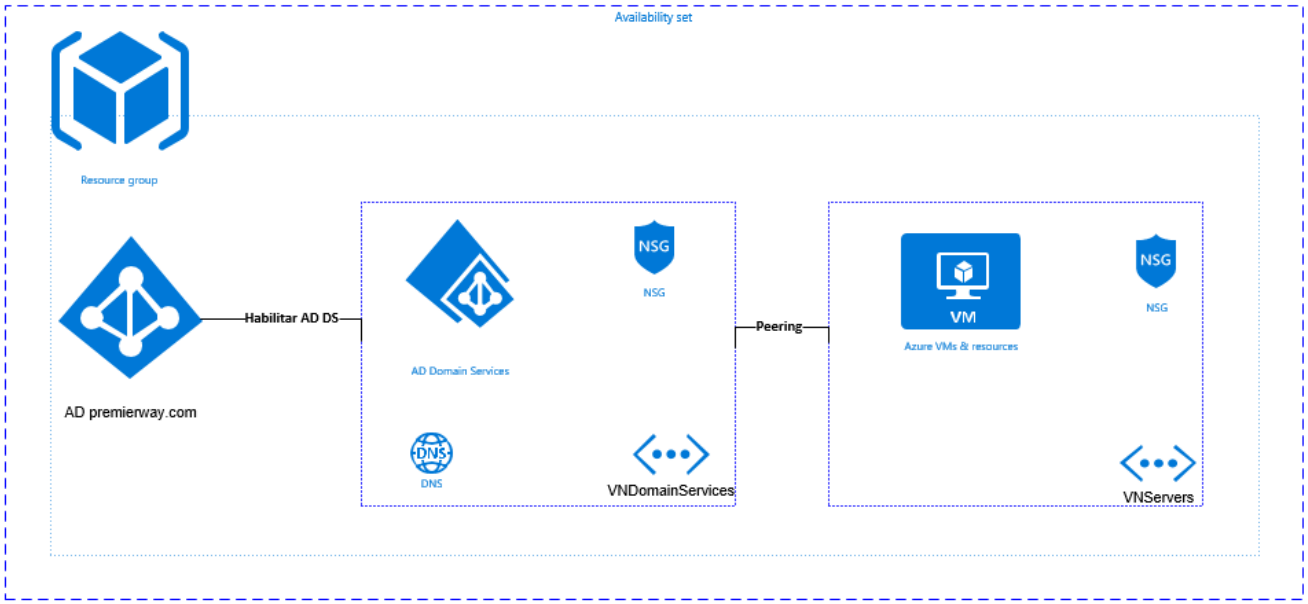


Figura 17. Active Directory, infraestructura en la nube

En la FIGURA 16 se pueden denotar los siguientes puntos:

1. Por políticas de Premier Soluciones todos sus procesos se deben manejar en el idioma inglés, por consiguiente, las opciones en Azure por la configuración de las maquinas donde se va a realizar el proceso se muestran en inglés, con lo cual, en esta guía, las opciones de menú se describen en ese idioma.
2. Se debe ingresar al sitio https://portal.azure.com con un usuario administrador con permisos para crear recursos.
3. Migración del active directory on-Premises

Se cuenta con un *active directory on-Premises llamado premierway.com*, sincronizado en la nube de Azure, con todos sus usuarios, roles y permisos. En la FIGURA 18, se ven algunos de los usuarios ya sincronizados en Azure.

Figura 18. Azure AD Premier Soluciones

Según la documentación de Azure, en su página (Microsoft Azure, 2019), lo siguiente es una recomendación a la hora de utilizar su active directory.

Procedimiento recomendado: Activación de la sincronización de hashes de contraseñas.

Detalles: La sincronización de hashes de contraseñas es una característica que se utiliza para sincronizar los hashes de los hashes de las contraseñas de los usuarios, desde una instancia de Active Directory local con una instancia de Azure AD en la nube.

Para la solución propuesta, es requisito esta sincronización de hashes, que permite tener una opción si los servidores locales sufren un error o dejan de estar disponibles temporalmente. Esto permite que los usuarios inicien sesión en el servicio con la misma contraseña que usan para iniciar sesión en su instancia local de Active Directory. También permite que Identity Protection detecte las credenciales que están en peligro, mediante la comparación de los algoritmos hash de dichas contraseñas, con contraseñas que se sepa que están en peligro, si un usuario ha usado su misma dirección de correo electrónico y contraseña en otros servicios que no estén conectados a Azure AD.

4. Se debe crear un grupo de recursos en Azure, con el fin de agrupar los recursos que se van a utilizar para esta solución, se propone el nombre de *“recoverygroup”.*
5. Se debe crear un Network Security Group por sus siglas en inglés NSG, para la red de dominio; se propone como nombre *“nsgdomainservices*”; crea reglas que permitan la entrada y salida de datos de esta red.
6. Se debe crear un Network Security Group para la red de servidores; se propone como nombre *“nsginternalservers*”, que permite crear reglas para la entrada y salida de datos de esta red. En este NSG se debe restringir la conexión a los servidores por *ips* públicos.
7. Se debe crear una red virtual de Azure (VN, por sus siglas en inglés) llamada *VNDomainServices*, en la que deben ubicarse los servicios de dominio; se debe agregar a este VN el NSG, creado anteriormente con el nombre de nsgdomainservices.
8. Se debe crear un Virtual Network llamado *VNServers*, en el cual estarán los servidores que involucran el core del negocio de Premier Soluciones; se debe agregar a este VN el NSG creado anteriormente con el nombre de nsginternalservers.

9. Se debe permitir la comunicación entre las redes virtuales VNDomainServices y VNServers por medio de un Azure Virtual Network Peering. La separación de las redes da a permitir ser más granular en la infraestructura, además de facilitar al administrador de la red aplicar seguridad a cada una de las redes, si así es requerido o dependiendo de los objetivos corporativos.
10. Se debe habilitar la opción de Active Directory Domain Service, para el dominio premierway.com en la nube de Azure; este va a estar separado de la demás infraestructura de por medio, del VN llamado VNDomainServices. Con la habilitación de esta funcionalidad Azure Active Directory Domain Service, Premier Soluciones, tendrá su controlador de dominio en Azure, sin la necesidad de implementar un servidor de dominio; si es necesario dar mantenimiento desde la nube, se deberá crear un servidor Windows dentro del VN, llamado VNDomainServices.

Se debe conocer que una vez se encuentre esta infraestructura creada en Azure, el administrador de la red podrá manejar el acceso de los recursos, mediante los roles y permisos que se manejan con la infraestructura on-Premises; por ello es transparente debido a que la migración del active directory incluyó todos los roles, permisos y usuarios.

5.6.2 VPN para acceso a recursos

Con el fin de proteger el acceso a los recursos de Azure, creados dentro de las redes virtuales VNDomainServices y VNServers, se propone, de manera opcional, una conexión VPN Point-to-Site, que permita, en caso de desastre, la utilización de este, para conectarse de una forma segura a la infraestructura en Azure.

En la FIGURA 19 se observa cuál va a ser la función del VPN y dónde se va a ubicar. Se puede ver que el VPN va a estar ligado directamente a la VNet, llamada VNServers. Esto va a permitir la conexión a sus recursos de un colaborador de Premier Soluciones desde su casa, de forma segura, por medio del VPN.

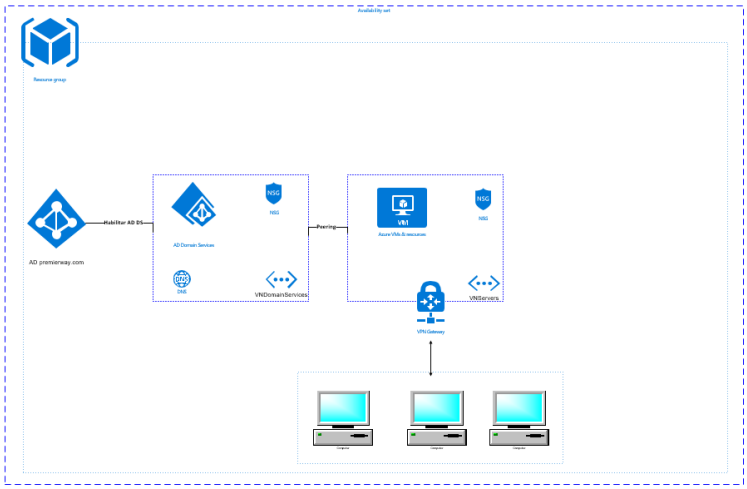


Figura 19. VPN Point to Site

Los siguientes son los pasos por seguir para la creación de la conexión VPN a la infraestructura de Premier Soluciones.

1. Por políticas de Premier Soluciones todos sus procesos se deben manejar en el idioma inglés, por consiguiente, las opciones en Azure por la configuración de las maquinas donde se va a realizar el proceso se muestran en inglés, con lo cual, en esta guía, las opciones de menú se describen en ese idioma.
2. Se debe ingresar al sitio https://portal.azure.com con un usuario administrador con permisos para crear recursos.
3. Se debe agregar cada recurso creado dentro del “recoverygroup”, previamente creado.
4. Abrir la VNet llamada VNServers.
    i Agregar el espacio de direcciones.
5. Crear un recurso en Azure llamado Virtual Network Gateway con las siguientes características:
    i VPN Type: Route-based.
    ii Gateway Type: VPN.
    iii Virtual network: VNServers.
    iv SKU: VpnGW3 para más de 30 usuarios con mayor rendimiento.
    v Agregar un certificado emitido por una CA valida.
    vi Tunnel Type: seleccionar ambos para soportar usuarios Mac y usuarios Windows.

vii Authentication Type: Azure certifícate.

viii El certificado cliente (.pfx) debe ser instalado en las maquinas que están autorizadas a tener acceso a la infraestructura Azure.

ix Cada usuario con acceso por medio de Active Directory al portal de Azure deberá descargar el VPN.

- En Azure seleccione el Virtual Network Gateway creado.
- En la opción Point-to-Site configuración, seleccione la opción "Download VPN Client", dependiendo su arquitectura.
- El VPN debe ser instalado en las máquinas autorizadas.

5.6.3 Infraestructura virtual en Telefónica

Se utiliza la suscripción Azure. En esta sección se desarrolla la migración de la infraestructura virtual ubicada en Telefónica de Miami, US. Los servidores están en un Virtual Network, separado al controlador de dominio, con sus propias reglas de acceso. Por motivos de seguridad, los servidores dentro de este Virtual Network no tendrán un ip público asignado y solamente podrán ser accedidos por medio de un VPN.

Los servidores nombrados en la Tabla 26 representan parte de la infraestructura existente en Telefónica y que, mediante estrategias, va a ser adaptadas a Azure, dentro del virtual network mencionado.

Hardware
Servidores de JD Edwards EnterpriseOne • Deployment Server. • Server Manager. • Enterprise Server. • Web Server (Web Logic).
Servidor de base de datos Oracle.
Servidor de base de datos IBM/400.
Servidor de base de datos SQL Server.
Servidor Web (desarrollo y pruebas).
Servidor de aplicación (desarrollo y pruebas).

Servidor de Producción.

Tabla 26. Servidores en Telefónica

Los servidores que conforman una arquitectura típica de un ambiente de JD Edwards EnterpriseOne en Premier Soluciones. Está compuesta por un deployment server, server manager, web server y enterprise server, que dan la funcionalidad principal del negocio. Es de ellos donde nace todo el core, las aplicaciones de Premier Soluciones, en donde su ventaja sobre las demás empresas es poder conectar en tiempo real con las bases de datos de este ERP de una forma amigable y transparente, tal y como hoy se comporta una aplicación de comercio electrónico como Amazon, eBay, entre otros.

Estos servidores actualmente funcionan con las características mínimas; se pueden observar sus especificaciones en la FIGURA 20.

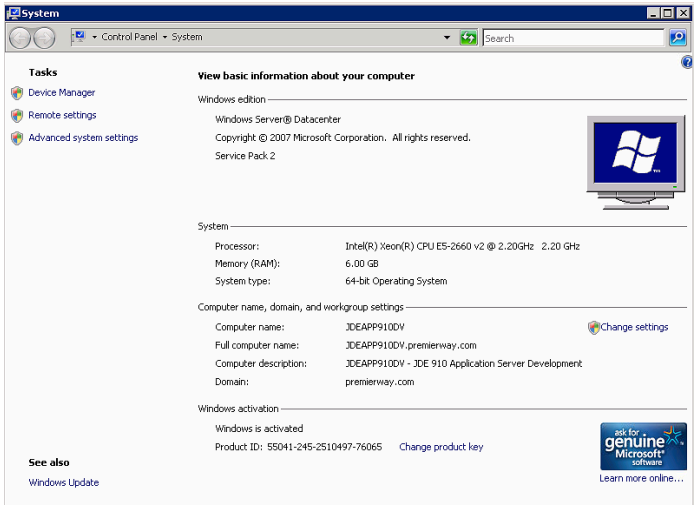


Figura 20. Características de un servidor JD Edwards

Para una mejor comprensión, la infraestructura JD Edward EnterpriseOne E920, de Premier Soluciones, cuenta con la estructura definida en la Figura 21.

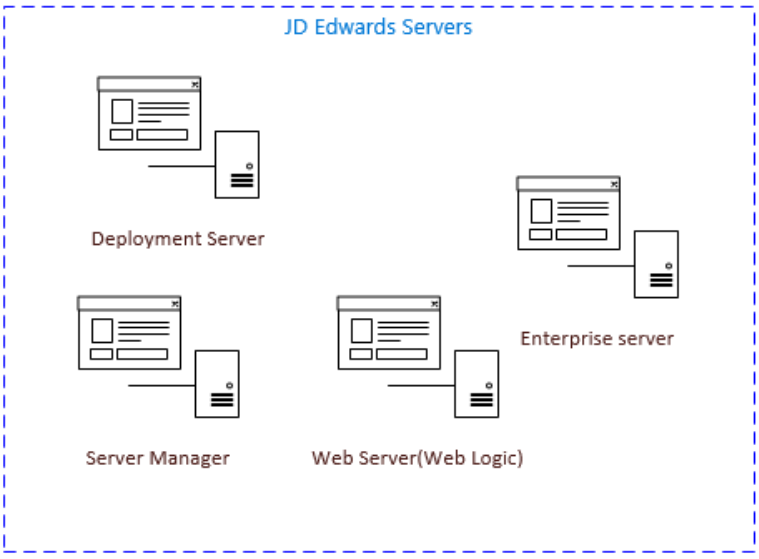


Figura 21. JD Edwards Servers

Se puede decir que el **enterprise server** es el encargado de administrar todo lo que pasa en JDE, tanto a nivel transaccional como a nivel de objetos. Todos los movimientos que se realizan con los datos de JD Edwards, pasan por este server y todo lo referente a los objetos de Edwards (creación de objetos nuevos, modificaciones a los objetos ya existentes y su eliminación). Hasta que dichas modificaciones no se apliquen o sincronicen con este server, no se ven reflejados en la funcionalidad e interfaz del usuario final.

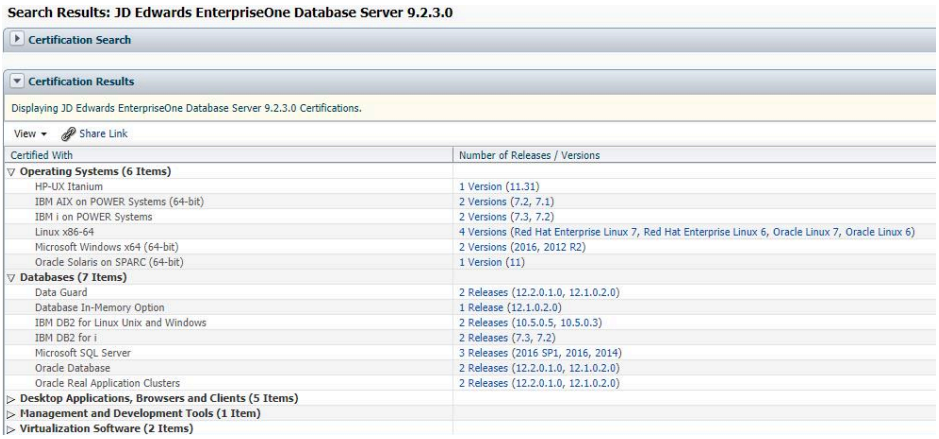
El **deployment server**, es el servidor por medio del cual se realizan algunas tareas de administración de JDE. En otras palabras, es la interfaz gráfica por medio de la cual se realizan las tareas de administración de datos, usuarios, seguridad y objetos, cuando estos últimos se modifican. Por medio del deployment server es que se aplican o se suben estos cambios al Enterprise server por medio de un full package o update package.

El **server manager** es un servidor de administración de la infraestructura de los servers de JD Edwards; por medio de este es que se aplican algunas actualizaciones como los tool releases, más conocidos como versiones. También se configuran algunos aspectos de comunicación entre servidores como puertos, funcionalidades específicas de cada servidor y pocos aspectos de seguridad.

El **Web Server**, Premier Soluciones utiliza el un Windows Server en donde tiene el *Weblogic.* Este tiene la funcionalidad de servidor de publicación de los clientes web, para acceder a JD Edwards, desde un navegador web; funciona como un IIS de Microsoft, pero propiedad de Oracle.

Conociendo la infraestructura actual, se puede comenzar a crear una réplica en la nube; en la migración de estas máquinas a la nube, se descarta la reutilización de los recursos existentes en Telefónica. Se recomienda la creación de una instalación desde 0, debido a principalmente a la cantidad de instalaciones y ambientes localizados en esos servidores y además la obsolescencia del sistema operativo (Windows Server) utilizado en estos servidores, que podría representar una vulnerabilidad de seguridad.

Con el fin de construir un set de servidores óptimo para el desarrollo, se optó por elegir la última versión 9.2.3.0 de JD Edwards EnterpriseOne, sobre la cual Premier Soluciones realiza sus nuevos desarrollos. No se van a soportar múltiples versiones de JD Edwards EnterpriseOne en nuestra infraestructura en la nube, debido a Oracle siempre impulsa sus clientes a moverse a versiones más recientes, la complejidad de estas instalaciones. No existe una necesidad real, porque con una sola versión, el equipo de desarrollo puede trabajar sin ningún problema. Esto ahorra tiempo de instalación y recursos. Según (Oracle Support, 2014), la versión de JD Edwards EnterpriseOne 9.2.3.0 permite su instalación en ambientes con las características vistas en la FIGURA 21.



Search Results: JD Edwards EnterpriseOne Database Server 9.2.3.0

Certification Search

Certification Results

Displaying JD Edwards EnterpriseOne Database Server 9.2.3.0 Certifications.

View ▾ Share Link

Certified With	Number of Releases / Versions
Operating Systems (6 Items)	
HP-UX Itanium	1 Version (11.31)
IBM AIX on POWER Systems (64-bit)	2 Versions (7.2, 7.1)
IBM i on POWER Systems	2 Versions (7.3, 7.2)
Linux x86-64	4 Versions (Red Hat Enterprise Linux 7, Red Hat Enterprise Linux 6, Oracle Linux 7, Oracle Linux 6)
Microsoft Windows x64 (64-bit)	2 Versions (2016, 2012 R2)
Oracle Solaris on SPARC (64-bit)	1 Version (11)
Databases (7 Items)	
Data Guard	2 Releases (12.2.0.1.0, 12.1.0.2.0)
Database In-Memory Option	1 Release (12.1.0.2.0)
IBM DB2 for Linux Unix and Windows	2 Releases (10.5.0.5, 10.5.0.3)
IBM DB2 for i	2 Releases (7.3, 7.2)
Microsoft SQL Server	3 Releases (2016 SP1, 2016, 2014)
Oracle Database	2 Releases (12.2.0.1.0, 12.1.0.2.0)
Oracle Real Application Clusters	2 Releases (12.2.0.1.0, 12.1.0.2.0)
Desktop Applications, Browsers and Clients (5 Items)	
Management and Development Tools (1 Item)	
Virtualization Software (2 Items)	

Figura 22. Compatibilidad de infraestructura según Oracle Support

Con base en la FIGURA 22, y, según (Oracle Support, 2014), para la versión 9.2.3.0 se certifica el funcionamiento de cada una de sus partes sobre la siguiente infraestructura, basado en Windows Servers debido a que Azure maneja las opciones y además el personal técnico de Premier Soluciones cuenta con amplia experiencia en el mundo Microsoft. En la Tabla 28, se pueden ver las posibles configuraciones para nuestra migración a la nube.

	Windows server de x64 2016	Windows server de x64 2012 R2
Microsoft SQL Server 2016 SP1.	X	
Microsoft SQL Server 2016.	X	X
Microsoft SQL Server 2014.	X	X
Oracle Database 12.2.0.1.0.	X	X
Oracle Database 12.1.0.2.0.		X

Tabla 28. Configuraciones JDE 9.2.3.0

En la Tabla 28 se puede mostrar como por ejemplo que la base de datos "Microsoft SQL Server 2016 SP1", es compatible con "Windows server de x64 2016", que el "Oracle Database 12.2.0.1.0" es compatible con "Windows server de x64 2016 y Windows server de x64 2012 R2".

Por otro lado, para la base de datos IBM, se cuenta con las siguientes configuraciones, según (Oracle Support, 2014):

- IBM DB2 for i 7.3 on IBM i on POWER Systems 7.3.
- IBM DB2 for i 7.2 on IBM i on POWER Systems 7.2.

5.6.3.1 Servidor de base de datos Oracle

Tomando en cuenta la información anterior, principalmente la Tabla 28, se debe replicar la base de datos Oracle, versión 12.1.0.2.0, ligada al ambiente E920, existente en Telefónica, con el fin de que la nueva instalación de JD Edwards se comunique con esta como primer base de datos, para seguir con la naturalidad Oracle de este ERP.

Cabe resaltar que Premier Soluciones actualmente cuenta con una Red de Área de Almacenamiento (SAN, por sus siglas en inglés), que genera respaldos de las bases de datos y *snapshops* de los servidores, uno al final de cada día. Adicional, hay otro respaldo almacenado en cintas físicas en una localización geográfica distinta; por ello, el proceso de respaldo es un procedimiento ya definido dentro de Premier Soluciones para su resguardo de información.

Con el fin de realizar la operación lo más rápido posible, se utiliza la funcionalidad de Azure Site Recovery, que es una tecnología que permite hacer una sincronización de los servidores de Premier Soluciones, ubicados en el centro de datos de Telefónica en Miami, sobre el servidor de Hyper-V; con esto se tendrán los servidores replicados en la nube y

actualizados en siempre. Los siguientes son los pasos por seguir dentro de Azure, para realizar la inclusión del servidor Oracle ubicado en Telefónica:

1. Por políticas de Premier Soluciones todos sus procesos se deben manejar en el idioma inglés, por consiguiente, las opciones en Azure por la configuración de las maquinas donde se va a realizar el proceso se muestran en inglés, con lo cual, en esta guía, las opciones de menú se describen en ese idioma.
2. Para mayor facilidad se debe realizar este procedimiento sobre el servidor Hyper-V que alberga la infraestructura ubicado en Telefónica.
3. Se debe ingresar al sitio https://portal.azure.com con un usuario administrador con permisos para crear recursos.
4. Se debe agregar cada recurso creado, dentro del *"recoverygroup",* previamente creado.
5. Se debe utilizar la cuenta de almacenamiento, previamente creada, llamada *"premiergroupstorage"*.
6. Se debe agregar el sitio de recuperación de Azure, dentro del menú *New->Storage->Backup and Site Recovery (OMS)*.
7. Una vez creado este recurso, se debe ingresar a él y dentro ingresar a la opción *"Site Recovery*".
8. El siguiente paso consiste en preparar la infraestructura por migrar; desde Telefónica hasta Azure, se debe seleccionar esta configuración Hyper-V hasta Azure.
    i Se debe agregar un nuevo sitio Hyper-V, que corresponderá al servidor Hyper-V ubicado en Telefónica.
    ii Dentro del sitio Hyper-V, se debe agregar el servidor Hyper-V y descargar el instalador de "Microsoft Azure Site Recovery", en el servidor de Hyper-V en Telefónica y será el encargado de la comunicación entre ambos elementos, por medio de un agente. Se debe descargar la llave de registro que liga el *Hyper-V on-Premises* con el Hyper-V, en Azure previamente creado.

iii En el proceso de instalación del “Microsoft Azure Site Recovery” este le va a solicitar la “Llave de Registro”, previamente descargada, sin ella el proceso no puede continuar.

iv Dentro del proceso de instalación, se debe asegurar marcar la opción de *“Conectar directamente a Azure Site Recovery sin necesidad de un servidor proxy”.*

v Una vez instalado el software, la conexión entre Azure y la infraestructura on-Premises, está lista. Se debe ingresar a Azure y seleccionar el sitio de recuperación; dentro de este debemos buscar la opción *“Site Recovery. Infrastructure ->Hyper-V Hosts”;* es en este lugar donde se verificará el estado actual de la inclusión de la conexión, la cual debe decir *“Connected”.*

vi El siguiente paso será crear la política de migración, en la cual se deben definir tiempos; por ejemplo, de cada cuanto tiempo se debe sincronizar el servidor on-Premises con Azure; debido a que el RPO de los datos en los procesos críticos descritos en el BIA es un máximo de 24 horas, se recomienda configurar tiempo debajo de este rango.

9. Consiste en replicar las máquinas virtuales que deseamos del Hyper-V on-Premises a Azure.

i La interfaz del sito de recuperación Azure es muy amigable y les guiará en el proceso. Hay cosas importantes por conocer, como por ejemplo este servidor de Oracle debe ser incluido en el Azure Virtual Network llamado VNServers y se debe seleccionar la cuenta de almacenamiento, previamente creada.

ii Azure, muestra las máquinas virtuales que están en Hyper-V on-Premises, para seleccionar las que se desea mover; en este caso se debe seleccionar el servidor donde se encuentra la base de datos Oracle 12.1.0.2.0, en la instancia de JD Edwards EnterpriseOne E920, llamado *“JDEORADV”.*

iii Dentro del sitio de recuperación en la opción “Replicated ítems” se puede ver el estatus de las virtuales migradas.

5.6.3.2 Servidor de base de datos Microsoft SQL Server

De acuerdo con la Tabla 28, se debe replicar la base de datos Microsoft SQL Server, versión 2014, ligada al ambiente E920, existente en Telefónica. Su objetivo es que la nueva instalación de JD Edwards se comunique con esta, como base de datos alternativa a la de Oracle; se recuerda que Premier Soluciones brinda sus soluciones en Oracle, Microsoft SQL Server y DB2. Ya se cuenta con una Red de Área de Almacenamiento (SAN, por sus siglas en inglés), que genera respaldos de las bases de datos y *snapshops* de los servidores, uno al final de cada día; adicional hay otro respaldo almacenado en cintas físicas en una localización geográfica distinta.

Al igual que con la base de datos, con Oracle se va a utilizar la misma funcionalidad de Azure Site Recovery, para replicar los servidores on-Premises dentro de Azure Site Recovery, previamente creado. Los siguientes son los pasos por seguir dentro de Azure para realizar la inclusión del servidor, donde se encuentra la base de datos SQL Server, vinculada al ambiente E920.

1. Por políticas de Premier Soluciones todos sus procesos se deben manejar en el idioma inglés, por consiguiente, las opciones en Azure por la configuración de las maquinas donde se va a realizar el proceso se muestran en inglés, con lo cual, en esta guía, las opciones de menú se describen en ese idioma.
2. Para mayor facilidad se debe realizar este procedimiento sobre el servidor Hyper-V, que alberga la infraestructura ubicada en Telefónica.
3. Se debe ingresar al sitio https://portal.azure.com, con un usuario administrador, con permisos para crear recursos.
4. Se debe agregar cada recurso, dentro del “Grupo de Recursos” previamente creado, llamado “recoverygroup”.
5. Se debe utilizar la cuenta de almacenamiento previamente creada, llamada “premiergroupstorage”.
6. Se debe seleccionar el sitio de recuperación de Azure, previamente creado; este se encuentra dentro del “recoverygroup”.

7. Se debe seleccionar la opción Site Recovery->Replicate Application, para agregarla el servidor Windows, en donde está el role de SQL Server, conectado al ambiente E920.
8. Dentro del sitio de recuperación en la opción “Replicated Ítems”, se puede ver el estatus de las virtuales migradas.

5.6.3.3 Servidores de JD Edwards EnterpriseOne

Como elección, decide crear la siguiente infraestructura en Windows Server 2012 debido a un tema de soporte de Oracle; la principal razón es que la base de datos Oracle actual se encuentra en versión 12.1.0.2.0, que es soportada por este sistema operativo solamente, según (Oracle Support, 2014). Serán dos máquinas creadas en Azure con requisitos básicos mínimos, para este caso y debido a la obsolescencia de las máquinas virtuales actuales se decide migrar de SO; con esto la utilización de Azure Recovery Site no aplica.

1. Se debe ingresar al sitio https://portal.azure.com con un usuario administrador con permisos, para crear recursos.
2. Se debe agregar cada recurso creado dentro del Grupo de Recursos, previamente creada, llamada “recoverygroup”.
3. Se debe utilizar la cuenta de almacenamiento, previamente creada, llamada “premiergroupstorage”.
4. No se recomienda la creación de un ip público, debido a que estos servidores son de acceso privado y serán accedidos por medio de su ip interno.
5. La máquina virtual debe estar dentro del Virtual Network de Azure llamado VNServers.
6. Azure te ofrece el servidor con la licencia, sin embargo, Premier Soluciones puede optar por adquirir la licencia con Microsoft y ahorrar presupuesto.
7. Se recomienda un disco duro de estado sólido para un mejor rendimiento, pero no es requerido; este debe ser, al menos, 256 GB.
8. Se recomienda, al menos, un procesador de dos núcleos para ambos servidores.
9. El primer servidor para crear se debe llamar SCDEP920DVAZ y funciona como Deployment Server y Server Manager; esto quiere decir que tendría ambos roles.

10. El segundo servidor para crear se debe llamar JDEAPP920DVAZ y va a funcionar como Enterprise Server y Web Server (Web Logic); quiere decir que tendría ambos roles.
11. El servidor SCDEP920DVAZ, JDEAPP920DVAZ debe ser agregado al dominio “premierway.com”, creado anteriormente en Azure.
12. Los accesos a estos servidores por medio del dominio se manejarán como ya se manejan, on-Premises, debido a que el AD fue migrado con todos sus roles, usuarios y permisos.
13. Se debe iniciar sesión en ambos servidores con el usuario administrador configurado.
14. Para cada uno de los servidores el IP debe ser estático y puede ser el mismo de la infraestructura on-Premises.
15. Se debe configurar una nueva instalación de JD Edwards EnterpriseOne 9.2.3.0 E920 completa, al dividir los roles, como se describió anteriormente.
16. Se inicia primeramente ligando JD Edwards con la base de datos migrada antes de Oracle, posteriormente con Microsoft SQL Server; esto quiere decir que la nueva instalación de JD Edwards, se comunicará con una réplica de bases de datos on-Premises, copiadas a la nube. Con esto, la configuración del ERP será más fácil debido a que ya hay configuraciones existentes.
17. Los datos de conexión a la BD van a cambiar de acuerdo con el nombre elegido, cuando se migró la base de datos Oracle y SQL Server; en este caso cambiaría el nombre del servidor solamente.

5.6.3.4 Servidor de aplicación utilizado para desarrollo y pruebas

Este es un servidor Windows 2012, que se encuentra en el servidor Hyper-V ubicado en Telefónica, que contiene un IIS en el cual es alojada la capa de negocio en inglés conocido como Business Layer. Este es el encargado de recibir peticiones del servidor web y obtener la información de la base de datos para devolver la petición con la información solicitada; en otras palabras, el orquestador entre el web y la base de datos. Al cumplir con los requisitos de migración al Azure Recovery Site, se elige esta como la estrategia de migración adecuada. Los siguientes son los pasos necesarios para la migración de esta máquina virtual al Azure Recovery Site:

1. Por políticas de Premier Soluciones todos sus procesos se deben manejar en el idioma inglés, por consiguiente, las opciones en Azure por la configuración de las maquinas donde se va a realizar el proceso se muestran en inglés, con lo cual, en esta guía, las opciones de menú se describen en ese idioma.
2. Para mayor facilidad se debe realizar este procedimiento sobre el servidor Hyper-V que alberga la infraestructura ubicada en Telefónica.
3. Se debe ingresar al sitio https://portal.azure.com, con un usuario administrador, con permisos para crear recursos.
4. Se debe agregar cada recurso creado dentro del grupo de Recursos previamente creado, llamado “recoverygroup”.
5. Se debe utilizar la cuenta de almacenamiento previamente creada, llamada “premiergroupstorage”.
6. Se debe seleccionar el sitio de recuperación de Azure previamente creado; este se encuentra dentro del “recoverygroup”.
7. Se debe seleccionar la opción Site Recovery->Replicate Application para agregar el servidor Windows, en donde están conectados los BL, a los que se debe conectar el servidor web, actualmente este servidor es llamado SCAPPDV.
8. Dentro del sitio de recuperación en la opción “Replicated Ítems” se puede ver el estatus de las virtuales migradas.

5.6.3.5 Servidor de web utilizado para desarrollo y pruebas

Este es un servidor Windows 2012 utilizado para mantener las aplicaciones web de Premier Soluciones como eCommerce, CMS, POS y Management Console, con acceso tanto para desarrolladores, como para el personal de QA. Este servidor cuenta con múltiples entradas en su IIS que permiten tener diferentes sitios para los diferentes ambientes en un mismo servidor. Por su arquitectura, cada sitio web se comunica con otro servidor que administra de igual forma la capa de negocios y se encarga de orquestar la comunicación entre la capa de negocios y los datos. Este servidor alberga decenas de sitios web de acceso restringido a los colaboradores dentro del dominio de premierway.com. Los siguientes son los pasos necesarios para la migración de este servidor virtual al Azure Recovery Site, creado anteriormente:

1. Por políticas de Premier Soluciones todos sus procesos se deben manejar en el idioma inglés, por consiguiente, las opciones en Azure por la configuración de las maquinas donde se va a realizar el proceso se muestran en inglés, con lo cual, en esta guía, las opciones de menú se describen en ese idioma.
2. Para mayor facilidad se debe realizar este procedimiento sobre el servidor Hyper-V que alberga la infraestructura ubicado en Telefónica.
3. Se debe ingresar al sitio https://portal.azure.com, con un usuario administrador con permisos para crear recursos.
4. Se debe agregar cada recurso creado dentro del grupo de recursos, previamente creado, llamado *"recoverygroup".*
5. Se debe utilizar la cuenta de almacenamiento, previamente creada, llamada *"premiergroupstorage".*
6. Se debe seleccionar el sitio de recuperación de Azure, previamente creado.
7. Se debe seleccionar la opción *Site Recovery->Replicate Application,* para agregar el servidor Windows en donde están alojados los sitios web, actualmente este servidor es llamado SCWEBDV.
8. Dentro del sitio de recuperación en la opción "Replicated Ítems" se puede ver el estatus de las virtuales migradas.

5.6.3.6 Servidor de producción

Este es un servidor Windows 2012, utilizado para mantener las aplicaciones web de Premier Soluciones como: eCommerce, CMS, POS y Management Console, para realizar pruebas o demostraciones a clientes. Es un servidor donde QA y desarrolladores no tienen acceso y cuenta con múltiples entradas en su IIS que permiten tener diferentes sitios con diferentes diseños dependiendo del cliente al cual se vaya a presentar. Por su arquitectura y al ser un servidor para demostraciones, los sitios web y la capa de negocios se encuentran en el mismo servidor, a diferencia de la arquitectura de desarrollo y QA.

Los siguientes son los pasos necesarios para la migración de este servidor al Azure Recovery Site, creado anteriormente:

1. Por políticas de Premier Soluciones todos sus procesos se deben manejar en el idioma inglés, por consiguiente, las opciones en Azure por la configuración de las

maquinas donde se va a realizar el proceso se muestran en inglés, con lo cual, en esta guía, las opciones de menú se describen en ese idioma.

2. Para mayor facilidad se debe realizar este procedimiento sobre el servidor Hyper-V que alberga la infraestructura ubicada en Telefónica.
3. Se debe ingresar al sitio https://portal.azure.com, con un usuario administrador con permisos para crear recursos.
4. Se debe agregar cada recurso creado dentro del “Grupo de Recursos”, previamente creado, llamado “recoverygroup”.
5. Se debe utilizar la cuenta de almacenamiento, previamente creada, llamada “premiergroupstorage”.
6. Se debe seleccionar el sitio de recuperación de Azure, previamente creado.
7. Se debe seleccionar la opción Site Recovery->Replicate Application, para agregar el servidor Windows, en donde están alojados los sitios web y capa de negocio, actualmente este servidor es llamado SCDEMO.
8. Dentro del sitio de recuperación en la opción “Replicated Items” se puede ver el estatus de las virtuales migradas.

5.6.4 Máquinas virtuales para colaboradores

Dentro de la plataforma Azure se deben crear máquinas virtuales de desarrollo que tengan instalado todo el software necesario para ejecutar las funciones máximas de un desarrollador. La máquina virtual debe ser un Windows 10, de al menos 128 GB de almacenamiento y se utilizará una licencia de Premier Soluciones. Esta máquina debe ser creada dentro el VNet llamado VNServers. Los siguientes pasos deben ser ejecutados sobre estas máquinas virtuales:

1. Crear cinco de estas máquinas.
2. Colocarles un IP fijo.
3. Hay que asegurar que no tengan un IP público.
4. Incluir la máquina al dominio y asignarla a un grupo definido en el Active Directory.
5. Realizar pruebas de conectividad de las máquinas virtuales contra los servidores, desde un sitio remoto.

5.6.5 Recuperación del Software

Con la migración del active directory on-Premises a la nube de Azure Premier Soluciones, se obtuvo el manejo de todo el software, necesario para su continuidad; queda solamente dependiente de una conexión a internet. La autenticación a las aplicaciones es por medio del mismo usuario del active directory.

Aplicaciones manejadas por Azure:

- Team Foundation Server.
- Office 365 (Word, Excel, Outlook).
- Teams.
- Skype for business.
- Visual Studio.

5.6.6 Recuperación de la infraestructura de Telecomunicaciones

Con la implementación de la infraestructura en la nube de Azure el hardware encargado de la comunicación on-Premises queda completamente sin uso alguno.

- Router Cisco 1900 Series.
- Switch 3COM.

5.6.7 Creación de infraestructura en Azure

El objetivo de este paso es unir todas las piezas involucradas en las acciones antes mencionadas, para lograr ejecutar el plan con éxito. Cabe resaltar que estos pasos guiarán a la persona encargada a la creación de la infraestructura en la nube.

1. Ejecución de pasos para configuración del active directory en la sección previamente mencionada con el título Azure active directory.
    - i Se recomienda validar algunos pasos de seguridad que pueden aplicarse sobre el active directory, con el fin de robustecer la seguridad en la siguiente referencia (Microsoft Azure, 2018).
2. Migración del servidor de base de datos Oracle en el sitio de recuperación de Azure, mediante los pasos creados anteriormente.
3. Migración del servidor de base de datos Microsoft SQL Server en el sitio de recuperación de Azure, mediante los pasos creados anteriormente.

4. Migración del servidor de aplicación utilizado para desarrollo y pruebas en el sitio de recuperación de Azure, mediante los pasos creados anteriormente.
5. Migración servidor de web utilizado para desarrollo y pruebas en el sitio de recuperación de Azure, mediante los pasos creados anteriormente.
6. Migración del servidor de producción pruebas en el sitio de recuperación de Azure, mediante los pasos creados anteriormente.
7. Lo siguiente será crear un plan de recuperación oficial para levantar la infraestructura creada en el sitio de recuperación de Azure, siguiendo algunos pasos indicados por Azure en su página web (Microsoft Azure, 2018). El plan deberá incluir los siguientes puntos.
    i Levantar la máquina virtual de Oracle.
    ii Levantar la máquina virtual de Microsoft SQL Server.
    iii Levantar la máquina virtual del servidor de aplicación utilizado para desarrollo y pruebas.
    iv Levantar la máquina virtual servidor de web utilizado para desarrollo y pruebas.
    v Levantar la máquina virtual del servidor de producción.
8. Una vez creado el plan de recuperación del sitio, se debe ejecutar el plan para levantar los recursos.
    i Se debe configurar un ip estático a cada una de las máquinas virtuales del sitio de recuperación de Azure.
    ii Se debe ingresar a cada una de máquinas virtuales del sitio de recuperación de Azure e incluirlas en el dominio.
9. Sobre el servidor de aplicación, cada entrada en el IIS está relacionada a un BL; este, a su vez, tiene su Web.Config, en donde se especifican los datos de conexión a JD Edwards y la conexión a la base de datos. Estos valores deben ser reasignados hacia el servidor de JD Edwards y Oracle o SQL Server, de la infraestructura creada en la nube.
    i Se recomienda borrar entradas en el IIS que sitios que no se van a utilizar en esta infraestructura en la nube, por ejemplo, BL con

conexión a IBM, o BL con conexión a versiones de JD Edwards diferentes a E920.

10. Sobre el servidor de web de pruebas y QA, cada entrada en el IIS está relacionada a un sitio Web que tiene su Web.Config en donde se especifican los datos de conexión al BL o capa de negocios; estos valores deben ser reasignados hacia el servidor que contiene la capa de negocios de la infraestructura creada en la nube.
    - Se recomienda borrar entradas en el IIS de sitios que no se van a utilizar en esta infraestructura en la nube, por ejemplo, sitios web conectados a BL referentes con conexión a IBM, o BL con conexión a versiones de JD Edwards diferentes a E920.
11. Sobre el servidor de producción cada entrada en el IIS relacionada a un BL tiene su Web.Config, en donde se especifican los datos de conexión a JD Edwards y la conexión a la base de datos. Estos valores deben ser reasignados hacia el servidor de JD Edwards y Oracle o SQL Server de la infraestructura creada en la nube.
    - Se recomienda borrar entradas en el IIS de sitios que no se van a utilizar en esta infraestructura en la nube, por ejemplo, sitios web conectados a BL referentes con conexión a IBM, o BL con conexión a versiones de JD Edwards diferentes a E920.
12. Terminar la ejecución del plan para guardar los cambios y dejar las configuraciones salvadas.
13. Se deben ejecutar los pasos previamente definidos para la creación de la máquina virtual que tendrá el rol de Deployment Server y Server Manager.
14. Se deben ejecutar los pasos previamente definidos para la creación de la máquina virtual que tendrá el rol de Enterprise Server y Web Server.
15. Se deben ejecutar los pasos previamente definidos para la creación de cinco máquinas virtuales de desarrollo.
16. Por petición de la gerencia, mediante correo electrónico se van a ir creando máquinas virtuales de desarrollo, idénticas a una de las ya creadas, hasta alcanzar el número de máquinas virtuales requeridas.
17. Se deben ejecutar los pasos previamente definidos para la creación de un VPN para acceso a recursos de forma segura.

18. Se deben realizar pruebas sobre toda la infraestructura
    i Conectividad.
    ii Acceso a recursos.
19. Se debe apagar toda la infraestructura para no generar costos adicionales.
20. Se debe documentar cada una de las pruebas realizadas sobre el DRP con el fin de mejorar aspectos que no trabajen según lo deseado. Este informe debe ser analizado entre todas áreas participantes en la creación del DRP, para discutir puntos de mejora. Los datos que deben ser capturados, después de creada la infraestructura en Azure y realizadas las pruebas, son los siguientes:
    i Nombre de la prueba.
    ii Máquina desde donde se acceso Azure.
    iii Nombre de las personas encargadas de la tarea.
    iv Fecha y hora.
    v Fallos detectados y posibles soluciones.
    vi Puntos de mejora detectados.

Con la ejecución de estos pasos se consigue tener una infraestructura en Azure, a la medida, para Premier Soluciones, que permita continuar con la ejecución de sus procesos y servicios, en caso de un desastre sobre algún componente de la infraestructura de TI.

5.6.8 Ejecución del plan

En caso de desastre que impida la continuidad del negocio de Premier Soluciones en Costa Rica, deben ejecutar los siguientes pasos para lograr integrar la infraestructura previamente creada en la nube de Azure. Hay dos acciones primordiales por hacer, para ejecutar el plan, que son las siguientes:

1. La alta gerencia, oficialmente debe emitir la declaración de desastre por medio de un correo electrónico.
2. Se debe activar el Working From Home como una estrategia de continuidad.

El equipo de respuesta a incidentes debe ingresar a Azure y ejecutar las siguientes acciones:

1. Ejecutar el plan creado para el sitio de recuperación de Azure con el cual se van a levantar los siguientes servidores:
    i. Servidor de base de datos Oracle.
    ii. Servidor de base de datos Microsoft SQL Server.
    iii. Servidor de aplicación utilizado para desarrollo y pruebas.
    iv. Servidor de web utilizado para desarrollo y pruebas.
    v. Servidor de producción pruebas.
2. Levantar el servidor virtual con los roles de Deployment Server y Server Manager.
3. Levantar el servidor virtual con los roles de Enterprise Server y Web Server.
4. Realizar las pruebas de conectividad de los servidores.
5. Notificar mediante correo electrónico a los colaboradores de Premier Soluciones, que se activa el plan y cada persona trabajará desde su casa, sea utilizando una máquina virtual asignada o bien utilizando una laptop de la empresa.
6. La gerencia debe reportar el número de máquinas virtuales de desarrollo requeridas para su creación en Azure. Por temas económicos se recomienda tener solo cinco máquinas virtuales creadas en Azure y en demanda; dependiendo de las necesidades del negocio, se irían creando nuevas máquinas réplicas de las ya existentes.
7. El software necesario adicional será incluido en un FTP, ya existente en AWS, del cual se brindarán los accesos a quienes lo necesitan en demanda.
8. En caso de trabajar con la laptop de la empresa, estas ya deben tener el certificado cliente de Premier Soluciones, instalado y el VPN configurado.
9. En caso de trabajar con una máquina personal, se debe instalar primero el certificado y seguidamente el VPN, para poder ejecutar la máquina virtual asignada en Azure.
10. El equipo de respuesta a incidentes debe brindar a cada usuario el ip de la máquina de desarrollo asignada.
11. Cuando el desastre haya pasado, todos los usuarios serán notificados para que guarden su trabajo en un máximo de 4 horas y después de ese tiempo la infraestructura en Azure será apagada nuevamente.

12. Después del desastre, las máquinas virtuales de desarrollo creadas adicionalmente a las cinco existentes deben ser eliminadas.
13. Cada usuario debe conocer el funcionamiento del plan, una vez terminado el desastre, cada usuario debe dar una retroalimentación a la gerencia y al departamento encargado de la respuesta a incidentes de cómo el plan se comportó y cuales puntos de mejora sugieren tomar en cuenta para mejorar.
14. Se debe documentar el estado y funcionamiento del plan con la siguiente información como mínimo:
    - i Nombre de la prueba.
    - ii Máquina desde donde se acceso Azure
    - iii Nombre de las personas encargadas de la tarea.
    - iv Fecha y hora.
    - v Fallos detectados y posibles soluciones.
    - vi Puntos de mejora detectados.

Una vez ejecutado el plan, se cuenta con una infraestructura completa que va a permitir la continuidad de los procesos y servicios de Premier Soluciones de una forma segura; al final del camino, la arquitectura resultante se puede ver en la Figura 23.

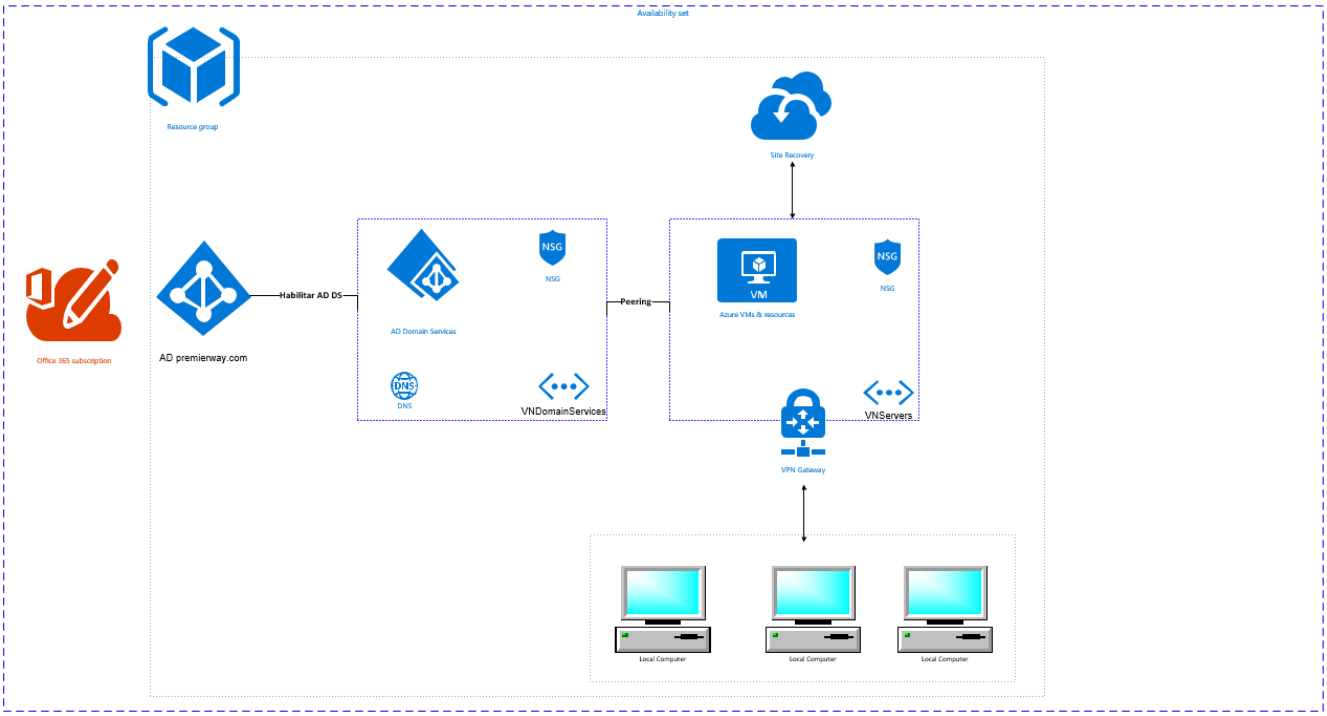


Figura 23. Infraestructura final

5.7 Definición de roles y responsabilidades

Dentro de esta estrategia de recuperación, es indispensable la definición de roles y responsabilidades que se le debe asignar al personal para poder desarrollar las tareas en caso de un desastre. Premier Soluciones cuenta con todo el personal necesario para el soporte de dicho plan; sin embargo, un equipo como tal, hoy no se encuentra formado. Se debe tomar en cuenta que, para la aplicación del plan, primero se deben seguir los pasos anteriormente descritos, para crear toda la infraestructura en Azure. Una vez creado y en caso de un evento, se debe poner a funcionar el plan propuesto anteriormente, para lo cual es necesario tener personas encargadas de los siguientes puntos:

1. Equipo de valoración del incidente, personas encargadas de valorar el impacto del desastre y decidir si es posible continuar las labores cotidianas o bien se debe activar el DRP para la continuidad del negocio.
2. Equipo de recuperación de desastres; este es el encargado de encender la infraestructura previamente creada en Azure y realizar las pruebas de conectividad de esta, siguiendo los pasos descritos en la sección anterior. Una vez encendida y probada la infraestructura en la nube, este equipo será el encargado de la puesta en marcha del ambiente *on-Premises*.

3. Equipo de comunicación; deben existir personas con suficiente importancia dentro de la organización encargada de la comunicación del incidente y mantener a los colaboradores de Premier Soluciones informados acerca de los pasos por seguir.

Cada equipo debe contar con un líder, para Premier Soluciones, en el punto 2, se recomienda nombrar una persona que tenga experiencia con la infraestructura en Azure y en redes; se recomienda que esta persona no trabaje sola y que esté acompañada de la persona que migró por primera vez la infraestructura a la nube.

5.8 Pruebas

Es recomendado realizar las pruebas de la infraestructura en Azure una vez creada, con el fin de afinar detalles; en caso de un incidente real se deberá tomar nota del comportamiento del plan con el fin de mejorar los procesos y evaluar los resultados.

6 Conclusiones

1. EL BIA permitió conocer los procesos y actividades críticas de Premier Soluciones.
2. El análisis de riesgos efectuados sobre los procesos críticos de Premier Soluciones da como resultado el identificar cuáles son los riesgos en sus actividades críticas.
3. El BIA permitió identificar los tiempos máximos de tolerancia de la disrupción de los procesos críticos de Premier Soluciones, así como la prioridad de recuperación de cada uno de ellos.
4. Se evidenció cómo se encuentra situación de la ciberseguridad dentro de Premier Soluciones, al comparar cada una de las áreas involucradas con el ISO 27001, contra lo que tiene la empresa actualmente.
5. Los procedimientos de recuperación van a permitir continuidad con la operación de Premier Soluciones, mientras un equipo en forma paralela se encarga de la recuperación de la infraestructura on-Premises.
6. Se definió una guía de implementación, que ayude a Premier Soluciones a crear un DRP, basado en la nube y que funcione de manera segura.
7. Este trabajo es de gran valor para Premier Soluciones, debido a que permite comenzar a implementar ciberseguridad como una rama, con la incursión de productos como el DRP, enfocado en la nube, con grandes ventajas a nivel operacional, competitivo y de seguridad. Entre los productos se pueden mencionar: la creación de un BIA, con el que logran conocer mejor sus procesos, al punto de priorizarlos y darles un tiempo de recuperación, adecuar a los objetivos del negocio y análisis de riesgos, con el que se evalúan los riesgos de TI, asociados con sus procesos críticos; esto permitirá a la compañía tratar de mitigar el riesgo. Otro producto es la comparación de la compañía en términos de ciberseguridad contra el ISO 270001 y por último los procedimientos que permitirán a la compañía crear un DRP, para su continuidad; todos y cada uno de estos productos dan pie a la gestión de ciberseguridad dentro de Premier Soluciones.
8. Se ejecutan validaciones de pertinencia en conjunto con colaboradores de Premier Soluciones obteniendo resultados positivos que conllevan a determinar que la solución propuesta es pertinente y aplicable.

9. Se hacen pruebas de concepto de cada una de las partes involucradas en la guía, además de tomar la opinión de consultores de JD Edwards y Microsoft Azure con el fin determinar la viabilidad de la guía, se encontró que la guía es completamente valida, viable y aplicable al entorno de Premier Soluciones.

Recomendaciones

1. Se recomienda la creación de una política de Ciberseguridad, firmada y aprobada por la alta gerencia, así como dar a conocerla a los colaboradores de la empresa.
2. Se recomienda la capacitación de los colaboradores de Premier Soluciones en temas de ciberseguridad.
3. Se recomienda crear una política de Working From Home firmada y aprobada por la alta gerencia.
4. Se recomienda ejecutar el DRP por medio de los pasos descritos en este trabajo, con el fin de mejorar la resiliencia de Premier Soluciones, ante una disrupción de sus procesos.
5. Se recomienda analizar los resultados de las pruebas del DRP o bien de la ejecución de este, con el fin de una mejora continua.
6. Se recomienda una prueba anual del DRP, con el fin de analizar su comportamiento o hacer ajustes, además de valorar mejoras en seguridad en la nube, que puedan ser incluidas en el DRP.
7. Se recomienda la actualización de BIA anualmente, con el fin de mejorar la información de los procesos actuales o bien incluir o quitar procesos, dependiendo del giro de negocio que surja con el paso del tiempo.
8. Se recomienda la creación de un departamento de ciberseguridad, de forma que se tenga al menos una persona encargada de estos temas.
9. Una vez aplicado el DRP, se recomienda apagar de forma completa la infraestructura on-Premises, con el fin de evitar ser víctima de un ciberataque. Después de un análisis y cuando la situación esté bajo control, se recomienda subir la infraestructura y realizar pruebas antes de regresar al esquema de trabajo normal.

Trabajos futuros

1. Tomando en cuenta este trabajo, un posible proyecto podría ser la implementación de este DRP y análisis de sus resultados para una mejora continua.
2. Manejo de accesos por medio de IAM.
3. Creación de un análisis de riesgos global, no solo contra los procesos críticos.
4. Realizar un BCP, con el fin de analizar la disrupción de procesos más generales y no solo la parte de TI.
5. Creación de una política de ciberseguridad en la empresa.

BIBLIOGRAFÍA

Contingency Planning Guide for Federal Information Systems. (01 de Mayo de 2010). *NIST.* Recuperado el 08 de 2018, de https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

Delgado, A. (23 de Marzo de 2014). *Los 10 términos claves de la computación en la nube*. Recuperado el 09 de 2018

European Knowledge Center for Information Technology. (01 de 01 de 2018). *TIC Portal*. Recuperado el 10 de 2018, de https://www.ticportal.es/

ISO 22301. (2012). *Societal security -- Business continuity management systems -- Requirements.*

ISO 31000. (02 de 02 de 2018). Risk management - Principles and guidelines.

ISO/IEC 27001. (2013). *Information security management systems.*

Leavitt, N. (2009). *Is Cloud Computing Really Ready for Prime Time?* California, USA: IEEE Computer.

MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. (19 de 01 de 2012). *Mintic.* Recuperado el 12 de 2019, de Mintic: https://www.mintic.gov.co/gestionti/615/articles-5482_G11_Analisis_Impacto.pdf

Mendoza, M. Á. (06 de 11 de 2014). *WeLiveSecurity | BIA*. Recuperado el 04 de 2019, de WeLiveSecurity: https://www.welivesecurity.com/la-es/2014/11/06/business-impact-analysis-bia/

Microsoft Azure. (27 de 11 de 2018). *Azure Recovery Plan | Microsoft Docs*. Recuperado el 10 de 02 de 2019, de Create and customize recovery plans for disaster recovery using Azure Site Recovery: https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-create-recovery-plans

Microsoft Azure. (18 de 12 de 2018). *Azure Virtual Network | Microsoft* . Recuperado el 02 de 2019, de Azure Virtual Network: https://docs.microsoft.com/es-es/azure/virtual-network/virtual-networks-overview

Microsoft Azure. (17 de 07 de 2018). *Five steps to secure your identity infrastructure in Azure Active Directory | Microsoft Docs*. Recuperado el 03 de 2019, de Five steps to secure

your identity infrastructure in Azure Active Directory: https://docs.microsoft.com/en-us/azure/security/azure-ad-secure-steps

Microsoft Azure. (20 de 02 de 2019). *Azure Security Identity Management Best Practices*| *Microsoft Docs*. Recuperado el 19 de 03 de 2019, de zure Security Identity Management Best Practices: https://docs.microsoft.com/es-es/azure/security/azure-security-identity-management-best-practices

Microsoft Azure. (20 de 02 de 2019). *Azure Virtual Network peering | Microsoft Docs*. Recuperado el 03 de 2019, de Azure Virtual Network peering: https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview

Nielsen. (02 de 06 de 2017). *Estudio Global: Comercio Conectado*. Obtenido de https://www.nielsen.com/latam/es/insights/reports/2017/Estudio-Global-Comercio-Conectado.html

Oracle. (1 de 10 de 2010). *Oracle's JD Edwards EnterpriseOne*. Recuperado el 10 de 2018, de ERP Software: http://www.jdedwardserp.com/

Oracle. (29 de 07 de 2015). *Oracle*. Recuperado el 03 de 2019, de Oracle | Integrated Cloud Applications and Platform Services: https://www.oracle.com/index.html

Oracle Docs. (02 de 04 de 2014). *Oracle Docs*. Recuperado el 02 de 2019, de https://docs.oracle.com/cd/E24902_01/doc.91/e22499/preface.htm#EOISA101

Oracle Support. (11 de 03 de 2014). *Oracle Support*. Recuperado el 03 de 2019, de https://support.oracle.com/epmos/faces/CertifyResults?_adf.ctrl-state=12o3u721un_4&searchCtx=st%255EANY%257Cpa%255Epi%255E2698_JD%2BEdwards%2BEnterpriseOne%2BDatabase%2BServer%257Evi%255E881509%257Epln%255EAny%257E%257C&_afrLoop=346939686927596

Revista Cloud Computing. (28 de 03 de 2019). *Glosario Cloud Computing | Revista Cloud Computing*. Recuperado el 04 de 2019, de Revista Cloud Computing: https://www.revistacloudcomputing.com/glosario-cloud-computing/

Sosinsky, B. (2010). *Cloud Computing Bible.* John Wiley and Sons Ltd.

The Acronis Global Disaster Recovery Index: 2011. (2011). Recuperado el 10 de 2018, de Acronis: http://promo.acronis.com/rs/acronis/images/BP-Acronis-Global-Disaster-Recovery-Index-EN-US-

110114.pdf?mkt_tok=3RkMMJWWfF9wsRonuKzOZKXonjHpfsX57OktWK%2Bzgokz2EFye%2BLIHETpodcMTcJgPa%2BNFAAgAZVnyRQFG%2BOHc45J6Q%3D%3D

The British Standards Institution. (2014). *BS 65000:2014: Guidance on organizational.* BSI Standards Limited 2014.

Toigo, J. W. (1996). *Disaster Recovery Planning: Strategies for Protecting Critical Information Assets.*

Zion IT Consulting. (08 de 10 de 2018). *Cloudwards | hyper-v*. Recuperado el 03 de 2019, de Cloudwards: https://www.cloudwards.net/hyper-v/

Glosario

Backup

Copia de seguridad que se realiza sobre ficheros o aplicaciones contenidas en un ordenador con la finalidad de recuperar los datos en el caso de que el sistema de información sufra daños o pérdidas accidentales de los datos almacenados (Revista Cloud Computing, 2019).

Data center

Un centro de almacenaje de datos y que provee servicios de negocio que entrega de forma segura aplicaciones y datos a usuarios remotos a través de Internet (Revista Cloud Computing, 2019).

Máquina virtual

Ordenador que está construido utilizando recursos virtualizados. Este sistema se comporta a nivel lógico de manera idéntica a la de un ordenador físico, de modo que el Sistema Operativo o aplicaciones que corren sobre él no detectan la diferencia (Revista Cloud Computing, 2019).

On-Premises

Modelo referido al esquema tradicional de licenciamiento, es decir la empresa adquiere las licencias que le otorgan derecho de uso de los sistemas del proveedor, los integra en sus propias instalaciones y mantiene sus datos dentro de su propia infraestructura de tecnología (Revista Cloud Computing, 2019).

SLA

“Service Level Agreement” o “Acuerdo de Nivel de Servicio”. Es un protocolo plasmado normalmente en un documento de carácter legal por el que una compañía que presta un servicio a otra se compromete a hacerlo bajo determinadas condiciones y con unas prestaciones mínimas (Revista Cloud Computing, 2019).

TI o IT

Tecnologías de información.

TIC o ICT

Tecnologías de información y la comunicación.

Virtualización

Es el concepto que describe cómo en un solo computador físico se coordina el uso de los recursos para que varios sistemas operativos puedan funcionar al mismo tiempo de forma independiente y sin que ellos (los SO) sepan que están compartiendo recursos con otros sistemas operativos (Revista Cloud Computing, 2019).

VPN

"Virtual Private Network", Red Privada Virtual, son configuraciones de redes informáticas que incluyen equipos que no pueden estar físicamente conectados a la red por motivos geográficos, posibilitando mediante el acceso en remoto y a través de Internet, que el personal de la compañía pueda acceder a la información que necesiten de su empresa, aunque esta sea de carácter privado (Revista Cloud Computing, 2019).

VNet

"Virtual Network", Red Virtual, es una red de Azure que permite comunicarse de forma segura entre ellos, con internet y con redes locales (Microsoft Azure, 2018).

Virtual network peering

Emparejamiento de redes virtuales permite conectar fácilmente Azure redes virtuales. Una vez emparejadas, a efectos de conectividad las redes virtuales aparecen como una sola. El tráfico entre las máquinas virtuales de las redes virtuales emparejadas se enruta a través de la infraestructura de la red troncal de Microsoft, de forma muy parecida a como se enruta el tráfico entre máquinas virtuales de la misma red virtual a través únicamente de direcciones IP privadas (Microsoft Azure, 2019).

Hyper-V

Es un software de virtualización que virtualiza el software. No solo puede virtualizar sistemas operativos, sino también componentes de hardware completos, como discos duros y

conmutadores de red. A diferencia de *Fusión y VirtualBox, Hyper*-V no se limita al dispositivo del usuario, ya que puede ser usado para la virtualización de servidores también (Zion IT Consulting, 2018)

BIA

Análisis de impacto del negocio (Business Impact Analysis o BIA por sus siglas en inglés) es otro elemento utilizado para estimar la afectación que podría padecer una organización como resultado de la ocurrencia de algún incidente o un desastre (Mendoza, 2014).