FACULTAD DE POSTGRADOS

DISEÑO DE UN PLAN DE RECUPERACIÓN DE DESASTRES (DRP) PARA EL DEPARTAMENTO DE TECNOLOGÍA DE INFORMACIÓN DE UNA EMPRESA PROCESADORA Y COMERCIALIZADORA DE ALIMENTOS

Trabajo de titulación presentado en conformidad a los requisitos establecidos para optar por el título de Magister en Gerencia de Sistemas y Tecnologías de la Información

Profesor guía

MsC. Katalina del Rocío Coronel Hoyos

Autor

Ing. David Paúl Vinueza Ludeña

Año

2016

DECLARACIÓN DEL PROFESOR GUÍA

“Declaro haber dirigido este trabajo a través de reuniones periódicas con el estudiante, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido, y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación.”

_____

Katalina del Rocío Coronel Hoyos
Magister en Gerencia de Tecnologías de la Información
CI: 1711000016

DECLARACIÓN DE AUTORÍA DEL MAESTRANTE

“Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.”

_____

Ing. David Paúl Vinueza Ludeña

CI: 1715084081

AGRADECIMIENTOS

A Dios por todas las bendiciones recibidas a lo largo de la carrera.

A mis compañeros de trabajo por su colaboración y a la empresa por confiar en mi para la elaboración del proyecto.

A mi tutor por su valiosa guía, colaboración y por compartir su conocimiento y experiencia.

DEDICATORIA

A mis padres que han estado siempre a mi lado apoyándome incondicionalmente.

A mis hermanos por sus consejos y a mi novia por motivarme a seguir creciendo personal y profesionalmente.

RESUMEN

El presente proyecto propone el Diseño de un Plan de Recuperación de Desastres para el departamento de Tecnología de Información (TI) de la empresa PRONACA, como una solución para la organización de proteger su información e infraestructura y dar continuidad a los procesos de negocio ante algún evento que pueda afectar su normal operación.

En el Capítulo I se define el Plan de Recuperación de Desastres, su objetivo e importancia y se identifican los tipos de planes para la continuidad de negocio. Finalmente se describen las etapas de la metodología propuesta por ITIL para la gestión de la continuidad de los servicios de TI.

Para el Capítulo II se describe la historia de la empresa, desde sus inicios y evolución en los diferentes negocios; se mencionan aspectos muy importantes para su éxito como son su filosofía, principios y valores. También se especifica la estructura organizacional, el organigrama de TI y la cadena de valor para tener una visión global del tipo de empresa.

En el Capítulo III se realiza el análisis de impacto en el negocio, donde se identifica y evalúa el impacto económico, comercial, operacional, imagen y legal de cuatro procesos críticos, también se determina el tiempo máximo de inactividad tolerable de la organización sin contar con los servicios de TI, los tiempos objetivos de recuperación y los puntos objetivos de recuperación. Adicionalmente se hizo un análisis de riesgo donde se identificó los activos, las vulnerabilidades, amenazas y los controles existentes; finalizando con la estimación y evaluación de riesgos.

Para el Capítulo IV se plantea la estrategia de continuidad de los servicios de TI la cual consiste en definir las medidas de respuesta a riesgos y las opciones de recuperación ante un desastre. Se realiza un análisis de costo

beneficio de la solución planteada y se definen los procedimientos y equipos de recuperación de desastres.

En el Capítulo V se presentan las conclusiones y recomendaciones del proyecto.

ABSTRACT

The present project proposes the Design of a Disaster Recovery Plan for the department of Information Technology (IT) of PRONACA Company, as a solution for the organization to protect the information and infrastructure to give continuity of the business process before some event could affect the normal operation.

Chapter I defines the Disaster Recovery Plan, the objective and the importance of it, identifies the types of plans for business continuity. Finally describes the stages of the methodology proposed by ITIL for the IT continuity services management.

Chapter II explains the history of the company, from the beginning and evolution in the different business; very important aspects are mentioned for its success based in the philosophy, principles and values. Specifies the organizational structure, the IT flowchart and the chain value to give us a global vision of the type of company.

Chapter III develops the business impact analysis, where it is identified and evaluated the economic, commercial, operational, reputational, image and legal impact of four critical processes; also determinates the maximum tolerable downtime of the organization without the IT services, the recovery time objective and the recovery point objective. Besides, the risk analysis permitted to identify the assets, vulnerabilities, threats and existing controls to; finishing with the estimation and risk evaluation.

Chapter IV applies the strategy of continuity IT services which consists of defining the measures of response to risks and the options of recovery after a disaster. Makes an analysis of cost and benefit of the suggested solution and defines the procedures and equipment needed for the disaster recovery.

Chapter V presents the conclusions and recommendations of the project.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

Procesadora Nacional de Alimentos C.A PRONACA es una empresa líder en el mercado Ecuatoriano que trabaja en la elaboración y comercialización de alimentos sanos, nutritivos y de calidad; la empresa cuenta con 105 centros de operación que contribuyen al desarrollo del sector agropecuario y promueven la educación en comunidades rurales.

PRONACA requiere que el departamento de Tecnología de Información cuente con un Plan de Recuperación de Desastres que le permita tener operativos los sistemas de información y servicios tecnológicos ante desastres naturales o errores humanos, al estar expuesta a interrupciones de sus actividades la organización puede tener pérdidas financieras, información valiosa, productividad y credibilidad.

Con el Plan de Recuperación de Desastres se procura conocer cuáles son los recursos y procesos críticos de la empresa y su impacto en el negocio ante una interrupción no deseada, además de conocer cuáles son los riesgos que pueden afectar su normal operación e identificar las amenazas y vulnerabilidades con la finalidad de establecer las estrategias para la recuperación de los servicios tecnológicos.

Se desea diseñar medidas preventivas y planes de acción que se deben seguir para una recuperación oportuna, en el menor tiempo posible y con la menor afectación en la disponibilidad de los recursos y servicios tecnológicos que soportan los procesos de negocio de tal manera que se pueda minimizar el impacto en la empresa. También se van a definir los procedimientos y formar los equipos requeridos para recuperar los servicios tecnológicos en caso de declararse un desastre.

1. Capítulo I. Marco teórico aplicado

1.1. Plan de recuperación de desastres (DRP)

1.1.1. Definición del DRP

Para comprender la definición de plan de recuperación de desastres se debe tener claro el significado de desastre que no es más que “cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa”. (ISO, 2012)

Plan de recuperación de desastres o DRP por sus siglas en inglés (*Disaster Recovery Plan*) es un “conjunto de estrategias, acciones, procedimientos planificados y responsabilidades definidas para minimizar el impacto de una interrupción imprevista de las funciones críticas y conseguir la restauración de las mismas dentro de unos límites de tiempo establecidos”. (Gaspar, 2010)

Para el *National Institute of Standards and Technology* (NIST, 2010) DRP es un “plan escrito para recuperar uno o más sistemas de información hacia una instalación alterna debido a una falla grave de hardware/software o destrucción de la instalación principal”.

1.1.2. Objetivos del DRP

El DRP debe cumplir con los siguientes objetivos:

- Aumentar la probabilidad de la continuidad de los procesos críticos de la organización en caso de una interrupción de los servicios tecnológicos.
- Proporcionar un enfoque organizado de las actividades de recuperación ante un incidente.

- Proveer una apropiada y rápida respuesta ante cualquier incidente, reduciendo el impacto que pueden originar las interrupciones.
- Aumentar la capacidad de la organización en recuperarse ante un incidente que haya afectado la infraestructura tecnológica.
- Reducir el tiempo de recuperación que permita minimizar las pérdidas económicas por causa de un desastre.
- Desarrollar los procedimientos necesarios para reducir la duración y el costo de recuperación de los servicios de TI.
- Minimizar el riesgo de errores y la duplicidad de esfuerzos. (Gaspar, 2010)

1.1.3. Importancia del DRP

EL DRP ha tomado relevancia en las organizaciones debido a la alta dependencia de las tecnologías de la información en las operaciones cotidianas y la automatización de sus procesos, que vuelve crítica la disponibilidad de los servicios de TI, es por esto que ha surgido la necesidad de que se contemplen en los presupuestos los recursos necesarios para crear planes que otorguen la capacidad de restablecer los servicios en el menor tiempo posible ante la ocurrencia de un desastre que pueda afectar el alcanzar los objetivos estratégicos de la organización. (Matos, Beriguete, & Reidy, 2015)

“Solamente el 6% de las empresas que sufren una pérdida de datos catastrófica sobreviven al desastre, mientras que el 43% no vuelven a abrir nunca y el 51% cierran en los 2 años siguientes”. (Hoffer, Jim, 2001)

El valor de la información se ha convertido en uno de los principales activos que tienen las empresas y su gestión es depositada en tecnologías, es por esto que los planes de contingencia deberían ser de utilidad en cualquier tipo de organización, sea ésta grande o pequeña. (Gaspar, 2010)

1.1.4. Tipos de planes

Existen varios tipos de planes que pueden ser implementados individualmente o en coordinación con otro de manera apropiada para responder a un evento disruptivo. (NIST, 2010)

Tabla 1. Tipos de planes.

Plan	Propósito	Alcance	Relación del Plan
Plan de Continuidad de Negocio (BCP)	Proporciona los procedimientos para mantener las operaciones de misión del negocio mientras se recupera de una interrupción significativa.	Direcciona los procesos de negocio al nivel inferior o ampliado de las funciones de misión esenciales COOP.	El plan centrado en los procesos de negocio puede activarse en coordinación con el COOP.
Plan de Continuidad de Operaciones (COOP)	Proporciona procedimientos y guías para mantener las funciones de misión esenciales de la organización a un sitio alterno por más de 30 días.	Direcciona las funciones de misión esenciales a una instalación alterna, los sistemas de información son direccionados basados únicamente en el soporte de las funciones de misión esenciales.	El plan centrado en las funciones de misión esenciales puede activar varios niveles de unidad de negocio BCP's, ISCP´s o DRP's según sea apropiado.
Plan de Comunicación de Crisis	Proporciona procedimientos para la difusión interna y externa de la comunicación; significa que provee el estatus de información crítica y controla rumores.	Direcciona la comunicación con el personal y el público, no se centra en los sistemas de información.	Plan basado en incidentes, usualmente se activa con el COOP o BCP, pero puede ser utilizado solo durante la exposición de un evento público.
Plan de Protección de la Infraestructura Critica (CIP)	Proporciona políticas y procedimientos para la protección de los componentes críticos de infraestructura, es definido en el Plan de protección de infraestructura nacional.	Direcciona los componentes críticos de infraestructura que están apoyados u operado por una organización o agencia.	El plan de gestión de riesgos que está apoyado por el COOP para organizaciones con infraestructuras críticas y activos de recursos claves.
Plan de Respuesta a Cyber Incidentes (CIRP)	Proporciona procedimientos para la mitigación y corrección de un ataque cibernético, como un virus, gusano o caballo de Troya.	Direcciona a la mitigación y aislamiento de los sistemas afectados, limpieza y minimizar la pérdida de información.	Plan enfocado en los sistemas de información que pueden activar un ISCP o DRP dependiendo el grado del ataque.
Plan de Recuperación de Desastres	Proporciona los procedimientos para la reubicación de las	Se activa después de una gran interrupción de los sistemas con	Sistemas de información enfocados en el plan que activa

(DRP)	operaciones de los sistemas de información a una ubicación alterna.	efectos a largo plazo.	uno o más ISCP's para la recuperación de los sistemas individuales.
Plan de Contingencia de los Sistemas de Información (ISCP)	Proporciona los procedimientos y capacidades para la recuperación de un sistema de información.	Direcciona la recuperación de un único sistema de información, si es apropiada la ubicación alterna.	Plan enfocado en los sistemas de información que pueden ser activados independientemente de otros planes o es parte de un mayor esfuerzo de recuperación coordinado con un DRP, COOP y/o BCP.
Plan de Emergencia de los Ocupantes (OEP)	Proporciona procedimientos coordinados para reducir al mínimo la pérdida de vidas, lesiones y proteger daños materiales en respuesta a una amenaza física.	Se centra en el personal y a la propiedad particular de una instalación especifica. No en procesos de negocios o sistemas basados en información.	Plan basado en incidentes que son iniciados inmediatamente después de un evento, previo a la activación del COOP o DRP.

Tomado de: (NIST, 2010)

La siguiente figura muestra la interrelación que existe entre los diferentes tipos de planes.

Figura 1. Relación entre los tipos de planes.
Tomado de: (NIST, 2010)

El presente trabajo está enfocado específicamente en la elaboración de un diseño de plan de recuperación de desastres para la empresa PRONACA.

1.2. Gestión de la continuidad de los servicios de TI

Para el diseño del DRP se tomará como referencia principal el modelo propuesto por ITIL para la gestión de la continuidad de servicios de TI o ITSCM; este modelo se preocupa en apoyar los procesos de continuidad de negocio impidiendo una interrupción en los servicios de TI, sean por desastres o por otras causas de fuerza mayor, asegurando que las instalaciones y servicios puedan estar disponibles dentro de un tiempo requerido y establecido por el negocio. (Axelos, 2011)

Existen otros marcos de referencia reconocidos mundialmente como es el caso de la norma internacional ISO 22301 (Seguridad de la sociedad: Sistemas de continuidad del negocio – Requisitos); la cual especifica los requisitos para la creación de un sistema eficaz de gestión de continuidad de negocio; esta norma será considerada como apoyo para el diseño del DRP ya que “este modelo aparece como producto de una evolución de lineamientos, buenas prácticas y estándares en continuidad del negocio”. (Axelos, 2011)

El proceso de ITSCM incluye:

- Acuerdos acerca del alcance y la definición de políticas.
- Análisis de impacto en el negocio BIA para cuantificar la afectación en el negocio con respecto a la pérdida de los servicios de TI.
- Análisis de riesgo RA para identificar y evaluar los riesgos que pueden afectar la continuidad del servicio, adicionalmente identificar las amenazas y la probabilidad de que estas ocurran.
- Estrategias globales donde se incluyen elementos para la reducción de riesgos y las opciones de recuperación adecuadas.
- Pruebas del plan.

- Puesta en marcha y mantenimiento del plan.

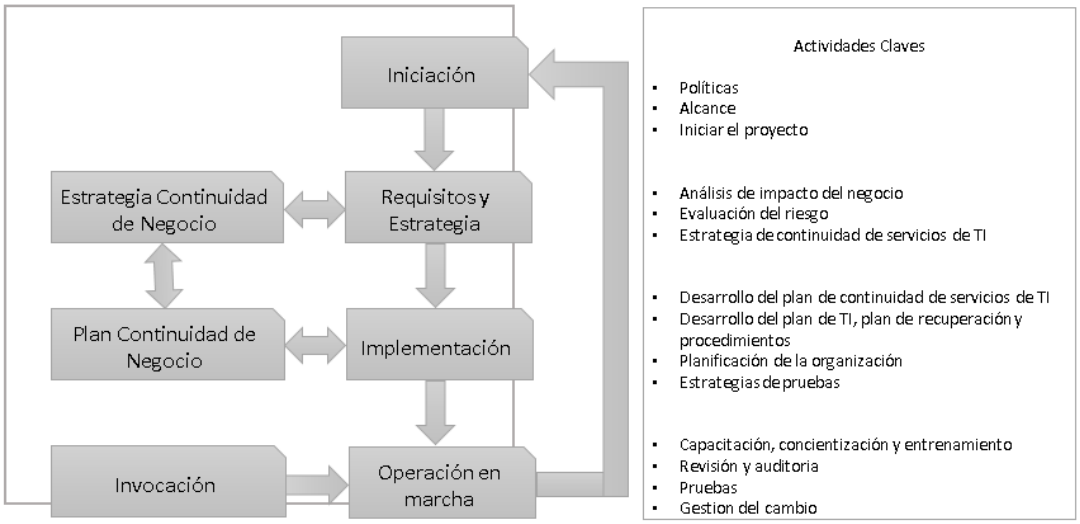


Figura 2. Ciclo de vida de la gestión de continuidad de servicios.
Tomado de: (Axelos, 2011)

1.2.1. Etapa de iniciación

La primera etapa consta de las siguientes actividades:

- Definir la política.- Se establece una política la cual debe ser comunicada a todas las personas involucradas o que se vieran afectadas por problemas de continuidad de servicios para que sean conscientes de sus responsabilidades y de su apoyo para cumplir con la gestión de continuidad de servicios.
- Especificar el alcance.- Se define el alcance y las responsabilidades de todo el personal de la organización.
- Asignar recursos.- Se considera los recursos humanos internos como externos (proveedores) y los recursos económicos.
- Definir la organización y control del proyecto.- Al ser un proyecto complejo es recomendable utilizar una metodología para el manejo del mismo.

1.2.2. Etapa de Requisitos y estrategia

El determinar los requisitos que necesita la empresa para dar continuidad a los servicios de TI es un componente crítico ya que se establece si una organización puede sobrevivir a una interrupción o un desastre y los gastos en los que debe incurrir; si el análisis de requisitos es incorrecto puede tener consecuencias graves en la eficacia del ITSCM.

Esta etapa se divide en dos fases:

- Requisitos.- Se realiza un análisis de impacto y evaluación de riesgos.
- Estrategia.- Una vez realizado el análisis de requisitos, la estrategia documenta las medidas de reducción de riesgos y las opciones de recuperación.

1.2.2.1. Requisitos – Análisis de impacto en el negocio

El propósito de un análisis de impacto es conocer la tolerancia del negocio a una interrupción, así como cuantificar la pérdida de servicio y cuál sería la afectación en el negocio; el impacto por ejemplo puede ser alto si se habla de pérdida económica e impacto medio o bajo por la parte legal debido al incumplimiento de contratos.

El BIA identifica los servicios más importantes de la organización para definir la estrategia de continuidad que garantice los tiempos de recuperación que el negocio requiere. Adicionalmente el BIA identifica:

- La forma en que los daños pueden afectar, por ejemplo
    - Pérdida de ingresos
    - Costos adicionales
    - Reputación afectada

    - Pérdida de ventaja competitiva
    - Riesgo para la seguridad del personal
    - Pérdida de la capacidad operativa
- En qué momento la interrupción de un servicio puede tener mayor afectación.
- Los recursos necesarios para que los procesos críticos puedan continuar operando a un nivel mínimo aceptable.
- El tiempo mínimo en que deben ser recuperados totalmente los servicios.
- La prioridad de recuperación para cada uno de los servicios de TI.

Este análisis permite realizar un mapeo de los servicios críticos, aplicaciones y tecnología que dan soporte a los procesos del negocio.

Al realizar un BIA es importante las opiniones de los altos representantes de los negocios, del personal de supervisión y del personal de menor rango para asegurar todos los aspectos de impacto que se puedan producir después de la pérdida de un servicio ya que a menudo se tienen diferentes puntos de vista los cuales deben ser tomados en cuenta para realizar una estrategia global.

En varias organizaciones resulta casi imposible o no será un costo justificable el recuperar la totalidad de los servicios y en un corto plazo. En muchos casos los procesos de negocio pueden ser restablecidos sin una dotación completa de personal, sistemas e instalaciones y todavía se puede mantener a un nivel aceptable los servicios a los clientes. Por lo tanto los objetivos de recuperación se deben expresar en términos de:

- El tiempo dentro del cual un equipo predefinido del personal base y las instalaciones mínimas establecidas deben ser recuperadas.
- El cronograma de recuperación del personal y de las instalaciones restantes.

Existe una necesidad de equilibrar el impacto contra el precio de recuperación para asegurar que los costos sean aceptables. Los objetivos de recuperación ofrecen un punto de partida desde el cual se pueden evaluar diferentes opciones de recuperación del negocio. (Axelos, 2011)

Tabla 2. Recopilación de datos para el BIA.

Procesos de negocio	Descripción	Categoría de impacto	MTD (Tiempo máximo de inactividad tolerable)	RTO (Tiempo objetivo de recuperación)	RPO (Punto objetivo de recuperación)

Adaptado de: (NIST, 2010)

1.2.2.2. Requisitos – Análisis de riesgos

Para el caso del DRP, riesgo es la probabilidad de que sucediera un desastre o una interrupción seria de los servicios. Se trata de una evaluación del nivel de amenaza y el grado en que una organización es vulnerable a dicha amenaza. El análisis de riesgo también puede utilizarse para evaluar y reducir la posibilidad de incidentes operacionales y es una técnica utilizada para garantizar la disponibilidad y los niveles de confiabilidad. El análisis de riesgo es un aspecto clave en la gestión de la seguridad de la información y de la continuidad de negocio.

El análisis de riesgo forma parte de una de las actividades del proceso de gestión del riesgo; la gestión de riesgos “incluye todas las actividades requeridas para identificar y controlar la exposición al riesgo, que pueden tener un impacto en el logro de los objetivos del negocio de una organización”. (Axelos, 2011)

Para ITIL la gestión de riesgos consiste en:

- Principios: Son esenciales para el desarrollo de buenas prácticas de gestión de riesgos.
- Enfoque: Debe ser acordado y definido en los siguientes documentos:
    - Política de gestión de riesgo
    - Guía del proceso
    - Registro de riesgos
    - Registro de errores
- Procesos: Los siguientes cuatro pasos describen las entradas, salidas y actividades que aseguran el control de los riesgos:
    - Identificar.- Las amenazas y oportunidades dentro de una actividad que puede afectar la capacidad de cumplir el objetivo.
    - Evaluar.- La comprensión del efecto de las amenazas y oportunidades identificadas.
    - Responder.- Preparar una respuesta que reduzca las amenazas y maximice las oportunidades.
    - Monitorear.- Vigilar la eficacia de los controles y tomar medidas correctivas.
- Incorporar y revisar.- Haber puesto los principios, enfoque y procesos en su lugar, estos tienen que ser revisados y mejorados continuamente para asegurarse que siguen siendo eficaces.
- Comunicación.- Tener las actividades de comunicación apropiadas para garantizar que todo el personal se mantenga informado de los cambios en las amenazas, oportunidades y otros aspectos de la gestión de riesgos. (Axelos, ITIL - Diseño del Servicio, 2011)

Una vez realizado el análisis de riesgo (identificación y evaluación), es posible determinar las respuestas apropiadas, es decir reducir el riesgo a un nivel aceptable o mitigar el riesgo. Las respuestas al riesgo deben ser implementadas para reducir ya sea el impacto o la probabilidad de que ocurran.

La Tabla 3 contiene una lista de ejemplos de los riesgos y amenazas que deben ser considerados.

Tabla 3. Ejemplos de riesgos y amenazas.

Riesgo	Amenaza
Pérdida de los sistemas internos de TI	• Fuego • Fallo de energía • Inundaciones • Desastre natural (terremotos, huracanes, etc.) • Ataque terrorista • Sabotaje • Daño accidental • Software de mala calidad
Pérdida de los sistemas externos de TI	• Excesiva demanda de servicios • Ataque de denegación de servicios • Falla tecnológica
Pérdida de datos	• Falla tecnológica • Errores humanos • Virus • Software malicioso
Pérdida de los servicios de red	• Daño o acceso denegado a la red de servicio del proveedor • Pérdida de los servicios de los proveedores de sistemas y red • Pérdida de información de los proveedores de servicios • Falla de los servicios del proveedor
Falta de disponibilidad de los técnicos claves y personal de soporte	• Acceso local denegado • Renuncia • Enfermedad • Dificultad en el transporte
Falta de proveedores de servicios de TI	• Fracaso comercial • Acceso local denegado • Falta de disponibilidad del personal del proveedor de servicios • Incumplimiento contractual de los niveles de servicio

Tomado de: (Axelos, 2011)

1.2.2.3. Estrategia de continuidad de los servicios de TI

Los resultados de análisis de impacto en el negocio y análisis de riesgo permitirán a las organizaciones tener una adecuada estrategia de continuidad de servicios de TI que vaya de acuerdo a las necesidades del negocio. La estrategia debe tener un equilibrio entre la reducción de riesgos y las opciones de recuperación considerando las prioridades de los servicios. Aquellos servicios que han sido identificados de alto impacto se requieren concentrar los esfuerzos en los métodos preventivos para reducir los riesgos mientras que los servicios de bajo impacto es mejor adaptarles a las opciones de recuperación integrales.

1.2.2.4. Medidas de respuesta a riesgos

La mayoría de las organizaciones tendrán que adoptar un enfoque equilibrado, donde la reducción del riesgo y la recuperación son complementarios y necesarios, esto implica reducir en lo posible los riesgos de la continuidad de los servicios de TI y eso se logra a través de la gestión de la disponibilidad ya que muchos de estos reducen la probabilidad de fallo que afecten los servicios.

Según ITIL las medidas típicas de reducción de riesgos incluyen:

- Instalación de un sistema de alimentación ininterrumpida (UPS*)*.
- Sistemas de tolerancia a fallos para aplicaciones críticas donde el mínimo tiempo de inactividad es inaceptable.
- Configuración de los discos en *RAID* de espejo para evitar las pérdidas de datos y garantizar la disponibilidad continua de los datos.
- Disponer de piezas de equipos que se utilizarán en caso de que fallen los equipos.
- Eliminación de puntos de red individuales o fuentes de alimentaciones únicas en los edificios.

- Resiliencia en las redes y sistemas de TI.
- Externalización de los servicios con más de un proveedor.
- Mayores controles de seguridad física de TI.
- Mejores controles para detectar interrupciones en el servicio como los sistemas de detección de incendios junto con los sistemas de extinción.
- Una estrategia de copia de seguridad y recuperación integral, incluyendo el almacenamiento fuera de sitio. (Axelos, ITIL - Diseño del Servicio, 2011)

Estas medidas no resolverán necesariamente un problema en la continuidad de los servicios de TI ni eliminarán el riesgo por completo, pero todos o una combinación de ellos pueden reducir significativamente los riesgos.

1.2.2.5. Opciones de recuperación

La estrategia del plan de recuperación de los servicios de TI debe tener un equilibrio entre los costos de las medidas de reducción de riesgo y las opciones de recuperación de los procesos críticos del negocio dentro de los plazos acordados. La siguiente es una lista propuesta por ITIL de las posibles opciones de recuperación de TI que deben tenerse en cuenta en el desarrollo de la estrategia.

- Soluciones manuales temporales.- Puede ser una medida provisional eficaz para un tiempo limitado hasta que se reanude el servicio de TI. Por ejemplo el registro de los tickets de mesa de ayuda se pueden ir registrando en una hoja de cálculo.
- Recuperación gradual.- Conocido como '*cold standby*' incluye un sitio alterno equipado con fuentes de poder, controles ambientales, cableado de red, telecomunicaciones, infraestructura y está disponible para ser utilizado en caso de un desastre. Este tipo de recuperación no es aplicable a los servicios que requieren una pronta

recuperación por el tiempo que implica reanudar los servicios, esta opción se recomienda para servicios que no sean críticos y que puedan soportar un tiempo de recuperación de días o semanas.

Se debe tener en cuenta el costo de esta opción frente al beneficio antes de escoger la recuperación gradual. Este tipo de alojamiento puede ser proporcionado por un tercero o puede ser propio y debe encontrarse en otro lugar a cierta distancia del sitio principal.

- Recuperación intermedia.- También llamado '*warm standby*' provee una recuperación y restauración rápida de los servicios, este puede ser en un sitio alterno arrendado por un tercero o en uno propio con los servidores, sistemas operativos, sistemas de aplicación y comunicación ya disponibles. En un caso de un fallo de sistema es posible cambiar con facilidad a una copia de seguridad con poca pérdida de servicio, normalmente utilizado para sistemas críticos ya que el restablecer los servicios está dentro de un periodo de 24 horas.
- Recuperación inmediata.- Igualmente se le conoce como '*hot standby*', '*mirroring*' o espejo, '*load balacing*' o balanceo de carga, establece la restauración inmediata y sin pérdida de los servicios. Exclusivamente utilizado para los servicios críticos del negocio que requieren una operación continua sin interrupciones, el equipamiento deber ser igual del sitio principal con el del sitio alterno. Esta opción es muy costosa pero justificable ya que la falta de disponibilidad por un periodo corto de tiempo puede ser de gran impacto para la organización. La instalación alterna tiene que estar situada lo suficientemente lejos del principal para que no sean afectadas las dos en caso de un desastre. (Axelos, ITIL - Diseño del Servicio, 2011)

Los diferentes servicios de la organización requieren diferentes tipos de recuperación, sea cual sea la opción elegida el costo debe ser justificado.

Como regla general mientras más tiempo puede el negocio sobrevivir sin un servicio la solución va a ser más económica.

Dentro de la planificación además de la recuperación de los equipos y servicios informáticos se debe incluir la recuperación de alojamiento e infraestructura tanto para el personal de TI como para los usuarios.

1.2.3. Etapa de implementación

El plan ITSCM es necesario para hacer frente a todas las actividades que permitan asegurar que los servicios, instalaciones y recursos sean entregados en un estado de funcionamiento aceptable y que son aptos para el propósito al ser aceptados por la organización, esto implica las pruebas necesarias de rendimiento, funcionales, operativas, antes de la entrega, y la validación de la integridad de los datos.

El formato de plan de recuperación debe permitir un acceso rápido a la información y todo el personal clave debe tener acceso a las copias de toda la documentación necesaria. Los planes deben ser documentos formalizados y controlados bajo la gestión del cambio para garantizar que las versiones más recientes estén disponibles, es importante asegurarse que una copia debe mantenerse fuera de las instalaciones.

Los planes de recuperación deben asegurar que todos los detalles con respecto a la recuperación de los servicios de TI después de un desastre están totalmente documentados, además deben ser suficientemente detallados y entendibles para que una persona técnica que no está familiarizado con los sistemas pueda seguir los procedimientos. Los planes de recuperación incluyen detalles como el punto de recuperación de los datos, una lista de los sistemas dependientes, requisitos de hardware y software del sistema, detalles de configuración e información relevante o esencial sobre el sistema.

Una buena práctica es incluir una lista de verificación que cubre las acciones específicas que se requieren durante todas las etapas de la recuperación del servicio, por ejemplo después de que el sistema se haya restaurado a un estado operativo realizar pruebas de conectividad, funcionalidad, consistencia de datos, integridad antes de realizar la entrega del servicio a la empresa.

Por último, cada área crítica para la empresa es responsable de la elaboración de un plan que detalle las personas que estarán en los equipos de recuperación y las tareas que deben realizarse al momento de activar el plan.

Otras actividades que ITIL sugiere que deben ser implementadas a raíz de la aprobación de la estrategia son:

- Planificación de la organización.- Durante el proceso de recuperación de desastres la estructura organizacional será modificada de su funcionamiento normal y se basará en:
    - Ejecutivo.- Junta ejecutiva de alto nivel, con la autoridad y control general de la organización y es responsable de la gestión de crisis y la coordinación con otros departamentos.
    - Coordinación.- Responsable de coordinar los esfuerzos globales de la recuperación dentro de la organización.
    - Recuperación.- Una serie de equipos de negocio y de recuperación de servicios que representan las funciones criticas del negocio y los servicios que necesitan ser establecidos para apoyar estas funciones. Cada equipo es responsable de la ejecución de los planes dentro de sus propias áreas y para la coordinación con el personal, los clientes y terceros. Las prioridades de recuperación del servicio y sus componentes son identificados en el BIA, los cuales deben ser documentados dentro de los planes y deben ser aplicados durante su ejecución.

- Pruebas.- Los planes de recuperación que no han sido totalmente probados no tienen siempre los resultados esperados, por lo tanto las pruebas son una parte crítica en este proceso y la única manera de comprobar que la estrategia seleccionada, los planes y procedimientos sean los adecuados.

  Existen cuatro tipos de pruebas que se pueden realizar:

  - Pruebas de recorrido.- Se pueden realizar cuando el plan está establecido simplemente para conseguir las personas pertinentes y en conjunto ver si el plan al menos trabaja de manera simulada.
  - Pruebas completas.- Deben llevarse a cabo tan pronto como sea posible en intervalos de por lo menos una vez al año, se deben incluir las unidades de negocio para ayudar a demostrar la capacidad de recuperación de los servicios de TI y de los procesos de negocio. Las pruebas completas pueden ser anunciadas es decir previamente planificadas y también sin previo aviso, es importante también que se involucren y se incluyan a personas que no estén muy familiarizados con los servicios y sistemas de TI ya que las personas con mayor conocimiento pueden no estar disponibles cuando un desastre ocurra en realidad.

    La prueba completa es la mejor manera de probar que todos los servicios se puedan recuperar en los plazos requeridos.
  - Pruebas parciales.- Pueden llevarse a cabo la recuperación de ciertos elementos como servicios individuales o servidores.
  - Pruebas de escenario.- Se pueden utilizar para probar las reacciones en condiciones, eventos y escenarios específicos. (Axelos, ITIL - Diseño del Servicio, 2011)

Las pruebas deben tener los objetivos claramente definidos para determinar el éxito o no del ejercicio.

1.2.4. Etapa de operación en marcha

Esta etapa consiste en:

- Educación, concientización y entrenamiento.- Esto debe cubrir a toda la organización y más aún al departamento de TI, esto asegura que todo el personal sea consciente de las implicaciones de la continuidad de los servicios para el negocio y que todas las personas involucradas en el plan conozcan la forma de aplicar sus acciones.
- Revisión.- Se deber realizar una revisión periódica de todos los entregables en el proceso para garantizar que sigan siendo los actuales.
- Pruebas.- Es necesario establecer un programa de pruebas regulares para garantizar que los componentes críticos de la estrategia se ponen a prueba de preferencia por lo menos anualmente. Es importante que cualquier cambio realizado en tecnología también sea incluido en la estrategia y debe ser implementado de manera adecuada y probado para su correcto funcionamiento. La copia de seguridad y recuperación de los servicios de TI también deben ser controlados y probados para asegurar que cuando se necesiten durante un incidente vayan a operar.
- Gestión del cambio.- Debe garantizar que todos los cambios son evaluados por su potencial impacto, el plan debe ser actualizado antes de implementar el cambio y debe ser aprobado como parte de las pruebas de cambio. También de forma permanente siempre que haya nuevos servicios o donde los servicios tengan grandes cambios es esencial que se haga una evaluación del BIA y RA, para finalmente modificar la estrategia y actualizar los planes como consecuencia. (Axelos, ITIL - Diseño del Servicio, 2011)

2. Capitulo II. Análisis del negocio

2.1. Descripción de PRONACA

2.1.1. Historia

A partir del año 1957 nace INDIA, compañía dedicada a la importación y distribución de insumos agropecuarios y artículos para la industria textil. Los inicios fueron encaminados en el negocio de incubación de huevos con la empresa INCA para luego crear INDAVES para la producción y comercialización de huevos.

En el año de 1979 se funda PRONACA Procesadora Nacional de Aves C.A., donde se efectúa el procesamiento y venta de pollos, en el mismo año nace SENACA donde se realiza investigación, desarrollo y producción de semillas de arroz y maíz para luego incursionar en la producción y comercialización de alimento balanceado.

En los años 90 existe una diversificación de productos con COMNACA, un negocio que produce conservas e INAEXPO que produce y exporta palmito en el mundo, también se da inicio a la crianza y producción de cerdos y se crea Fundación San Luis la cual contribuye al desarrollo de proyectos sociales y comunitarios. Un hito importante se marca en el año 1999 ya que PRONACA se convierte en lo que hoy en día es Procesadora Nacional de Alimentos C.A.

A partir del año 2000 empieza el negocio de precocidos con la marca MR. COOK con producción y comercialización tanto en Ecuador como en Colombia. En 2009 se inaugura un nuevo centro de distribución en la ciudad de Guayaquil, con una infraestructura y tecnología de punta.

2.1.2. Actualidad

PRONACA cuenta con 105 centros de producción divididos en:

- 59 granjas de aves y cerdos
- 27 plantas
- 6 centros de distribución
- 6 almacenes
- 4 centros administrativos
- 3 laboratorios / centros de investigación

Además dispone de 8067 colaboradores que contribuyen al continuo desarrollo de la compañía. En la actualidad se cuenta con un portafolio de 31 marcas, 2074 items y 13 líneas de productos.

Figura 3. Marcas de PRONACA.
Tomado de: (Intranet PRONACA)

2.1.3. Misión y Visión

2.1.3.1. Misión

“Ser una empresa líder e innovadora en la industria alimenticia nacional e internacional, satisfaciendo a los consumidores y clientes con calidad óptima y excelente servicio”.

2.1.3.2. Visión

“Ser una empresa que cree en su gente y en su desarrollo, líderes en calidad y seguridad alimentaria, innovadores y creativos, con un alto sentido de responsabilidad social, preocupados por el mantenimiento del equilibrio ambiental”.

2.1.4. Valores y Principios

2.1.4.1. Valores

- Integridad: Decir la verdad y obrar de forma transparente.
- Responsabilidad: Trabajar bien, de forma eficiente.
- Solidaridad: Colaborar con los demás de forma generosa.

2.1.4.2. Principios

- Consumidores, produce alimentos sanos y de calidad para la salud y bienestar de sus consumidores.
- Colaboradores, lidera con ética y justicia a sus colaboradores en un ambiente de solidaridad y respeto.
- Proveedores, mantiene relaciones sólidas y de confianza con sus proveedores ofreciendo un crecimiento compartido.
- Clientes, atiende a sus clientes con un servicio rápido y eficiente.

- Sociedad, fomenta buenas relaciones con sus grupos de interés en un ambiente de armonía y colaboración.
- Asociados, actúa responsablemente con productores y emprendedores creando relaciones beneficiosas para todas las partes involucradas.

2.1.5. Filosofía

PRONACA existe para alimentar bien, generando desarrollo en el sector agropecuario.

2.1.6. Estructura organizacional

Para cumplir con las metas y acompañar al crecimiento continuo, la empresa cuenta con una estructura organizacional dinámica que se ajusta a los requerimientos estratégicos.

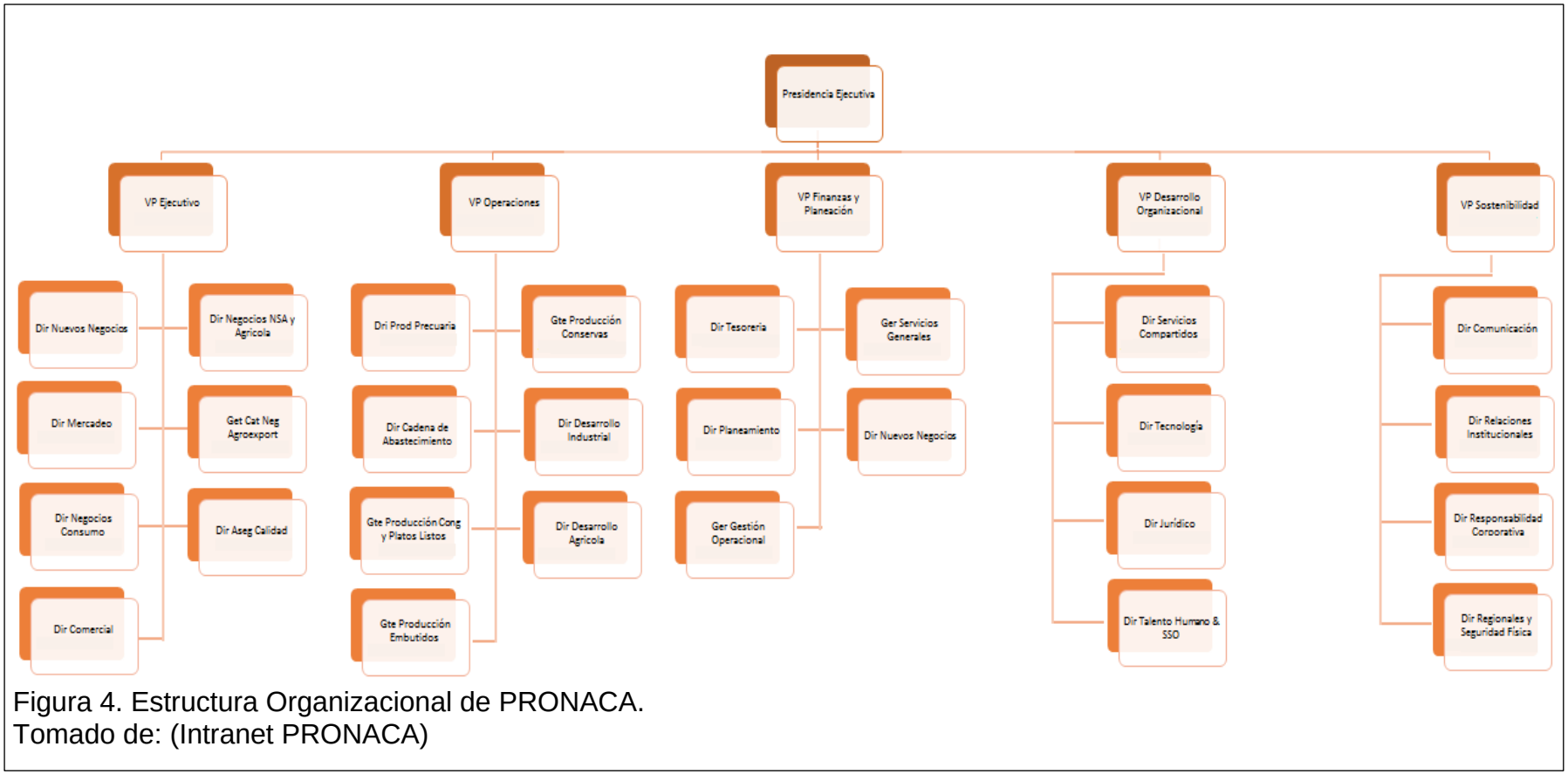


Figura 4. Estructura Organizacional de PRONACA.
Tomado de: (Intranet PRONACA)

2.1.7. Organigrama de TI

En la Figura 5 se puede observar la estructura actual de TI con la que cuenta la empresa.

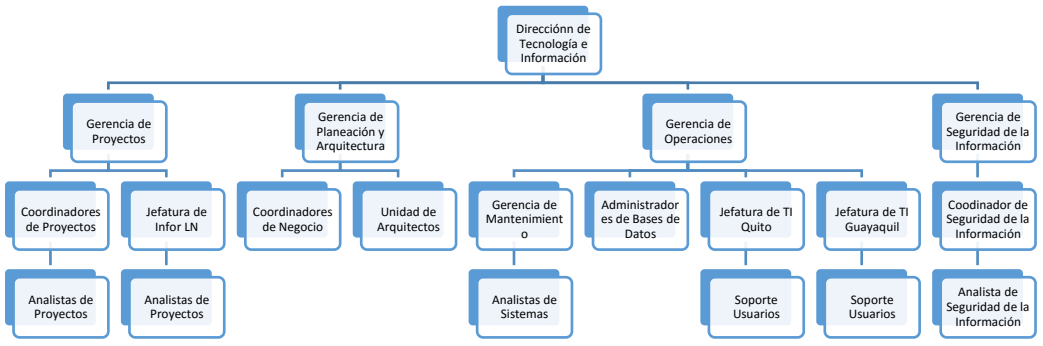


Figura 5. Organigrama de TI.

2.1.8. Cadena de Valor

En la Figura 6 se muestra la cadena de valor de PRONACA, donde se puede visualizar las actividades primarias y secundarias. Las actividades primarias o centrales son los procesos claves para satisfacer los requerimientos y necesidades del cliente generando valor, es decir rentabilidad para la empresa, mientras que las actividades secundarias o procesos de soporte son necesarios para que los procesos centrales operen eficaz y eficientemente.

Figura 6. Cadena de Valor de PRONACA.

Tomado de: (Morales, 2015)

2.2. Problemática actual

PRONACA tiene la necesidad de contar con un plan de recuperación de desastres puesto que sus procesos pueden experimentar situaciones de emergencia directa o indirectamente paralizando sus operaciones y afectando en gran medida las ventas de la empresa las cuales superan los 860 millones de dólares. (PRONACA, 2013), es por esto que se requiere tener respuestas inmediatas ante incidentes que puedan afectar su normal funcionamiento por la dependencia que tiene la empresa en la tecnología.

Se desea contribuir con un plan de recuperación de desastres para proteger los procesos críticos de la empresa ante eventos no esperados como fallas o catástrofes. Al estar ubicados en una ciudad con riesgos sísmicos y volcánicos es de gran responsabilidad de la organización el estar preparados con planes de recuperación de desastres para garantizar la continuidad de los procesos de negocio y salvaguardar la información antes casos de emergencia.

3. Capitulo III. Requisitos para el DRP

El siguiente capítulo comprende la etapa de iniciación, donde se definirá la política del DRP y la fase de requisitos de la etapa requisitos y estrategia del modelo ITSM propuesto por ITIL, donde se realizará el análisis de impacto en el negocio y el análisis de riesgo de PRONACA.

3.1. Iniciación

3.1.1. Política

La política definida a continuación está elaborada por el departamento de Operaciones de TI y el departamento de seguridad de la información conforme al formato que se encuentra en el Anexo B establecido por la compañía.

CATEGORIZACIÓN: Políticas administrativas
NEGOCIO: Corporativos **Fecha emisión:** 28/11/2015
PROCESO: Tecnología informática **Fecha publicación:**
ÁREA: Tecnología Informática **Fecha Última Actualización:**
POLÍTICA: Recuperación de desastres **Código:** TICPTIPT1

3.1.1.1. Objetivo

Definir los requerimientos de un plan de recuperación de desastres para ser desarrollado e implementado y describir los procesos de recuperación de los servicios de TI ante cualquier tipo de desastre que cause una interrupción grave.

3.1.1.2. Alcance

Esta política está dirigida al personal de gestión de TI de PRONACA que se encarga de asegurar la disponibilidad de los servicios tecnológicos y de que el plan de recuperación de desastres se desarrolle, pruebe y actualice.

3.1.1.3. Exposición de la política

- Realizar un análisis de impacto para determinar cómo el negocio se vería afectado por una interrupción de los servicios de TI.
- Realizar una evaluación de los riesgos para determinar las vulnerabilidades actuales de los servicios de TI.
- Mantener un inventario de los activos de TI actualizado tanto de hardware como de software.
- Tener identificadas las aplicaciones, sistemas y datos críticos para la empresa.
- Disponer de la documentación de los procedimientos a seguir en caso de un desastre.

3.1.1.4. Responsabilidades

- Administradores de bases de datos (DBA)
  Las siguientes responsabilidades aplica para los dos grupos de DBA's especialistas en bases de datos & sistemas operativos y redes & comunicaciones.
  - Mantenimiento de las instalaciones alternas.
  - Salvaguardar las copias de seguridad de los datos.
  - Determinar acuerdos de niveles de servicios con los proveedores de servicios.
  - Obtener la información de contacto tanto del equipo de recuperación de servicios como el de los proveedores de servicios.

- Determinar el método de comunicación con el equipo de recuperación de servicios en caso de un desastre.
- Documentar el plan de recuperación de desastres y almacenar copias fuera del sitio principal.
- Realizar pruebas anualmente del plan de recuperación de desastres, documentar las pruebas y actualizar el plan de ser necesario; esta responsabilidad es compartida con auditoria interna.

- Analistas y coordinadores
  - Realizar pruebas de legibilidad de las copias de seguridad de los datos al menos dos veces por año para comprobar la integridad y fiabilidad de los datos.
  - Realizar pruebas de funcionamiento de los sistemas restaurados.
- Gerente de Operaciones
  - Definir un equipo de recuperación de servicios con funciones y responsabilidades.
  - Coordinar el plan de recuperación de desastres.
- Director de TI
  - Realizar campañas de concientización sobre la importancia del plan de recuperación de desastres.
  - Activar el plan de recuperación de desastres, esta responsabilidad es compartida con el vicepresidente de desarrollo organizacional.

3.1.1.5. Anexos

N/A

_____	_____	_____
Elaborado por:	**Revisado por:**	**Aprobado por:**
Administrador de Base de datos	Supervisor Control Interno Gerente Auditor	Director Tecnología e Información

3.2. Requisitos

3.2.1. Análisis de impacto en el negocio (BIA)

3.2.1.1. Identificación de los procesos críticos del negocio

El primer paso para elaborar un análisis de impacto es identificar los procesos críticos del negocio que dependen o se apoyan en los sistemas tecnológicos.

Para definir como proceso crítico de negocio se consideró como factor más importante los ingresos que percibe la compañía. Para PRONACA los ingresos vienen de los procesos de ventas y recaudaciones que se lo realiza por negocio.

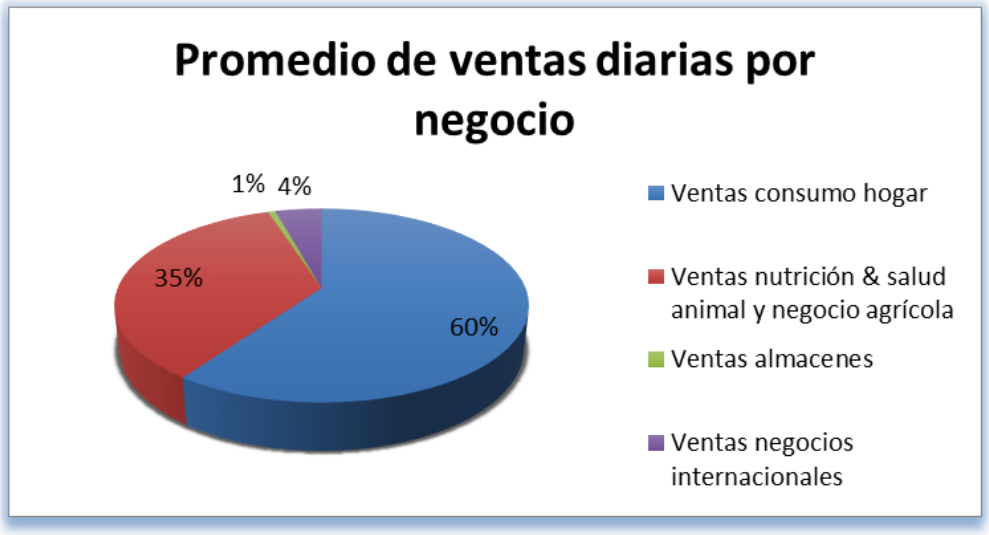


Figura 7. Promedio de ventas diarias por negocio.

Al ser los valores más representativos y de mayor impacto en el promedio de ventas diarias se define como críticos los procesos de negocio de gestión de ventas consumo hogar con un 60% del total de las ventas y gestión de ventas

nutrición & salud animal y negocio agrícola con 35%. Una vez realizadas las ventas la empresa tiene que realizar las recaudaciones, cobros o cuentas por cobrar por negocio a los clientes para que se haga efectivo el ingreso; es por esto que se definen como críticos los procesos de negocio de recaudaciones de consumo humano y recaudaciones nutrición & salud animal y negocio agrícola. Es importante mencionar que estos procesos son claves para la empresa y forman parte de la cadena de valor. Otros procesos críticos que no se encuentran dentro del alcance del proyecto son:

- Compras de materias primas, necesario para la producción del inventario.
- Pago a proveedores, importante para contar con el abastecimiento de los productos o servicios para la operación.
- Producción, indispensable para fabricar el inventario que va a ser comercializado.
- Gestión de nómina, requerido para el pago de las personas vinculadas laboralmente a la empresa.

Tabla 4. Procesos críticos de negocio.

Procesos de negocio	Descripción
Gestión de ventas consumo hogar	Proceso que contribuye a que las ventas de los productos de consumo humano se realicen y atender las necesidades de los consumidores para llegar a sus hogares.
Gestión de ventas nutrición & salud animal y negocio agrícola	Proceso que contribuye a que las ventas de los productos de nutrición & salud animal y negocio agrícola se realicen y atender las necesidades de los clientes.
Recaudaciones consumo hogar	Proceso que gestiona las cuentas por cobrar de del negocio de consumo hogar.
Recaudaciones nutrición & salud animal y negocio agrícola	Proceso que gestiona las cuentas por cobrar del negocio de nutrición & salud animal y negocio agrícola

3.2.1.2. Impacto en los procesos de negocio

El impacto es evaluado en el momento más crítico de cada proceso y los tipos de impacto que se van a considerar son económico, comercial, operacional, de imagen y legal para determinar la afectación en toda la organización si se interrumpe un proceso de negocio.

Los valores se especifican de manera cuantitativa para el impacto económico y de manera cualitativa para el impacto comercial, operacional, de imagen y legal debido a la complejidad de los procesos propios del negocio. A continuación se detalla la categoría de impacto:

- Impacto Nulo = 0
- Impacto Leve = 1
- Impacto Medio = 2
- Impacto Grave = 3
- Impacto Catastrófico = 4

La pauta que se tomará para la calificación del impacto se resume en la siguiente tabla:

Tabla 5. Pauta para valoración de impactos.

Tipos de impacto	**Criterios y evaluación**			
	Leve	**Medio**	**Grave**	**Catastrófico**
Económico	< de 1 millón dólares	De 1 a 3 millones dólares	De 3 a 7 millones dólares	> de 7 millones dólares
Comercial	Produce una interrupción leve en el suministro de servicios o productos con mínimo impacto en la operativa de los clientes. La pérdida de ventas se	Obliga al cliente a cambiar de proveedor de forma transitoria. Las ventas no realizadas no se recuperan.	Pérdida de algunos clientes de forma definitiva. Impacto leve en la cartera de prospectos.	Pérdida de clientes clave. Impacto grave en la cartera de prospectos.

	recupera al reanudar la actividad.			
Operacional	Produce retrasos en procesos no vitales.	Produce retrasos leves en procesos vitales.	Produce retrasos graves en funciones vitales.	Produce la interrupción inmediata de procesos vitales.
Imagen	Conocido solamente por algunos clientes. Sin presencia en los medios de comunicación.	Pérdida de confianza en un producto o servicio específico o en una parte de la organización. Comentarios adversos en medios locales.	Pérdida de confianza en una gama de productos o servicios o en varias áreas de la organización. Comentarios adversos en los medios nacionales.	Pérdida de la confianza del mercado y daños a la imagen de marca. Campaña continuada en los medios nacionales. Impacto en la bolsa.
Legal	Produce una falta leve en el cumplimiento de algún contrato.	Produce una falta en el cumplimiento de algún contrato que obliga a renegociar.	Produce una falta grave en el cumplimiento de algún contrato que acarrea responsabilidades legales.	Deja la organización al margen de la ley.

Tomado de: (Gaspar, 2010)

Tabla 6. Impacto cualitativo del proceso de gestión de ventas consumo hogar.

Gestión de ventas consumo hogar				
	Gravedad			
Impacto	4 horas	1 día	2 días	1 semana
Económico	1	2	3	4
Comercial	0	1	2	3
Operacional	1	2	3	4
Imagen	0	1	1	3
Legal	1	1	2	3

Adaptado de: (Gaspar, 2010)

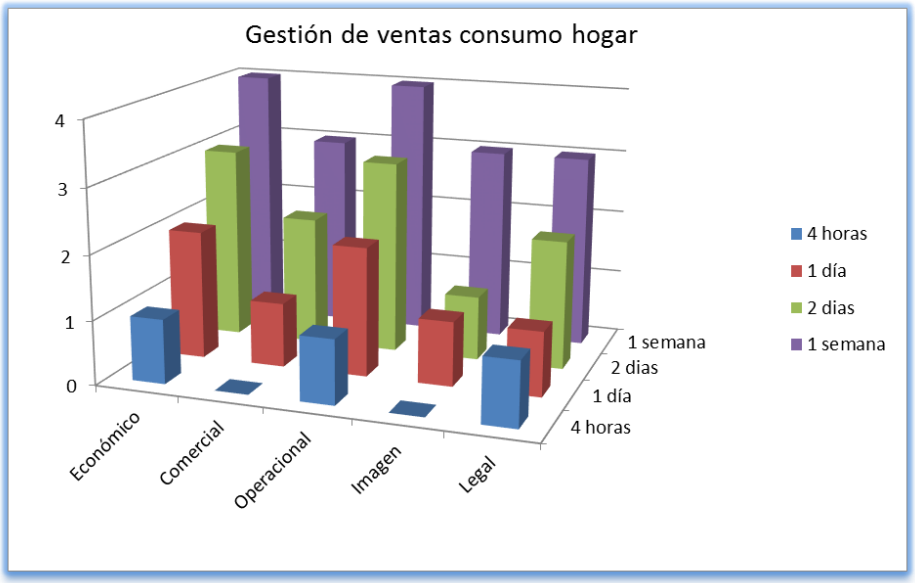


Figura 8. Impacto cualitativo del proceso de gestión de ventas consumo hogar.
Adaptado de: (Gaspar, 2010)

Como resultado del análisis de impacto en el proceso de gestión de ventas consumo hogar se puede evidenciar que en caso de una interrupción en este proceso puede afectar de manera significativa y en mayor medida al negocio en la parte económica y operacional. Económicamente afecta a los ingresos de la compañía ya que no se puede vender ni despachar el producto, pero

también puede afectar en costos adicionales que se deben incurrir como por ejemplo en el almacenaje del producto. Operacionalmente tiene un alto impacto en el negocio debido a que si no se vende el producto se puede parar la producción al ser un negocio en su mayoría de producción y comercialización de aves y cerdos, estos tienen que seguir alimentándose cayendo en costos adicionales; otros costos importantes a considerar son los operativos como horas extras y logísticos como transporte.

La parte comercial, imagen y legal también se ven gravemente afectadas ante una interrupción del proceso, en lo comercial impacta directamente a los clientes en este caso distribuidores zonales, cadenas de supermercado, etc. Quienes a su vez no pueden vender los productos al cliente final, esto puede dar lugar a pérdida de futuros negocios, participación de mercado, cambio de proveedor. En la parte de imagen la organización se vería afectada su credibilidad ante los clientes y organismos externos como entidades financieras. En lo legal la empresa se vería afectada al no poder cumplir con los proveedores con las obligaciones de pagos o emisiones de retenciones en los tiempos obligados por el ente fiscal, adicionalmente existiría incumplimiento en los contratos por la entrega a destiempo o no entrega del producto incurriendo en penalizaciones.

Tabla 7. Impacto cualitativo del proceso de gestión de ventas nutrición & salud animal y negocio agrícola.

Gestión de ventas nutrición & salud animal y negocio agrícola				
	Gravedad			
Impacto	4 horas	1 día	2 días	1 semana
Económico	1	2	3	4
Comercial	1	2	2	3
Operacional	1	1	2	3
Imagen	0	0	1	3
Legal	0	1	2	4

Adaptado de: (Gaspar, 2010)

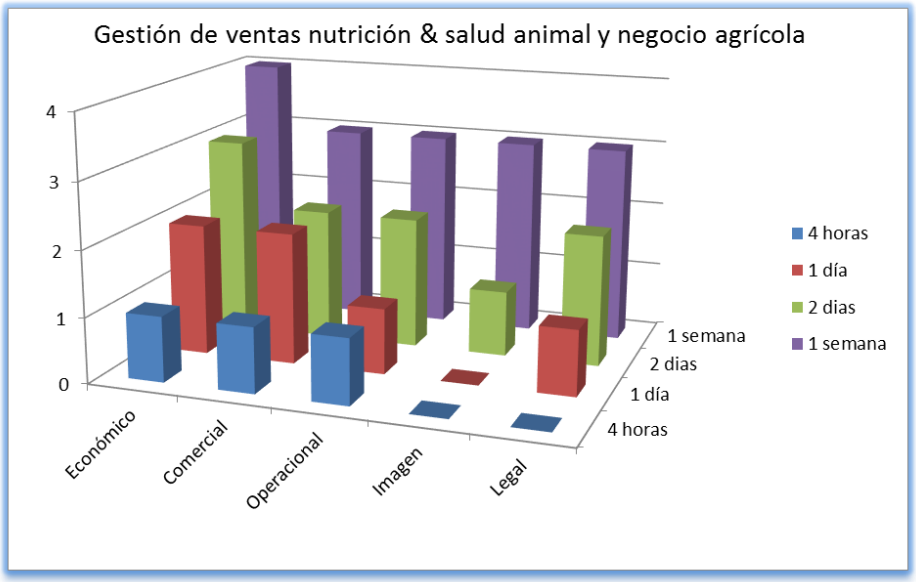


Figura 9. Impacto cualitativo del proceso de gestión de ventas nutrición & salud animal y negocio agrícola.
Adaptado de: (Gaspar, 2010)

El impacto ante la interrupción del proceso de gestión de ventas nutrición & salud animal y negocio agrícola puede afectar de manera importante en la parte económica ya que afecta directamente a los ingresos de la compañía al no poder vender el producto al cliente.

En lo comercial tiene impacto en el negocio ya que no se podrá satisfacer la necesidad del cliente provocando que este puede optar por la compra de producto a la competencia y la empresa perdería sus clientes. En lo operacional se detendría el proceso productivo, ya que la producción inicia en función a los pedidos de venta que se realizan diariamente. La imagen de la empresa se vería afectada ante los clientes perdiendo su credibilidad y legalmente se puede incurrir en incumplimiento de contratos o sensaciones tributarias por la no emisión de documentos legales como retenciones a tiempo.

Tabla 8. Impacto cualitativo del proceso recaudaciones consumo hogar.

Recaudaciones consumo hogar				
	Gravedad			
Impacto	4 horas	1 día	2 días	1 semana
Económico	1	2	3	4
Comercial	1	2	3	4
Operacional	1	1	2	3
Imagen	0	1	1	1
Legal	1	2	3	4

Adaptado de: (Gaspar, 2010)

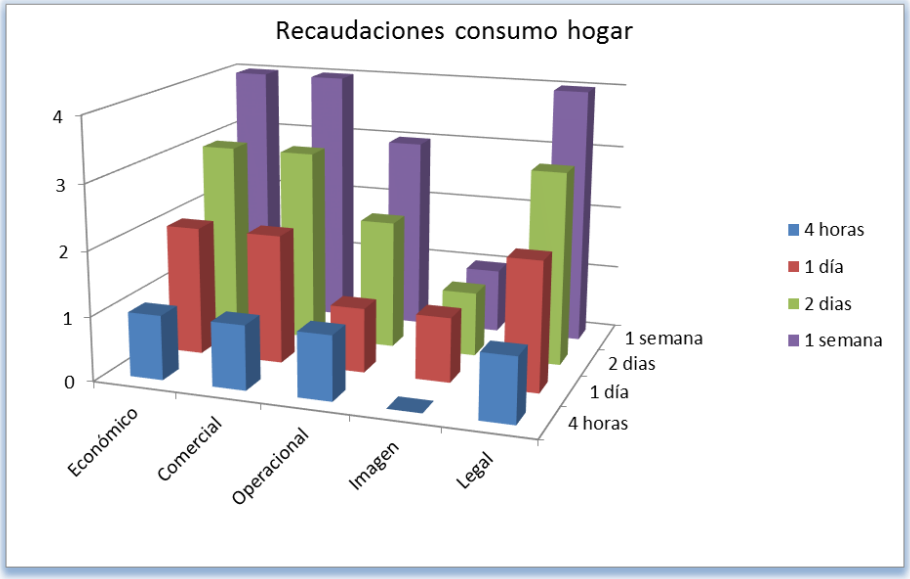


Figura 10. Impacto cualitativo del proceso de recaudaciones consumo hogar.
Adaptado de: (Gaspar, 2010)

El impacto más representativo en el proceso de recaudaciones consumo hogar corresponde al económico puesto que no se podrá realizar el cobro a los clientes afectando directamente a los ingresos de la compañía, también se debe incurrir en costos adicionales como son horas extras a los trabajadores.

En lo comercial afectaría con la venta no efectuada a clientes de contado, los cuales pueden optar por cambiar de proveedor.

El impacto operacional también quedaría afectado ya que al no percibir ingresos la empresa no podría continuar con sus procesos y cumplir sus obligaciones al no tener un flujo de caja que permita pagar a tiempo a los proveedores de suministros y materias primas. En la parte de imagen existiría un impacto mínimo hacia los clientes mientras que en la parte legal habría afectación ya que no se podrían registrar las retenciones de nuestros clientes con lo cual no se realizarían los reclamos de devolución de impuestos a la entidad fiscal.

Tabla 9. Impacto cualitativo del proceso de recaudaciones nutrición & salud animal y negocio agrícola.

Recaudaciones nutrición & salud animal y negocio agrícola				
	Gravedad			
Impacto	4 horas	1 día	2 días	1 semana
Económico	1	1	2	3
Comercial	2	2	2	3
Operacional	1	1	2	3
Imagen	1	2	2	3
Legal	1	1	2	3

Adaptado de: (Gaspar, 2010)

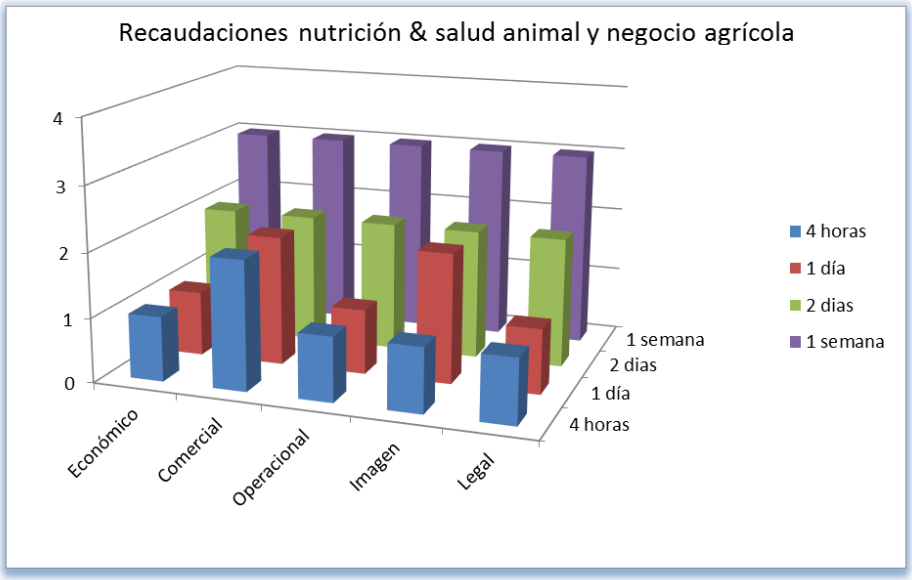


Figura 11. Impacto cualitativo del proceso de recaudaciones nutrición & salud animal y negocio agrícola.
Adaptado de: (Gaspar, 2010)

El impacto económico es importante en el proceso de recaudaciones nutrición & salud animal y negocio agrícola puesto que no se recibiría el ingreso por las ventas realizadas al no poder realizar la gestión de cobranzas, a diferencia de los demás procesos este se lo puede gestionar de forma manual por dos días hasta que se restablezca el servicio. Comercialmente impacta al negocio en cuento a las reclamaciones que puede existir por parte de cliente hasta provocar la pérdida del mismo.

En la parte operacional también se verían afectados otros procesos como el de compras a proveedores. La imagen se vería afectada en este caso del lado del proveedor al no poder pagar a tiempo por falta de flujo de dinero, en la parte legal de la misma manera que en el proceso de recaudaciones de consumo hogar no se podrían registrar las retenciones de los clientes y realizar la reclamación de devolución de impuestos a la entidad fiscal.

PRONACA al ser una empresa económicamente estable y solvente puede soportar la interrupción de los procesos de negocio hasta más de dos días pero se vería fuertemente impactada si el proceso no se restablece en una semana.

Los resultados del análisis de impacto se obtuvieron mediante las encuestas realizadas a los gerentes dueños de los procesos.

- Proceso gestión de ventas de consumo hogar - Gerente de consumo hogar logística.
- Proceso gestión de ventas nutrición & salud animal y negocio agrícola – Gerente de logística agropecuaria.
- Proceso recaudaciones consumo hogar – Gerente crédito y cobranzas comercial.
- Proceso recaudaciones nutrición & salud animal y negocio agrícola – Gerente crédito y cobranzas pecuario.

Las encuestas realizadas se encuentran en el Anexo C.

3.2.1.3. Determinación del MTD

Tiempo máximo de inactividad tolerable (MTD), se refiere el máximo tiempo en que una empresa puede tolerar la ausencia o la disponibilidad de un proceso en particular. Los procesos de negocios tienen diferentes MTD y si el proceso es de misión crítica el MTD será más corto. El MTD se compone de dos elementos que son la suma del tiempo objetivo de recuperación más el tiempo de trabajo en recuperación. (Snedaker, 2007)

La definición del MTD fue proporcionada por los gerentes responsables de los procesos de negocio.

Tabla 10. Tiempo máximo de inactividad tolerable.

Procesos de negocio	MTD
Gestión de ventas consumo hogar	4 horas
Gestión de ventas nutrición & salud animal y negocio agrícola	1 día
Recaudaciones consumo hogar	2 días
Recaudaciones nutrición & salud animal y negocio agrícola	2 días

Adaptado de: (NIST, 2010)

3.2.1.4. Determinación del RTO y WRT

Tiempo objetivo de recuperación (RTO) es el tiempo disponible para recuperar los sistemas y recursos interrumpidos. Tiempo de trabajo en recuperación (WRT) es el tiempo necesario para que los procesos de negocio vuelvan a funcionar una vez restaurados los sistemas. (Snedaker, 2007)

La definición del RTO y WRT fue realizado por el departamento de TI con todas las personas dueñas de las aplicaciones donde se analizó las necesidades del negocio y los recursos de TI.

Para determinar cuáles son los servicios de TI que intervienen en cada actividad de los procesos de negocio, se realizó el levantamiento de los procesos que se encuentran en el Anexo A.

Tabla 11. Tiempo objetivo de recuperación y Tiempo de trabajo en recuperación.

Proceso de negocio	Servicios	RTO	WRT
Gestión de ventas consumo hogar	ERP	1 Hora	2 Horas
	Sistema de gestión de pedidos y cobros	2 Horas	1 Hora
	Mensajería	2 Horas	1 Hora
	Bus de integración	2 Horas	1 Hora
	Sistema optimizador de rutas	3 Horas	1 Hora
	Sistema de gestión de inventarios	3 Horas	1 Hora
	Sistema de registro de pesos	3 Horas	1 Hora
	Sistema de etiquetas	2 Horas	1 Hora

	Integración en nube	2 Horas	1 Hora
	Sistema de facturación electrónica	-	-
	Gateway	2 Horas	1 Hora
	Enlace de red interno	3 Horas	1 Hora
	Enlace de red externo	3 Horas	1 Hora
	Firewall	3 Horas	1 Hora
	Internet	2 Horas	1 Hora
	Sistema de Impresión	3 Horas	1 Hora
Gestión de ventas nutrición & salud animal y negocio agrícola	ERP	1 Hora	2 Horas
	Mensajería	2 Horas	1 Hora
	Bus de integración	2 Horas	1 Hora
	Sistema de gestión de pedidos Plantas	2 Horas	1 Hora
	Correo	-	-
	Enlace de red interno	3 Horas	1 Hora
	Enlace de red externo	3 Horas	1 Hora
	Firewall	3 Horas	1 Hora
	Internet	2 Horas	1 Hora
	Sistema de Impresión	3 Horas	1 Hora
Recaudaciones consumo hogar	ERP	1 Hora	2 Horas
	Sistema de gestión de pedidos y cobros	2 Horas	1 Hora
	Mensajería	2 Horas	1 Hora
	Bus de integración Internet	2 Horas	1 Hora
	Enlace de red interno	3 Horas	1 Hora
	Enlace de red externo	3 Horas	1 Hora
	Firewall	3 Horas	1 Hora
	Internet	2 Horas	1 Hora
	Sistema de Impresión	3 Horas	1 Hora
Recaudaciones nutrición & salud animal y negocio agrícola	ERP	1 Hora	2 Horas
	Enlace de red interno	3 Horas	1 Hora
	Enlace de red externo	3 Horas	1 Hora
	Firewall	3 Horas	1 Hora
	Internet	2 Horas	1 Hora
	Sistema de Impresión	3 Horas	1 Hora

Adaptado de: (NIST, 2010)

3.2.1.5. Determinación del RPO

El punto objetivo de recuperación (RPO) es la cantidad de pérdida de los datos que el negocio puede tolerar, esto depende de las copias de seguridad si son diarias, semanales o mensuales. (Snedaker, 2007)

Respecto al RPO, se realizó el análisis conjuntamente entre el equipo de operaciones de TI y proveedores para determinar las mejores opciones de copias de seguridad y definir tiempos cercanos a la realidad.

Tabla 12. Punto objetivo de recuperación.

Servicios	RPO
ERP	5 Minutos
Sistema de gestión de pedidos y cobros	1 día
PDA	1 día
Mensajería	1 día
Bus de integración	1 día
Sistema optimizador de rutas	1 día
Sistema de gestión de inventarios	6 horas
Sistema de registro de pesos	1 día
Sistema de etiquetas	-
Integración en nube	1 día
Sistema de facturación electrónica	1 minuto
Correo	1 minuto
Sistema de gestión de pedidos Plantas	1 día
ERP Plantas	1 día
Sistema de impresión	1 día
Sistema de respaldos	1 día

Adaptado de: (NIST, 2010)

3.2.2. Análisis de riesgo (RA)

El análisis de riesgo es el “estudio de las amenazas a que están sometidos los activos de una organización y evaluación de su vulnerabilidad”. (Gaspar, 2010)

Para el análisis de riesgo se va a tomar como referencia la norma ISO 27005.

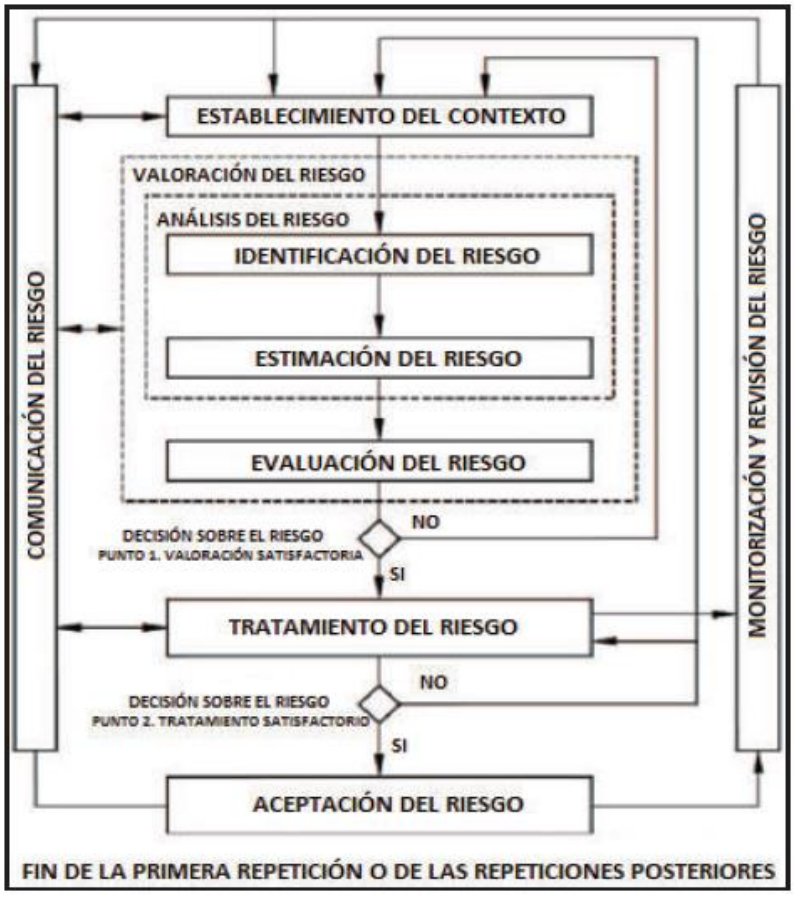


Figura 12. Proceso de gestión del riesgo en la seguridad de la información. Tomado de: (ISO, 2011)

3.2.2.1. Identificación de riesgos

La identificación de riesgos es el “proceso para encontrar, enumerar y caracterizar los elementos de riesgo”. (ISO, 2011)

3.2.2.1.1. Identificación de activos

Para realizar la valoración de los activos de la empresa es necesario identificarlos. Los activos se van a diferenciar en dos clases: activos primarios y activos de soporte.

- Activos Primarios.- Son los procesos y la información central de la organización. Estos se dividen en procesos y actividades de negocio e información.
    - Los procesos y actividades de negocio contienen tecnología y son necesarios para el cumplimiento de la misión de la organización ya que pueden afectar si estos se interrumpen o degradan.

Tabla 13. Procesos y actividades de negocio.

Procesos	Actividades
Gestión de ventas consumo hogar	GV1.1.1 Asignar Stock por vendedor GV1.1.2 Registrar pedidos en PDA GV1.1.3 Registrar orden de venta en ERP GV1.2.1 Regularizar insuficiencias de inventario GV1.2.2 Reservar stock para despachar órdenes de venta GV1.3.1 Asignar rutas de distribución GV1.3.2 Generar reportes para *picking* y *packing* GV1.4.1 Despachar inventarios GV1.4.3 Facturar órdenes de venta GV1.4.4 Generar Guías de remisión
Gestión de ventas nutrición & salud animal y negocio agrícola	GVN1.1.1 Generar la necesidad de alimento el cliente GVN1.1.2 Receptar pedido del cliente GVN1.1.3 Registrar o modificar pedido

	GVN1.1.4 Generar orden de venta GVN1.1.5 Descargar orden de venta para despacho GVN1.1.6 Generar ticket de peso entrada GVN1.1.8 Generar *outbound* GVN1.1.9 Generar reporte de carga GVN1.1.10 Generar ticket de carga GVN1.1.11 *Picking* de producto en anden GVN1.1.13 Generar ticket de peso salida GVN1.1.14 Generar factura y guía de remisión
Recaudaciones consumo hogar	RE1.1.1 Seleccionar facturas para cobro RE1.1.2 Identificar canal de cobro RE1.1.3 Generar la remesa manual de cobro RE1.1.4 Generar remesa automática de cobro RE1.1.5 Exportar remesa de cobro RE1.1.8 Gestionar cobranza de acuerdo a canal RE1.1.9 Identificar el cliente de pago RE1.1.10 Emitir y entregar el recibo de cobro al cliente RE1.2.4 Imprimir resumen de caja RE1.2.5 Sincronizar PDA RE1.2.7 Agrupar recaudos RE.1.2.8 Importar recaudos RE1.2.9 Revisar en conjunto los cheques al día y post-fechados RE1.2.13 Registrar cobros RE1.2.14 Realizar el cuadre de caja y finalizar el asiento RE1.2.17 Generar consolidación bancarias
Recaudaciones nutrición & salud animal y negocio agrícola	REN1.1.1 Seleccionar facturas para cobro REN1.1.2 Generar la remesa manual de cobro RE1.2.14 Registrar cobros RE1.2.15 Realizar el cuadre de caja y finalizar el asiento RE1.2.18 Generar consolidación bancarias

Adaptado de: (Guanoluisa & Maldonado, 2015)

- La información primaria o estratégica que es vital para la ejecución de la misión del negocio.

Tabla 14. Información Primaria

Fuente	Información
Base de datos ERP	Finanzas • Cartera de clientes • Cartera de proveedores • Contabilidad general • Contabilidad de costos • Presupuestos • Tesorería • Activos fijos • Gestión tributaria Logística • Control de inventarios • Gestión de ventas • Gestión de compras Producción • Ordenes de fabricación • Formulas y rutas de ítems • Consumo de materiales Planificación • MRP Gestión de datos comunes • Clientes • Proveedores • Artículos • Almacenes Modelizador empresarial • Roles • Perfiles
Base de datos Sistema de gestión de pedidos y cobros	Ventas • Pedidos Cobros • Cartera de clientes
Base de datos sistema optimizador de rutas	Clientes Pedidos
Base de datos sistema de gestión de inventarios	Control y gestión de Inventarios.

Base de datos sistema de facturación electrónica	Facturación Cartera de clientes Cartera de proveedores
Base de datos sistema de gestión de pedidos plantas	Ventas • Pedidos
Base de datos ERP plantas	Finanzas • Cartera de clientes • Cartera de proveedores • Compras agrícolas • Control de fideicomisos Logística • Gestión de ventas • Gestión de compras • Gestión de transferencias Producción • Consumo de materias primas Transporte • Conciliación y pago a transportistas
Base de datos sistema de respaldos	Respaldos de todas las bases de datos de la compañía

Adaptado de: (Guanoluisa & Maldonado, 2015)

- Activos de Soporte.- Son los componentes de hardware, software, redes, personal, sitio y estructura de la organización de los cuales dependen los activos primarios. (ISO, 2011)

Tabla 15. Servidores y aplicaciones.

Aplicación	Sistema Operativo	Base de Datos	Memoria GB	Procesa.	Almace. GB	Virtual Físico	Ubicación	Responsables
ERP	AIX 7.1 AIX 6.1	Oracle 11g N/A	110 70	10 8	7200 120	Virtual Virtual	DC Inverna Quito DC Inverna Quito	Administrador BD Analista Sistemas
Sistema de gestión de pedidos y cobros	Windows Server 2003 Windows Server 2003 Windows Server 2003 Windows Server 2003 Windows Server 2003	Sql 2000 Sql 2000 Sql 2000 Sql 2000 Sql 2000	4 2 4 2 4	2 1 2 1 1	125 100 115 80 300	Virtual Físico Virtual Físico Físico	DC Inverna Quito Guayaquil Metro park DC Inverna Quito Regional Santo Domingo CD Montecristi	Administrador BD Analista Sistemas
PDA	Windows mobile 6.1 y 6.5	FoxPro	N/A	N/A	N/A	N/A	N/A	Analista Sistemas
Mensajería Bus de integración	AIX 7.1	N/A	12	0.5	130	Virtual	DC Inverna Quito	Administrador BD Arquitecto App
Sistema optimizador de rutas	Windows 7 Windows 7 Windows 7	Access Access Access	4 4 4	1 1 1	500 500 500	Físico Físico Físico	CD Quito CD Quito CD Guayaquil	Administrador BD Analista Sistemas

	Windows 7	Access	4	1	500	Físico	CD Guayaquil	
Sistema de gestión de inventarios	Red Hat Ent Linux 4 Red Hat Ent Linux 4	Oracle 10g Oracle 10g	4 4	4 2	210 460	Físico Físico	CD Quito CD Guayaquil	Administrador BD Analista Sistemas Coord Negocio
Sistema de registro de pesos	Windows Server 2008 Windows Server 2003 Windows Server 2003 Windows Server 2003 Windows Server 2003	Sql 2005 Sql 2005 Sql 2005 Sql 2005 Sql 2005	4 2 1 2 4	4 2 2 2 4	500 500 500 500 500	Físico Físico Físico Físico Físico	CD Quito CD Guayaquil CD Cuenca CD Montecristi Valle Hermoso	Administrador BD Coord Proyectos
Sistema de etiquetas	Windows 7 Windows 7 Windows 7 Windows 7 Windows 7 Windows 7 Windows 7 Windows 7 Windows 7 Windows 7	N/A N/A N/A N/A N/A N/A N/A N/A N/A N/A	4 4 4 4 4 4 4 4 4 4	1 1 1 1 1 1 1 1 1 1	500 500 500 500 500 500 500 500 500 500	Físico Físico Físico Físico Físico Físico Físico Físico Físico Físico	CD Quito CD Quito CD Guayaquil CD Guayaquil CD Cuenca CD Cuenca CD Montecristi CD Montecristi Valle Hermoso Valle Hermoso	Soporte Usuarios
Integración en nube	AIX 7.1 *Appliance*	Oracle 11g N/A	4 8	0.5 6	60 65	Virtual Virtual	DC Inverna Quito DC Inverna Quito	Administrador BD Arquitecto App
Sistema de facturación electrónica	Ubuntu 14 Ubuntu 14 Ubuntu 14	N/A Postgre 9 N/A	8 8 8	2 2 2	200 250 200	Virtual Virtual Virtual	Amazon Web Ser Amazon Web Ser Amazon Web Ser	Arquitecto App

	Ubuntu 14	N/A	8	2	200	Virtual	Amazon Web Ser	
Gateway	*Appliance*	*Appliance*	2	2	75	Físico	DC Inverna Quito	Administrador BD
Correo	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Administrador BD
Sistema de gestión de pedidos Plantas	Windows Server 2008	Sql Server 2008	4	2	250	Virtual	DC Inverna Quito	Administrador BD Coord Proyectos
ERP Plantas	Windows Server 2008 Windows Server 2008 Windows Server 2008 Windows Server 2008 Windows Server 2008 Windows Server 2008	Sql 2005 N/A Sql 2005 N/A Sql 2005 N/A	32 4 16 4 8 4	6 2 4 2 4 2	230 70 250 150 500 70	Virtual Virtual Virtual Virtual Físico Virtual	DC Inverna Quito DC Inverna Quito DC Inverna Quito DC Inverna Quito Planta Puembo DC Inverna Quito	Administrador BD Analista Sistemas
Sistema de impresión	Windows Server 2008 Windows Server 2008	Sql 2008 N/A	8 8	4 4	300 500	Virtual	DC Inverna Quito	Administrador BD
Sistema de respaldos	AIX 7.1	DB2	12	0.5	1700	Virtual	DC Inverna Quito	Administrador BD

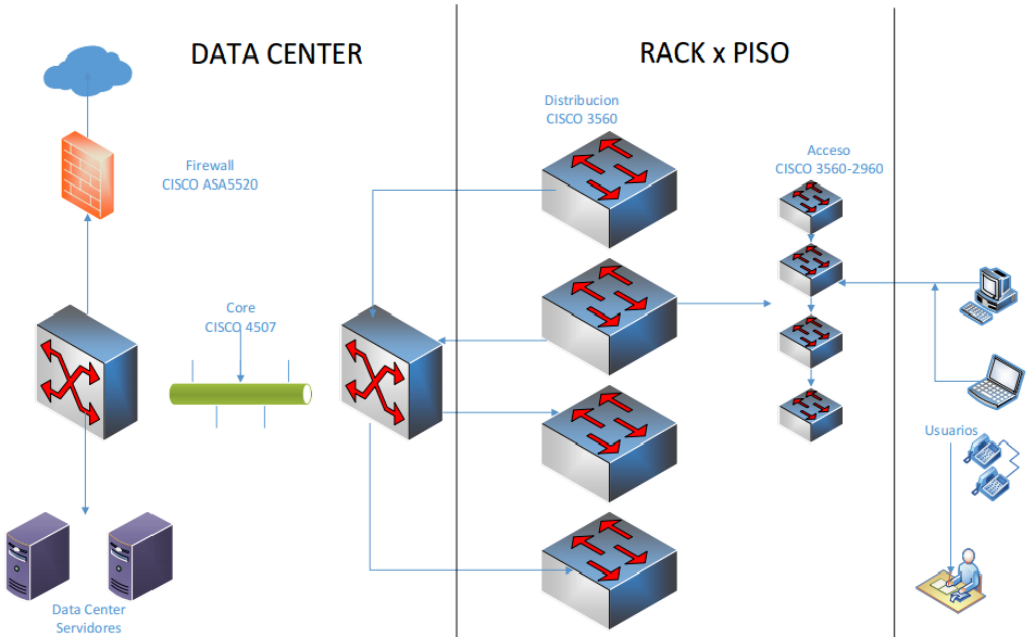


Figura 13. Esquema de red Edificio Inverna.

Tabla 16. Equipos de comunicación.

Ubicación	*Switches* 4507	*Switches* 3560	*Switches* 2960	*Routers* 2801	*Access Point* 2702	*Firewall* 5520
DC Inverna Quito	2	5	18	7	23	1
CD Quito	0	0	6	2	16	0
CD Guayaquil	0	0	7	2	15	0
CD Montecristi	0	0	4	2	2	0
CD Cuenca	0	0	3	2	1	0
Guayaquil Metro park	0	0	5	2	5	0
Regional Santo Domingo	0	0	4	2	3	0
Valle Hermoso	0	0	8	2	3	0
Planta Puembo	0	0	8	2	6	0

Tabla 17. Impresoras.

Ubicación	Proceso de negocio	Modelo	Total
CD Quito	Gestión de ventas consumo hogar Recaudaciones consumo hogar	MS812de MX611dhe	3 1
CD Guayaquil	Gestión de ventas consumo hogar Recaudaciones consumo hogar	MS812de MX611dhe	3 1
CD Montecristi	Gestión de ventas consumo hogar Recaudaciones consumo hogar	MS812de MX611dhe	1 1
CD Cuenca	Gestión de ventas consumo hogar Recaudaciones consumo hogar	MS812de MX611dhe	1 1
Regional Santo Domingo	Gestión de ventas consumo hogar Recaudaciones consumo hogar	MS812de MX611dhe	1 1
Planta Puembo	Gestión de ventas nutrición & salud animal y negocio agrícola	MS812de	1
Planta Durán	Gestión de ventas nutrición & salud animal y negocio agrícola	MS610de	1
Planta Quevedo	Gestión de ventas nutrición & salud animal y negocio agrícola	MS812de	1
Bodega Amaguaña	Gestión de ventas nutrición & salud animal y negocio agrícola	MX611dhe	1
Bodega Durán	Gestión de ventas nutrición & salud animal y negocio agrícola	MS610de	1
Inverna Quito	Recaudaciones consumo hogar Recaudaciones nutrición & salud animal y negocio agrícola	MS812de MX611dhe	1 1
Regional Guayaquil	Recaudaciones consumo hogar	MS812de	1
Durán	Recaudaciones nutrición & salud animal y negocio agrícola	MX611dhe	1

Tabla 18. Recurso Humano.

Recurso Humano	Total de Recurso Humano	Servicios
Administrador de base de datos	4	• ERP • Sistema de gestión de pedidos y cobros • Mensajería • Bus de integración • Sistema optimizador de rutas • Sistema de gestión de inventarios • Sistema de registro de pesos • Integración en nube • *Gateway* • Correo • Sistema de gestión de pedidos Plantas • ERP Plantas • Sistema de impresión • Sistema de respaldos • *Gateway* • Enlace de red interno • Enlace de red externo • *Firewall* • Internet
Analista de sistemas	3	• ERP • Sistema de gestión de pedidos y cobros • PDA • Sistema optimizador de rutas • Sistema de gestión de inventarios • ERP Plantas
Arquitecto de aplicaciones	1	• Mensajería • Bus de integración • Integración en nube • Sistema de facturación electrónica
Coordinador de negocio	1	• Sistema de gestión de inventarios
Coordinador de proyectos	2	• Sistema de registro de pesos • Sistema de gestión de pedidos Plantas
Soporte Usuarios	1	• Sistema de etiquetas

Proveedores	12	• ERP (1) • Sistema de gestión de pedidos y cobros – PDA (1) • Mensajería – Bus de integración (1) • Sistema optimizador de rutas (1) • Sistema de gestión de inventarios (1) • Sistema de registro de pesos (1) • Integración en nube (1) • Sistema de gestión de pedidos Plantas (1) • Sistema de impresión (1) • Sistema de respaldos (1) • Enlace de red externo – Internet (1) • *Firewall* (1)

La Tabla 18. Recurso Humano muestra el total de recurso humano requerido para dar disponibilidad de los servicios de TI para los cuatro procesos de negocio.

3.2.2.1.2. Valoración de activos

Los criterios de valoración de activos se establecen de acuerdo a la importancia y dependencia de estos en los procesos de negocio. La categorización para la evaluación es:

- Bajo = 1
- Moderado = 2
- Alto = 3
- Crítico = 4

En la siguiente tabla se detallan las pautas de evaluación para la valoración de activos.

Tabla 19. Pauta para valoración de activos.

Atributos	Criterios y evaluación			
	Bajo	**Moderado**	**Alto**	**Crítico**
Dependencia	Ningún otro activo depende de este para entregar servicios a usuarios.	Pocos activos dependen de este para entregar servicio a usuarios.	Una gran cantidad de activos dependen de este para entregar servicios a usuarios.	Todos los activos dependen de este para entregar servicios a usuarios.
Funcionalidad	Activos con capacidades tecnológicas muy limitadas.	Activo con capacidades tecnológicas limitadas.	Activo con capacidades tecnológicas avanzadas.	Activo con capacidades tecnológicas de última generación
Confidencialidad **Integridad** **Disponibilidad**	La divulgación, modificación y no disponibilidad del activo puede afectar de forma insignificante la entrega de servicios a usuarios.	La divulgación, modificación y no disponibilidad del activo puede afectar en parte la entrega de servicios a usuarios.	La divulgación, modificación y no disponibilidad del activo puede afectar significativamente la entrega de servicios a usuarios.	La divulgación, modificación y no disponibilidad del activo puede afectar totalmente la entrega de servicios a usuarios.

Adaptado de: (Guanoluisa & Maldonado, 2015)

Tabla 20. Valoración de activos.

Activos	Atributos			Valoración
	Dependencia	Funcionalidad	Confidencialidad Integridad y Disponibilidad	
ERP	4	4	4	64
Sistema de gestión de pedidos y cobros	4	3	4	48
PDA	4	3	4	48
Mensajería	4	4	4	64
Bus de integración	4	4	4	64
Sistema optimizador de rutas	3	3	3	27
Sistema de gestión de inventarios	2	3	3	18
Sistema de registro de pesos	3	3	3	27
Sistema de etiquetas	2	2	2	8
Integración en nube	4	4	4	64
Sistema de facturación electrónica	4	4	4	64
Gateway	2	1	2	4
Correo	1	4	1	4
Sistema de gestión de pedidos Plantas	4	3	4	28
ERP Plantas	4	4	4	64
Sistema de respaldos	4	4	4	64
Enlace de red interno	4	4	4	64
Enlace de red externo	4	4	4	64
Firewall	4	4	4	64
Internet	4	4	4	64
Sistema de impresión	4	4	4	64

Adaptado de: (Guanoluisa & Maldonado, 2015)

El valor del activo es igual a dependencia * funcionalidad * (confidencialidad, integridad y disponibilidad).

Una vez que se ha determinado la dependencia de los activos primarios y secundarios de los procesos críticos de negocio, es necesario identificar el tipo de vulnerabilidades que presentan aquellos, así como sus amenazas.

Para (Axelos, 2011) la vulnerabilidad es “una debilidad que podría ser aprovechada por una amenaza” y una amenaza es “cualquier cosa que podría aprovechar una vulnerabilidad. Cualquier causa potencial de un incidente puede ser considerada una amenaza”. Existen varios tipo de amenazas que pueden causar daños a los activos de la empresa estos pueden ser de origen natural o humano y podrían ser accidentales o deliberadas. (ISO, 2013)

Para identificar el origen de la amenaza se utilizará la letra A (Accidentales), D (Deliberadas) y E (Ambientales). (ISO, 2011)

Tabla 21. Vulnerabilidades y amenazas.

Tipo de Amenaza	Fuente de Amenaza	Origen	Vulnerabilidad
Eventos naturales	Fenómenos sísmicos	E	Se tiene un plan de contingencia únicamente para ciertas aplicaciones y el sitio alterno soporta de la misma manera ciertas aplicaciones.
	Fenómenos volcánicos	E	Se tiene una protección a las condensadoras la cual no garantiza el 100% de protección de ceniza afectando el sistema de enfriamiento al centro de datos.
Pérdida de servicios esenciales	Perdida de suministro de energía.	A,D,E	Se cuenta con una planta generadora de energía que abastece al centro de datos, en caso de daño de la planta de energía no se cuenta con otra planta alterna.
	Falla en el equipo de telecomunicaciones	A,D	No se tiene en sitio alta disponibilidad en los equipos de borde de los proveedores de servicios de internet (ISP).

Fallas técnicas	Falla de equipos	A	Equipos antiguos fuera de garantía y no se encuentran bajo contrato de mantenimiento.
	Mal funcionamiento de equipos	A	No existe un sistema de monitoreo de *logs* de los equipos.
	Mal funcionamiento de software	A	No se cuenta con un ambiente de calidad o pre producción. No se aplica la política de control de cambios en todos los sistemas de información.
Acciones no autorizadas	Corrupción de datos	D	Usuarios con privilegios para modificar información en los sistemas.
	Procesamiento ilegal de datos	D	No se aplica la política de resguardo de usuarios y contraseñas.
	Hacking	D	Falta de actualizaciones en los servidores, redes y perímetro. Usuarios con acceso a toda la red de servidores. No se tiene activado el *firewall* a nivel de servidores y aplicaciones.
	Sabotaje interno	A,D	Falta de cámaras de grabación en el centro de datos. *Racks* sin llave de seguridad. No se tiene definido la responsabilidad de la llave de ingreso al data center.
	Errores humanos	A	Trabajo no supervisados y negligencia del personal.

Adaptado de: (ISO, 2011)

3.2.2.1.3. Identificación de controles existentes

La presencia de vulnerabilidades y amenazas a los activos de TI pueden generar eventos de riesgo que deben ser mitigados a través de la implementación de controles que permitan reducir su impacto o su probabilidad de ocurrencia.

La naturaleza de los controles permite mitigar los riesgos y facilitar el tratamiento de los incidentes y de los eventos de una manera más eficaz y proactiva. (ISO, 2011)

Para cada uno de los tipos de amenaza identificados anteriormente, a continuación se detallan los controles que actualmente se encuentran implementados en la plataforma y activos de TI.

Tabla 22. Controles existentes.

Tipo de Amenaza	Controles	Descripción
Daño físico	Sistema contra incendios	El centro de datos cuenta con un sistema de detección de incendios con gas FM200 que es un agente extintor. Adicionalmente se realizan pruebas y el mantenimiento cada tres meses para su correcto funcionamiento.
	Sistema de humedad	El centro de datos tiene un detector de humedad el cual envía notificaciones vía correo electrónico, también se realizan pruebas y el mantenimiento cada tres meses.
	Sistema de enfriamiento	El centro de datos posee 3 aires acondicionados los cuales rotan automáticamente para 1 estar de respaldo. Adicionalmente se tiene un sistema de monitoreo y de alertas de temperatura vía correo electrónico. Las pruebas y el mantenimiento se lo realiza cada 3 meses
	Sistema de control de agua	El centro de datos cuenta con un sistema de detección de agua el cual envía alertas vía correo electrónico, adicionalmente se realizan pruebas y mantenimiento cada tres meses.
Pérdida de servicios esenciales	UPS	El centro de datos tiene UPS que soportan la energía por un lapso de 20 minutos.
	ATS	El centro de datos cuenta con ATS el cual permite la transferencia de alimentación eléctrica entre dos fuentes para equipos que no soportan doble entrada eléctrica.

Fallas técnicas	Contrato de mantenimiento de equipos.	Se tiene contrato de mantenimiento para en el caso de dañarse una parte o equipo que requiera ser reemplazado.
	Configuración de almacenamiento	Configuración de almacenamiento en *RAID* 5 y *RAID*10, adicionalmente por cada caja de almacenamiento se tiene un disco en *hot spare*.
	Redundancia en equipos	Todos los servidores, almacenamiento y *switches* tienen redundancia de red y fibras.
	Respaldos	Se tiene respaldos de los sistemas de información de acuerdo a la política establecida en cintas magnéticas mediante la herramienta de TSM.
	Software licenciado	El software se encuentra licenciado y se cuenta con soporte de los fabricantes.
Acciones no autorizadas	Antivirus	La empresa con un antivirus para la protección de servidores Windows.
	Firewall	Se tiene un control de acceso a la red de datos.
	Uso de recursos de red	Se lleva un monitoreo constante de la red y un control de acceso de internet.
	Usuario y contraseñas	Se tiene implementado la política de usuarios y contraseñas.
	Acceso al centro de Datos	Se tiene un sistema de acceso al centro de datos, adicionalmente bitácora de registro de acceso.
	Auditorías internas y externas	Se realizan auditorías internas y externas para garantizar la eficiencia y eficacia de los controles establecidos en los procesos de negocio.

Adaptado de: (Guanoluisa & Maldonado, 2015)

3.2.2.2. Estimación del riesgo

La estimación del riesgo es un “proceso de comparar los resultados del análisis de riesgos con los criterios de riesgo para determinar si el riesgo y/o su magnitud es aceptable o tolerable”. (ISO, 2011)

3.2.2.2.1. Valoración del impacto

La valoración de impacto se realizó a todos los activos de soporte identificados previamente en un comité de TI. Para esto se tomó como referencia los siguientes criterios.

Tabla 23. Pauta para valoración de impacto.

Valoración	Impacto	Descripción
1	Bajo	El impacto entre la confidencialidad, integridad, y disponibilidad es mínimo.
2	Medio	El impacto entre la confidencialidad, integridad, y disponibilidad es medio.
3	Alto	El impacto entre la confidencialidad, integridad, y disponibilidad es alto.

Tomado de: (Guanoluisa & Maldonado, 2015)

El valor del impacto se calcula en base al promedio entre los criterios de confidencialidad, integridad y disponibilidad; si el valor es diferente a un número entero, el decimal se redondea al inmediato superior siempre y cuando sea igual o mayor a 5. A continuación se muestra un ejemplo de esta valoración, mientras que en la Tabla 29. Evaluación del riesgo activos críticos y Tabla 30. Evaluación del riesgo activos importantes se encuentra el detalle completo de la valoración realizada.

Tabla 24. Ejemplo valoración de impacto.

Tipo de Amenaza	Fuente de Amenaza	Vulnerabilidad	Confidencialidad Integridad Disponibilidad	Impacto
Eventos naturales	Fenómenos sísmicos	Se tiene un plan de contingencia únicamente para ciertas aplicaciones y el sitio alterno soporta de la misma manera ciertas aplicaciones.	1 1 3	2
	Fenómenos volcánicos	Se tiene una protección a las condensadoras la cual no garantiza el 100% de protección de ceniza afectando el sistema de enfriamiento al centro de datos.	1 1 3	2

Adaptado de: (Guanoluisa & Maldonado, 2015)

3.2.2.2.2. Valoración de incidentes

La valoración de incidentes se realizó a todos los activos de soporte con el equipo de operaciones de TI. Para la valoración de la probabilidad se tomó como referencia los siguientes criterios.

Tabla 25. Pauta para valoración de probabilidad de incidentes.

Valoración	Probabilidad	Descripción
1 (0 – 25)%	Poco Probable	Probabilidad muy baja de que una amenaza explote una vulnerabilidad.
2 (26 – 50)%	Medianamente Probable	Probabilidad baja de que una amenaza explote una vulnerabilidad.
3 (51 – 75)%	Probable	Probabilidad alta de que una amenaza explote una vulnerabilidad.
4 (76 – 100)%	Muy Probable	Probabilidad muy alta de que una amenaza explote una vulnerabilidad

Tomado de: (Guanoluisa & Maldonado, 2015)

De manera similar a la valoración del impacto, a continuación se muestra un ejemplo de la aplicación de las pautas para la valoración de la probabilidad de incidentes.

Tabla 26. Ejemplo valoración de probabilidad de incidentes.

Tipo de Amenaza	Fuente de Amenaza	Vulnerabilidad	Probabilidad
Eventos naturales	Fenómenos sísmicos	Se tiene un plan de contingencia únicamente para ciertas aplicaciones y el sitio alterno soporta de la misma manera ciertas aplicaciones.	1
	Fenómenos volcánicos	Se tiene una protección a las condensadoras la cual no garantiza el 100% de protección de ceniza afectando el sistema de enfriamiento al centro de datos.	1

Adaptado de: (Guanoluisa & Maldonado, 2015)

3.2.3. Evaluación de riesgo

La evaluación de riesgo es el “proceso global de identificación, análisis y estimación de riesgos.” (ISO, 2011)

Para la evaluación del riesgo se van a clasificar los activos en tres grupos de acuerdo a su importancia, según la valoración que se realizó en la Tabla 20. Valoración de Activos.

Tabla 27. Pauta para valoración de Importancia de activos.

Rango	Nivel de importancia	Importancia	Descripción
1 – 16	1	Poco importante	El activo tiene poca importancia para la entrega de servicios a través de la red de datos, de acuerdo a los criterios de dependencia, funcionalidad y confidencialidad, integridad y disponibilidad.

17 – 34	2	Importante	El activo es importante para la entrega de servicios a través de la red de datos, de acuerdo a los criterios de dependencia, funcionalidad y confidencialidad, integridad y disponibilidad.
35 – 64	3	Crítico	El activo es vital para la entrega de servicios a través de la red de datos, de acuerdo a los criterios de dependencia, funcionalidad y confidencialidad, integridad y disponibilidad.

Adaptado de: (Guanoluisa & Maldonado, 2015)

Aplicando la agrupación de activos señalada en la tabla anterior, a continuación se muestra la valoración de la importancia de cada uno de los activos.

Tabla 28. Clasificación de activos de acuerdo a su importancia.

Importancia	Activos	Valoración
Poco importante	Sistema de etiquetas	8
	Gateway	4
	Correo	4
Importante	Sistema optimizador de rutas	27
	Sistema de gestión de inventarios	18
	Sistema de registro de pesos	27
	Sistema de gestión de pedidos Plantas	28
Crítico	ERP	64
	Sistema de gestión de pedidos y cobros	48
	PDA	48
	Mensajería	64
	Bus de integración	64
	Integración en nube	64
	Sistema de facturación electrónica	64
	ERP Plantas	64
	Sistema de respaldos	64
	Switchs	64
	Routers	64
	Firewall	64
	Internet	64
	Impresoras	64

Una vez identificados los activos críticos, importantes y poco importantes, así como también las vulnerabilidades, el impacto que provoca una amenaza y la probabilidad de que ocurra, se procede a realizar la evaluación de riesgos.

Tabla 29. Evaluación del riesgo activos críticos.

Tipo de Amenaza	Fuente de Amenaza	Vulnerabilidad	Confidencia. Integridad Disponibili.	Impacto	Probabili.	Nivel de riesgo	Plan de Tratamiento del riesgo
Eventos naturales	Fenómenos sísmicos	Se tiene un plan de contingencia únicamente para ciertas aplicaciones y el sitio alterno soporta de la misma manera ciertas aplicaciones.	1 2 3	3	1	3	Aceptar
	Fenómenos volcánicos	Se tiene una protección a las condensadoras la cual no garantiza el 100% de protección de ceniza afectando el sistema de enfriamiento al centro de datos.	1 1 3	3	1	3	Aceptar
Pérdida de servicios esenciales	Perdida de suministro de energía.	Se cuenta con una planta generadora de energía que abastece al centro de datos, en caso de daño de la planta de energía no se cuenta con otra planta alterna.	1 2 3	3	2	6	Reducir
	Falla en el equipo de telecomunicaciones	No se tiene en sitio alta disponibilidad en los equipos de borde de los proveedores de ISP.	1 1 3	2	1	2	Aceptar
Fallas técnicas	Falla de equipos	Equipos antiguos fuera de garantía y no se encuentran bajo contrato de mantenimiento.	1 1 3	2	2	4	Reducir
	Mal funcionamient	No existe un sistema de monitoreo de *logs* de los equipos.	1 1	1	2	2	Aceptar

	o de equipos		2				
	Mal funcionamiento de software	No se cuenta con un ambiente de calidad o pre producción. No se aplica la política de control de cambios en todos los sistemas de información.	1 3 2	2	3	6	Reducir
Acciones no autorizada	Corrupción de datos	Usuarios con privilegios para modificar información en los sistemas.	3 3 2	3	3	9	Reducir
	Procesamiento ilegal de datos	No se aplica la política de resguardo de usuarios y contraseñas.	3 3 2	3	3	9	Reducir
	Hacking	Falta de actualizaciones en los servidores, redes y perímetro. Usuarios con acceso a toda la red de servidores. No se tiene activado el *firewall* a nivel de servidores y aplicaciones.	2 3 3	3	2	6	Reducir
	Sabotaje interno	Falta de cámaras de grabación en el centro de datos. *Racks* sin llave de seguridad. No se tiene definido la responsabilidad de la llave de ingreso al data center.	2 3 3	3	2	6	Reducir
	Errores humanos	Trabajo no supervisados y negligencia del personal.	1 3 3	3	3	9	Reducir

Adaptado de: (Guanoluisa & Maldonado, 2015)

Tabla 30. Evaluación del riesgo activos importantes.

Tipo de Amenaza	Fuente de Amenaza	Vulnerabilidad	Confidencia. Integridad Disponibili.	Impacto	Probabili.	Nivel de riesgo	Plan de Tratamiento del riesgo
Eventos naturales	Fenómenos sísmicos	Se tiene un plan de contingencia únicamente para ciertas aplicaciones y el sitio alterno soporta de la misma manera ciertas aplicaciones.	1 2 3	2	1	2	Aceptar
	Fenómenos volcánicos	Se tiene una protección a las condensadoras la cual no garantiza el 100% de protección de ceniza afectando el sistema de enfriamiento al centro de datos.	1 1 3	2	1	2	Aceptar
Pérdida de servicios esenciales	Perdida de suministro de energía.	Se cuenta con una planta generadora de energía que abastece al centro de datos, en caso de daño de la planta de energía no se cuenta con otra planta alterna.	1 1 3	2	2	4	Reducir
	Falla en el equipo de telecomunicaciones	No se tiene en sitio alta disponibilidad en los equipos de borde de los proveedores de ISP.	1 1 3	2	1	2	Aceptar
Fallas técnicas	Falla de equipos	Equipos antiguos fuera de garantía y no se encuentran bajo contrato de mantenimiento.	1 1 3	2	2	4	Reducir
	Mal funcionamient	No existe un sistema de monitoreo de *logs* de los equipos.	1 1	1	2	1	Aceptar

	o de equipos		2				
	Mal funcionamiento de software	No se cuenta con un ambiente de calidad o pre producción. No se aplica la política de control de cambios en todos los sistemas de información.	1 2 2	1	3	2	Aceptar
Acciones no autorizada	Corrupción de datos	Usuarios con privilegios para modificar información en los sistemas.	3 3 2	2	3	4	Reducir
	Procesamiento ilegal de datos	No se aplica la política de resguardo de usuarios y contraseñas.	2 2 2	2	3	4	Reducir
	Hacking	Falta de actualizaciones en los servidores, redes y perímetro. Usuarios con acceso a toda la red de servidores. No se tiene activado el *firewall* a nivel de servidores y aplicaciones.	2 3 3	2	2	4	Reducir
	Sabotaje interno	Falta de cámaras de grabación en el centro de datos. *Racks* sin llave de seguridad. No se tiene definido la responsabilidad de la llave de ingreso al data center.	2 3 3	2	2	4	Reducir
	Errores humanos	Trabajo no supervisados y negligencia del personal.	1 3 3	2	3	6	Reducir

Adaptado de: (Guanoluisa & Maldonado, 2015)

La evaluación de riesgos para los activos poco importantes no se realiza debido a que el nivel de riesgo sobre estos activos es mínimo y es aceptado por el negocio ya que no tiene incidencia en los procesos.

4. Capitulo IV. Diseño del DRP

El siguiente capítulo comprende la fase de estrategia de la etapa requisitos y estrategia del modelo ITSM propuesto por ITIL, donde se definirá las medidas de respuesta a riesgos y las opciones de recuperación en caso de un desastre y la etapa de implementación donde únicamente se definirán los procesos y el equipo del DRP.

4.1. Estrategia de continuidad de los servicios de TI

4.1.1. Medidas de respuesta a riesgos

Para definir la respuesta a los riesgos identificados y evaluados se continuará utilizando el modelo propuesto por la norma ISO 27005.

4.1.1.1. Tratamiento del riesgo

Las opciones escogidas para el tratamiento del riesgo son las siguientes:

- Reducción del riesgo: mediante controles se pueda reducir el riesgo.
- Retención del riesgo: aceptar los riesgos objetivamente con conocimiento. (ISO, 2011)

En la siguiente tabla se define los umbrales para el plan de tratamiento de los riesgos.

Tabla 24. Umbrales para el plan de tratamiento del riesgo.

Nivel de riesgo	Plan de tratamiento del riesgo
Menor a 4	Aceptar
Mayor o igual a 4	Reducir

4.1.1.2. Selección de controles

Una vez realizada la evaluación de riesgo de los activos, en la Tabla 29. Evaluación del riesgo activos críticos y Tabla 30. Evaluación del riesgo activos importantes se definió qué riesgos se deberían reducir mediante la selección de controles para que el riesgo sea aceptable. (ISO, 2011)

A continuación se describen los controles que permitirán reducir los riesgos identificados, de acuerdo a la prioridad de la amenaza y la importancia del activo.

Tabla 32. Controles de riesgo para activos críticos e importantes.

Tipo de Amenaza	Fuente de Amenaza	Vulnerabilidad	Nivel de riesgo	Nivel de importancia	Prioridad	Controles seleccionados
Pérdida de servicios esenciales	Perdida de suministro de energía.	Se cuenta con una planta generadora de energía que abastece al centro de datos, en caso de daño de la planta de energía no se cuenta con otra planta alterna.	6	3	18	El área de servicios generales en conjunto con TI realizarán las pruebas de funcionamiento de la planta y el control del mantenimiento periódico. Responsables: Gerente de servicios generales y DBA. Tiempo de ejecución: 3 meses
Fallas técnicas	Falla de equipos	Equipos antiguos fuera de garantía y no se encuentran bajo contrato de mantenimiento.	4	3	12	Migrar servidores antiguos a nueva plataforma de virtualización en equipos que estén en garantía o mantenimiento. Responsables: DBA Tiempo de ejecución: 6 meses
	Mal funcionamiento de software	No se cuenta con un ambiente de calidad o pre producción. No se aplica la política de control de cambios en todos los sistemas de información.	6	3	18	Rentar como servicio servidores de pre producción para las aplicaciones que lo requieran. El área de mantenimiento de software será la encargada de llevar el control de cambios de todas las aplicaciones. Responsables: Gerente de operaciones, DBA y Gerente de mantenimiento de software.

						Tiempo de ejecución: 3 meses
Acciones no autorizadas	Corrupción de datos	Usuarios con privilegios para modificar información en los sistemas.	9	3	27	El área de seguridad de la información hará la depuración de roles y privilegios de los usuarios de las aplicaciones. Responsables: Coordinador de seguridad de la información Tiempo de ejecución: 6 meses
	Procesamiento ilegal de datos	No se aplica la política de resguardo de usuarios y contraseñas.	9	3	27	El área de seguridad de la información se encargará de implementar las mejores prácticas de resguardo de contraseñas. Responsables: Coordinador de seguridad de la información Tiempo de ejecución: 3 meses
	Hacking	Falta de actualizaciones en los servidores, redes y perímetro. Usuarios con acceso a toda la red de servidores. No se tiene activado el *firewall* a nivel de servidores y aplicaciones.	6	3	18	El área de seguridad de la información hará las pruebas de *hacking* ético para evaluar las vulnerabilidades y aplicar las mejoras con el apoyo del área de operaciones. Responsables: Gerente de seguridad de la información, Gerente de operaciones, DBA. Tiempo de ejecución: 6 meses.
	Sabotaje interno	Falta de cámaras de grabación en el centro de datos. *Racks* sin llave de seguridad. No se tiene	6	3	18	El área de centro de monitoreo en conjunto con TI implementara las cámaras de vigilancia en el centro de datos. Se pondrán llaves en cada uno de los *rack* y se

		definido la responsabilidad de la llave de ingreso al data center.				definirán responsables de los mismos. Responsables: Gerente de seguridad física, Gerente de operaciones, DBA. Tiempo de ejecución: 6 meses.
	Errores humanos	Trabajo no supervisados y negligencia del personal.	9	3	27	Establecer procedimientos para la gestión y operación de los sistemas de información y segregar tareas para reducir el riesgo de un mal uso deliberado o por negligencia. Responsables: Gerente de operaciones, DBA, Gerente de Mantenimiento de software y Analistas de sistemas. Tiempo de ejecución: 6 meses.

Adaptado de: (Guanoluisa & Maldonado, 2015)

El valor de la prioridad es igual al nivel de riesgo tomado de la Tabla 29. Evaluación del riesgo activos críticos, multiplicado por el nivel de importancia que es tomado de la Tabla 27. Pauta para valoración de Importancia de activos de acuerdo a la Tabla 20. Valoración de activos.

Los controles de riesgos a los activos aplican tanto para los activos críticos e importantes y estos fueron evaluados entre el área de operaciones de TI y el área de seguridad de la información.

4.1.2. Opciones de recuperación

Con los resultados del análisis de impacto y el análisis de riesgos se plantea la estrategia de tener un sitio alterno arrendado a un tercero en la ciudad de Guayaquil que sea activo – pasivo, es decir toda la información del sitio primario debe ser replicada a un centro de datos alterno, el cual entraría en funcionamiento en caso de que el sitio primario deje de operar por un largo periodo de tiempo.

El sitio alterno debe cumplir con los siguientes servicios:

- Centro de datos.- Permita instalar varios servidores y que cumpla con las condiciones necesarias para garantizar la disponibilidad y continuidad de la operación de los servicios de TI.
    - Sistemas de seguridad física con vigilancia 7x24x365.
    - Sistemas de detección y extinción de incendios.
    - Plantas eléctricas redundantes.
    - Sistemas de energía con UPS y en redundancia.
    - Climatización óptima con aires acondicionados redundantes.
- *Hosting* Virtual.- Permita aprovisionar servidores bajo demanda y estos deben ser gestionados por el proveedor de servicios.
- Monitoreo.- Garantizar un correcto monitoreo 7x24x365 de los servidores, *routers*, *switches*, sistemas operativos, bases de datos.

Adicionalmente se deben emitir reportes mensuales del estado y de los niveles de servicio así como incidentes ocurridos, soluciones y planes de prevención.

- Respaldos.- El proveedor de servicios es el encargado de ejecutar el proceso de respaldos y de las pruebas o peticiones bajo demanda de restauración, también debe resguardar y proteger la información mediante el almacenamiento en dispositivos alternativos sean cintas o discos.
- Almacenamiento.- Garantizar la velocidad de acceso y transferencia, disponibilidad y redundancia de la información y crecimiento bajo demanda.
- Administración de sistema operativo.- Asegurar condiciones óptimas del funcionamiento de los sistemas operativos AIX, Linux y Windows, esto comprende desde la instalación del sistema, configuración y administración.
- Administración de base de datos.- Asegurar el manejo eficiente de las bases de datos Oracle y SQL Server, esto incluye desde la instalación, configuración y administración.
- Seguridad.- Los servicios de seguridad deben ser administrados por el proveedor y debe estar compuesto por un *firewall* principal y componentes adicionales como:
    - Dispositivos perimetrales
    - Monitoreo de la funcionalidad del *firewall*.
    - Soporte técnico 24x7x365 cubriendo aspectos de conectividad a internet por medio de la red privada virtual (VPN).
    - Respaldo de la configuración del *firewall*.
    - Actualización del *firewall*.
    - Servicios adicionales de ISP, VPN, Antivirus.

4.1.2.1. Arquitectura de la solución

La siguiente figura muestra el esquema deseado del sitio principal en Quito y del sitio alterno en Guayaquil conforme al relevamiento de la infraestructura requerida que se encuentra en la Tabla 15. Servidores y aplicaciones.

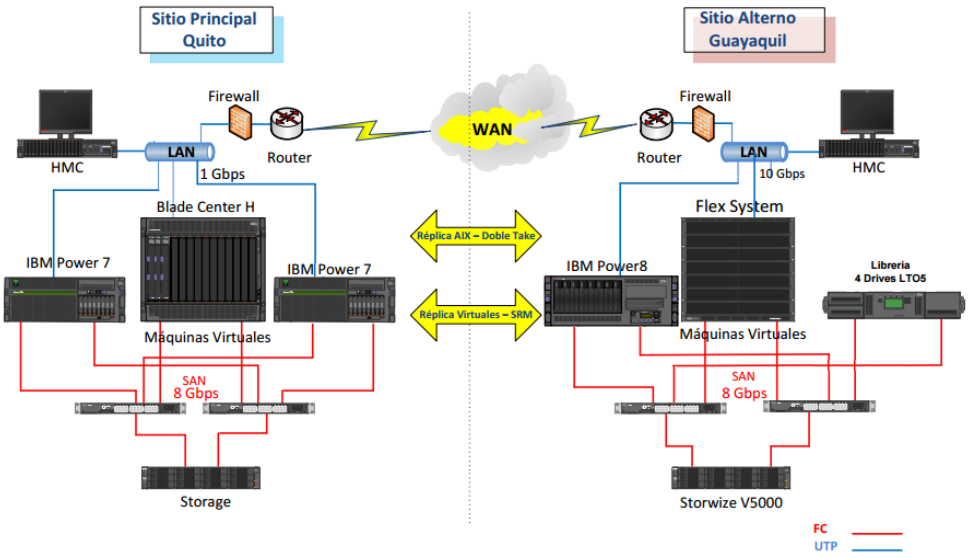


Figura 14. Esquema de replicación deseado.

Para el esquema de replicación deseado se requiere la siguiente lista de equipos y que cumplan con las características mencionadas, estos equipos van a soportar la replicación de todas las aplicaciones al sitio alterno. Es importante mencionar que la propuesta está diseñada para tener una holgura de hardware aproximada de dos años para el crecimiento de las aplicaciones y escalabilidad para nuevas aplicaciones.

Tabla 33. Equipos requeridos para sitio alterno.

Cantidad	Descripción	Características
1	Servidor IBM *Power* 8 (S824)	
4		HBA 8 Gigabit PCI Express Dual Port
5		4-port 1Gb Adapter
4		64 GB RAM
2		Procesadores *Power* 8 12 Cores 3.52 GHz
3		HDD 300 GB a 15k RPM SAS
1	*Chassis Flex System*	
2		LAN *Switch* 10 Gbps
2		SAN *Switch* 8 Gbps
2	Nodos X240 M5	
2		64 GB de memoria RAM
2		discos de 300 GB
2		procesadores Xeon E5-2640 V3 8 Cores
1		NIC 10 Gbps
1		HBA 8 Gbps
1	HMC 7042-CR8	
1		8 GB Pluggable USB Memory
1		IBM 500 GB SATA HDD
1	*Enclosure* V5000	
15		600 GB SAS 15K RPM
9		400 GB SSD
2	Expansión V5000	
24		600 GB SAS
1	Librería de cintas TS 3200	
4		Drives F/C LTO5
2	*Switch* de SAN	24p 8Gbps (16 Activated)
2	*Switch* de comunicaciones Cisco Catalyst 3850	24 Port Data IP Services
1	*Standard Rack*	IBM

La siguiente figura muestra el esquema de distribución de los equipos diseñado para tener un crecimiento en el tiempo.

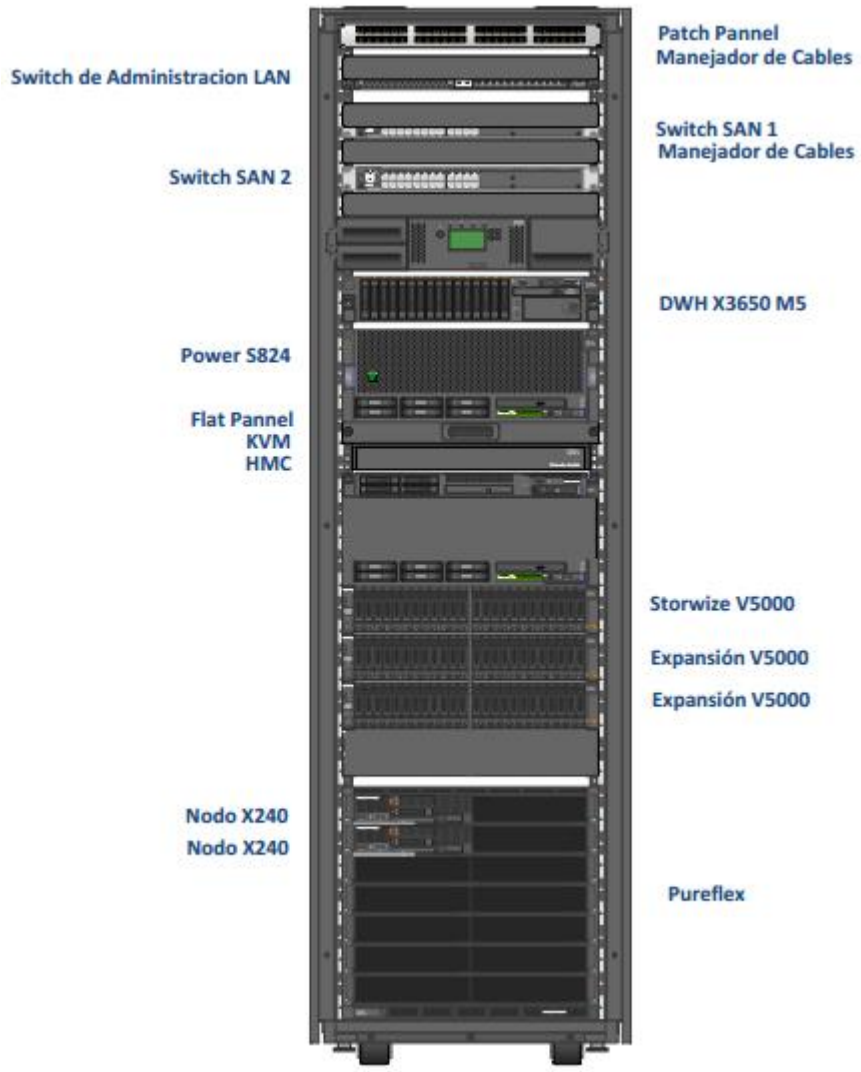


Figura 15. Esquema de distribución de equipos.

Para optimizar la arquitectura de replicación al sitio alterno propuesta se debe realizar la centralización y virtualización de los servidores físicos que se encuentran en las plantas, para esto se evaluó con los responsables de los aplicativos quienes a su vez validaron con los proveedores la factibilidad de realizar el cambio. Los servidores que se van a centralizar y virtualizar mantendrán sus características de sistema operativo, base de datos, memoria, procesador y disco.

Tabla 34. Servidores por virtualizar.

Aplicación	Ubicación Actual	Nueva Ubicación	Tiempo de implementación
Sistema de gestión de pedidos y cobros	Guayaquil Metro Park Regional Santo Domingo CD Montecristi	DC Inverna Quito DC Inverna Quito DC Inverna Quito	3 meses
Sistema optimizador de rutas	CD Quito CD Quito CD Guayaquil CD Guayaquil	DC Inverna Quito DC Inverna Quito DC Inverna Quito DC Inverna Quito	2 meses
Sistema de gestión de inventarios	CD Quito CD Guayaquil	DC Inverna Quito DC Inverna Quito	2 meses
Sistema de registro de pesos	CD Quito CD Guayaquil CD Cuenca CD Montecristi Valle Hermoso	DC Inverna Quito DC Inverna Quito DC Inverna Quito DC Inverna Quito DC Inverna Quito	3 meses
ERP Plantas	Planta Puembo	DC Inverna Quito	1 mes

La virtualización de los servidores es un requisito previo para la implementación del DRP y es parte del proyecto de centralización y migración de servidores a nueva infraestructura. El costo de migración de los servidores es de $84,000, este valor no es parte del presupuesto del DRP.

Las herramientas para replicación al sitio alterno que se van a utilizar son *Double-Take Availability* para los servidores AIX y para los servidores Linux y Windows VMWare *Site Recovery Manager*.

Double-Take Availability protege los datos y aplicaciones críticas de negocio que se encuentren bajo sistemas operativos AIX virtuales o físicos, esta herramienta realiza replicación en tiempo real y protección continua de los datos en un servidor local o remoto, su recuperación instantánea y su gestión simplificada permite cumplir con los RTO y RPO más rigurosos.

Dentro de las características más importantes destacan:

- Minimiza el tiempo de inactividad.
- Protege la pérdida de datos.
- Permite combinar diferentes marcas de hardware para sistemas operativos y almacenamiento.
- Reduce carga de trabajo con procedimientos automatizados y la posibilidad de que se produzcan errores humanos.
- Simplifica la gestión de la disponibilidad de servicios y de la recuperación de desastres.
- Protege los entornos de AIX.
- Protege la disponibilidad de los datos y aplicaciones. (VisionSolutions, 2014)

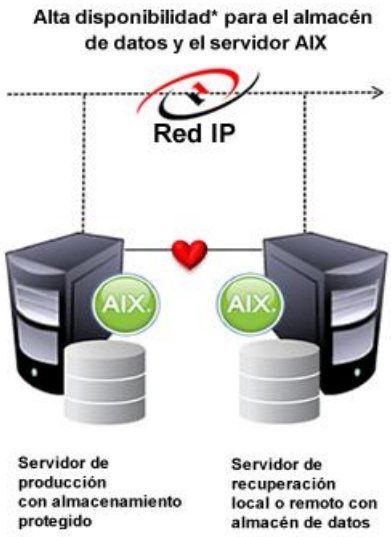


Figura 16. *Double-Take Availability*.
Tomado de: (VisionSolutions, 2014)

VMWare *Site Recovery Manage*r es una solución diseñada para habilitar movilidad y disponibilidad de las aplicaciones virtualizadas en sitios locales o remotos. Es un software que permite la automatización de la recuperación ante

desastres acelerando el proceso de restauración de las aplicaciones y elimina los riesgos de ejecución manuales.

Sus características son:

- Recuperación ante desastres de manera rápida y confiable.
- Administración simple basada en políticas.
- Movilidad de aplicaciones con mínimo o sin tiempo fuera de servicio.
- Reducción del costo total de propiedad. (VMWARE, 2015)

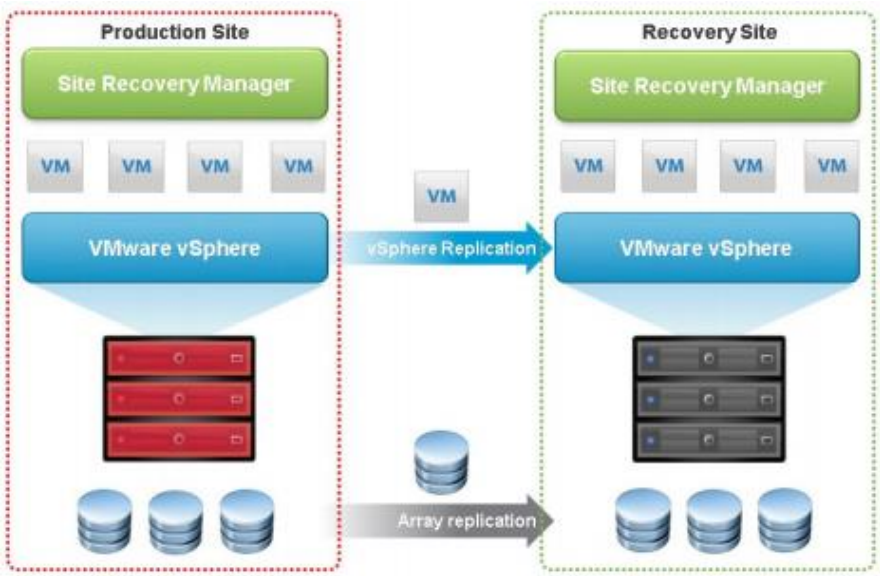


Figura 17. *Site Recovery Manager*.
Tomado de: (VMWARE, 2015)

Adicionalmente se continuará con el proceso de respaldos a cinta que se encuentra definido e implementado en la organización. La información del proceso de almacenamiento y custodia de respaldos se encuentra en al anexo D.

4.1.2.2. Consideraciones para la estrategia de recuperación

Para tener una óptima estrategia de recuperación se deben tomar en cuenta las siguientes consideraciones:

- Dado el volumen de datos que se van a replicar y para dar soporte al RPO ya definido es necesario tener un enlace entre el sitio principal de Quito y el sitio alterno en Guayaquil de 100 Mbps de ancho de banda y este debe ser redundante.
- Los servidores a replicar deben cumplir requerimiento mínimo de sistema operativo los cuales deben ser actualizados para los nuevos equipos propuestos.
- Se debe definir un centro de control donde se realicen las actividades de valoración inicial, coordinación y toma de decisiones ante un desastre, este lugar de preferencia debe ser en un lugar donde no se vea afectado por el mismo desastre.
- Se deben evaluar las facilidades para que las personas claves del equipo de recuperación de servicios puedan llegar al centro de control, esto incluye a los proveedores de las aplicaciones.

4.1.3. Análisis económico de sitios alternos

El siguiente análisis presenta dos propuestas que consiste tener un sitio alterno propio de la empresa o arrendar un sitio alterno como servicio.

4.1.3.1. Sitio alterno propio

Los valores presentados en la propuesta de sitio alterno propio son referenciales y a precio de lista proporcionados por el proveedor de infraestructura de equipos tecnológicos de la empresa.

Tabla 35. Inversión sitio alterno propio.

Equipos	Cantidad	Valor
Servidor IBM *Power* 8	1	$182,525
Chassis Flex System	1	$48,734
Nodos X240 M5	2	$132,722
HMC 7042-CR8	1	$10,184
Enclosure V5000	1	$151,933
Expansión V5000	2	$203,770
Librería de cintas TS 3200	1	$40,195
Cintas para respaldos	100	$4,000
SAN *Switch*	2	$42,586
Switch de comunicaciones Cisco Catalyst 3850	2	$29,379
Centro de Datos Compacto	1	$38,000
Licenciamiento y Mantenimiento vmware 3 años	1	$34,484
Licenciamiento y Mantenimiento *double-take availability* 3 años	1	$185,063
Servicios de instalación	1	$183,233
	Total	**$1,286,808**

Tabla 36. Costos operativos sitio alterno propio.

Costos Operativos	Cantidad	Valores Mensuales
Sueldo DBA incluido beneficios	1	$2,948
Enlaces	3	$20,000
Mantenimiento Centro de Datos	3	$200
Electricidad	3	$200
	Total	**$23,348**

Para conocer el valor total del proyecto a 3 años se va aplicar el concepto de valor presente neto que es “uno de los criterios económicos más ampliamente utilizados en la evaluación de proyectos”. (Coss Bu, 2005)

A continuación se muestra la (Ecuación 1) que se va a utilizar para evaluar el valor presente neto de los flujos generados del proyecto.

$$VPN = S_o + \sum_{t=1}^{n} \frac{S_t}{(1+i)^t}$$ (Ecuación 1)

Donde:

- VPN = Valor presente neto.
- S_o = Inversión inicial
- S_t = Flujo de efectivo neto del periodo t.
- n = Número de períodos de vida del proyecto.
- i = Tasa de recuperación mínima atractiva. (Coss Bu, 2005)

El valor de la tasa de recuperación mínima para el cálculo del valor presente neto es del 8%, este valor se tomó como referencia las tasas de interés pasivas efectivas de depósitos a plazo del sector financiero que en promedio es del 7,85% (BCE, 2016); este dato se encuentra disponible en la página web del Banco Central del Ecuador.

Tabla 37. Valor presente neto sitio alterno propio.

Primer Año												
Mes	1	2	3	4	5	6	7	8	9	10	11	12
Costos Operativos												
Sueldo DBA incluido beneficios	$2,948	$2,948	$2,948	$2,948	$2,948	$2,948	$2,948	$2,948	$2,948	$2,948	$2,948	$2,948
Enlaces	$20,000	$20,000	$20,000	$20,000	$20,000	$20,000	$20,000	$20,000	$20,000	$20,000	$20,000	$20,000
Mantenimiento Centro de Datos	$200	$200	$200	$200	$200	$200	$200	$200	$200	$200	$200	$200
Electricidad	$200	$200	$200	$200	$200	$200	$200	$200	$200	$200	$200	$200
Total	$23,348	$23,348	$23,348	$23,348	$23,348	$23,348	$23,348	$23,348	$23,348	$23,348	$23,348	$23,348
Valor Presente Neto	**$23,193**	**$23,040**	**$22,887**	**$22,736**	**$22,585**	**$22,436**	**$22,287**	**$22,139**	**$21,993**	**$21,847**	**$21,702**	**$21,559**
Segundo Año												
Mes	13	14	15	16	17	18	19	20	21	22	23	24
Costos Operativos												
Sueldo DBA incluido beneficios	$2,948	$2,948	$2,948	$2,948	$2,948	$2,948	$2,948	$2,948	$2,948	$2,948	$2,948	$2,948
Enlaces	$20,000	$20,000	$20,000	$20,000	$20,000	$20,000	$20,000	$20,000	$20,000	$20,000	$20,000	$20,000
Mantenimiento Centro de Datos	$200	$200	$200	$200	$200	$200	$200	$200	$200	$200	$200	$200
Electricidad	$200	$200	$200	$200	$200	$200	$200	$200	$200	$200	$200	$200
Total	$23,348	$23,348	$23,348	$23,348	$23,348	$23,348	$23,348	$23,348	$23,348	$23,348	$23,348	$23,348
Valor Presente Neto	**$21,416**	**$21,274**	**$21,133**	**$20,993**	**$20,854**	**$20,716**	**$20,579**	**$20,443**	**$20,307**	**$20,173**	**$20,039**	**$19,907**
Tercer Año												
Mes	25	26	27	28	29	30	31	32	33	34	35	36
Costos Operativos												
Sueldo DBA incluido beneficios	$2,948	$2,948	$2,948	$2,948	$2,948	$2,948	$2,948	$2,948	$2,948	$2,948	$2,948	$2,948
Enlaces	$20,000	$20,000	$20,000	$20,000	$20,000	$20,000	$20,000	$20,000	$20,000	$20,000	$20,000	$20,000
Mantenimiento Centro de Datos	$200	$200	$200	$200	$200	$200	$200	$200	$200	$200	$200	$200
Electricidad	$200	$200	$200	$200	$200	$200	$200	$200	$200	$200	$200	$200
Total	$23,348	$23,348	$23,348	$23,348	$23,348	$23,348	$23,348	$23,348	$23,348	$23,348	$23,348	$23,348
Valor Presente Neto	**$19,775**	**$19,644**	**$19,514**	**$19,384**	**$19,256**	**$19,128**	**$19,002**	**$18,876**	**$18,751**	**$18,627**	**$18,503**	**$18,381**

Tabla 38. Costo total de sitio alterno propio.

Concepto	Valores Totales
Inversión	$1,286,808
Costos operativos (3 años)	$745,080
Total Proyecto	**$2,031,888**

4.1.3.2. Sitio alterno arrendado

Tabla 39. Inversión sitio alterno arrendado.

Equipos	Cantidad	Valor
Cargo inicial por servicio	1	$65,000
	Total	**$65,000**

Tabla 40. Costos operativos sitio alterno arrendado.

Costos Operativos	Cantidad	Valores Mensuales
Cargo mensual por servicio	1	$21,000
Enlaces	2	$20,000
	Total	**$41,000**

El cargo mensual por servicio del sitio alterno fue escogido de la mejor oferta de dos propuestas de diferentes proveedores la cual incluye:

- Capacidades
  - Capacidades de tecnología Unix (IBM *Power*).
  - Capacidades de tecnología Intel.
  - Capacidades de almacenamiento.
  - Capacidades de seguridad perimetral.

- Provisión en uso de licencias de software
  - Licencias de sistema operativo AIX.
  - Licencias de respaldos para capacidades *Power* e Intel.
  - Licencias de VMWare y *Site Recovery Manage*r para replicación de Windows y Linux.
  - Licencias de software de monitoreo.

    - Licencias de *Double-Take Availability* para replicación de AIX.
- Servicios de Mantenimiento
    - Mantenimiento de hardware 7x24 por los 3 años de servicio.
    - Un mantenimiento preventivo de hardware anual por los 3 años de servicio.
    - Actualización de firmware una vez al año.
- Servicios de soporte para contingencia horario 7x24
    - Soporte de especialistas para realizar pruebas de contingencia, una vez al año.
    - Soporte para actualización de parches en sistema operativo.
- Servicios de monitoreo en horario 7x24
    - Hardware: Procesador, memoria RAM, paginación, espacio en disco, alertas de hardware.
    - Enlaces de comunicación entre sitio alterno y PRONACA.
    - Logs de eventos de sistema operativo y base de datos.
    - Monitoreo de almacenamiento y de réplica
- Servicio de respaldos
    - Respaldos de las máquinas ofertadas en base a las políticas de respaldo de PRONACA.

Tabla 41. Valor presente neto sitio alterno arrendado.

Primer Año												
Mes	1	2	3	4	5	6	7	8	9	10	11	12
Costos Operativos												
Cargo mensual por servicio	$21,000	$21,000	$21,000	$21,000	$21,000	$21,000	$21,000	$21,000	$21,000	$21,000	$21,000	$21,000
Enlaces	$20,000	$20,000	$20,000	$20,000	$20,000	$20,000	$20,000	$20,000	$20,000	$20,000	$20,000	$20,000
Total	$41,000	$41,000	$41,000	$41,000	$41,000	$41,000	$41,000	$41,000	$41,000	$41,000	$41,000	$41,000
Valor Presente Neto	**$40,728**	**$40,459**	**$40,191**	**$39,925**	**$39,660**	**$39,398**	**$39,137**	**$38,878**	**$38,620**	**$38,364**	**$38,110**	**$37,858**
Segundo Año												
Mes	13	14	15	16	17	18	19	20	21	22	23	24
Costos Operativos												
Sueldo DBA incluido beneficios	$21,000	$21,000	$21,000	$21,000	$21,000	$21,000	$21,000	$21,000	$21,000	$21,000	$21,000	$21,000
Comunicaciones	$20,000	$20,000	$20,000	$20,000	$20,000	$20,000	$20,000	$20,000	$20,000	$20,000	$20,000	$20,000
Total	$41,000	$41,000	$41,000	$41,000	$41,000	$41,000	$41,000	$41,000	$41,000	$41,000	$41,000	$41,000
Valor Presente Neto	**$37,607**	**$37,358**	**$37,111**	**$36,865**	**$36,621**	**$36,378**	**$36,137**	**$35,898**	**$35,660**	**$35,424**	**$35,189**	**$34,956**
Tercer Año												
Mes	25	26	27	28	29	30	31	32	33	34	35	36
Costos Operativos												
Sueldo DBA incluido beneficios	$21,000	$21,000	$21,000	$21,000	$21,000	$21,000	$21,000	$21,000	$21,000	$21,000	$21,000	$21,000
Comunicaciones	$20,000	$20,000	$20,000	$20,000	$20,000	$20,000	$20,000	$20,000	$20,000	$20,000	$20,000	$20,000
Total	$41,000	$41,000	$41,000	$41,000	$41,000	$41,000	$41,000	$41,000	$41,000	$41,000	$41,000	$41,000
Valor Presente Neto	**$34,725**	**$34,495**	**$34,267**	**$34,040**	**$33,814**	**$33,590**	**$33,368**	**$33,147**	**$32,927**	**$32,709**	**$32,493**	**$32,277**

Tabla 42. Costo total de sitio alterno arrendado.

Concepto	Valores Totales
Inversión	$65,000
Costos operativos (3 años)	$1,308,384
Total Proyecto	**$1,373,384**

Una vez obtenidos los costos de un sitio alterno propio y un sitio alterno arrendado, se concluye que económicamente es más factible tener un sitio alterno arrendado ya que existe un ahorro para la empresa de $658,504 en 3 años.

4.1.4. Análisis de costo-beneficio del proyecto

Realizar un análisis costo-beneficio es importante ya que “permite fundamentar la decisión del desarrollo del proyecto”. (Rodríguez & William, 2006)

El costo total del proyecto con el sitio alterno arrendado para 3 años es de $1,373,384.

Los beneficios del proyecto se detallan a continuación.

- Beneficio económicos.
    - Evitar una pérdida económica de más de 2 millones de dólares por indisponibilidad de los servicios de TI.
    - Economía de escala.
    - Control de gastos dentro del presupuesto.
    - Disminuir el costo de inversión.
- Beneficios cualitativos
    - Sistema de monitoreo 24x7x365.
    - Mejor gestión de eventos.
    - Acuerdos de niveles de servicio.
    - Profesionales expertos y capacitados.

    - Tecnología de punta.
- Beneficios estratégicos
    - Flexibilidad en la disponibilidad de recursos.
    - Enfoque al negocio.
    - Dedicación del personal a tareas que generen valor a la empresa.

4.2. Etapa de implementación

Para esta etapa únicamente se van a definir los procedimientos que se deben implementar y los equipos de trabajo para el DRP; se va a excluir la fase de pruebas la cual se haría una vez implementado el presente proyecto.

4.2.1. Definición de procedimientos para el DRP

Los procedimientos requeridos para el DRP son los siguientes:

- Recuperación de los enlaces de comunicación.
- Recuperación de los sistemas operativos.
- Recuperación de aplicaciones.
- Recuperación de bases de datos.

Los procedimientos deben estar muy bien definidos, cuidadosamente elaborados y ensayados por el equipo de recuperación para que la restauración de los servicios de TI en el sitio alterno sea acorde al MTD, RTO y RPO establecidos.

4.2.2. Definición de los equipos para el DRP

La empresa cuenta con un comité de riesgos que tiene como objetivo asegurar una respuesta rápida, sistemática, organizada y efectiva frente a eventos de crisis que puedan afectar los intereses de la compañía, su personal,

imagen y/o inversión, con el propósito de proteger a la organización, minimizar los efectos negativos y permitir la continuidad del negocio.

Las responsabilidades del comité de riesgos son:

- Proteger y precautelar la vida e integridad de las personas.
- Asegurar que las actividades realizadas durante la respuesta a la crisis sean consistentes con las políticas corporativas.
- Minimizar posibles daños sobre bienes de la empresa.
- Establecer una línea de comunicación clara que permita la transmisión oportuna de la información.
- Emplear con efectividad los recursos de la compañía, de organismos estatales y de convenios de ayuda mutua.
- Considerar los aspectos legales relevantes para evitar demandas.
- Proveer información precisa a los medios de comunicación y/o terceras partes involucradas.
- Iniciar las actividades para la recuperación del negocio.

La estructura del comité de riesgos es la siguiente:

Figura 18. Estructura estratégica.

El Presidente del Comité de Crisis será reemplazado en caso de ausencia en el orden que se presenta la Figura 18. Estructura Estratégica.

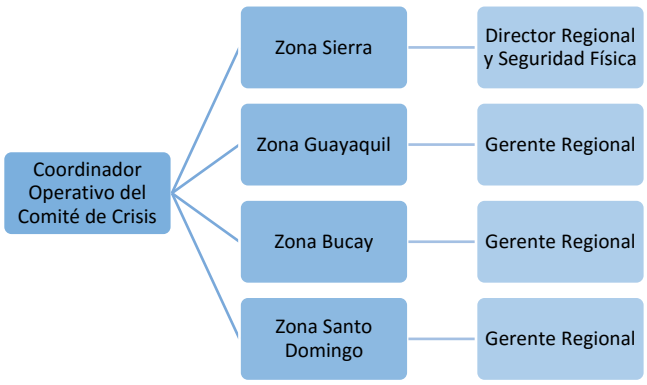


Figura 19. Estructura Operativa.

El Coordinador Operativo del Comité de Crisis, es el responsable de:

- Facilitar la ejecución de las acciones internas y externas
- Mantener contacto directo con el Comité Ejecutivo para informar y recibir direccionamientos

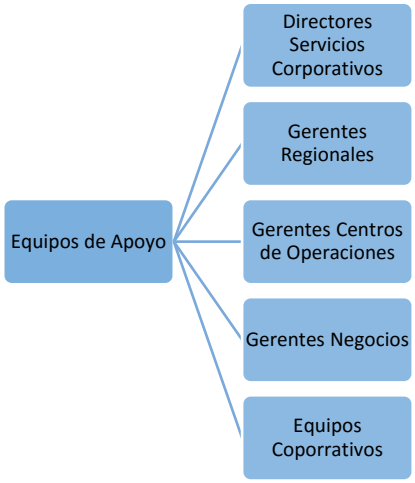


Figura 20. Equipos de apoyo interno.

Dependiendo del tipo de crisis y su magnitud, se incorporarán los integrantes de los equipos corporativos que son de servicios.

Tabla 43. Equipo de comité de riesgos.

Miembros del equipo de comité de riesgos					
Nombre	**Apellido**	**Cargo**	**Teléfono Oficina**	**Teléfono Celular**	**Ubicación**
LuiXXX	BakXXX	Presidente Ejecutivo	023976XXX ext XXXX	XXXXXXXXXX	Quito
JohXXX	BakXXX	Vicepresidente Ejecutivo	023976XXX ext XXXX	XXXXXXXXXX	Quito
JulXXX	AguXXX	Vicepresidente Operaciones	023976XXX ext XXXX	XXXXXXXXXX	Quito
MauXXX	PadXXX	Vicepresidente Desarrollo Organizacional	023976XXX ext XXXX	XXXXXXXXXX	Quito
JuaXXX	PitXXX	Vicepresidente de Finanzas y Planeación	023976XXX ext XXXX	XXXXXXXXXX	Quito
ChrXXX	BakXXX	Vicepresidente de Sostenibilidad	023976XXX ext XXXX	XXXXXXXXXX	Guayaquil
FraXXX	ValXXX	Director Regionales y Seguridad Física	023976XXX ext XXXX	XXXXXXXXXX	Quito

Adaptado de: (Gaspar, 2010)

Las responsabilidades del equipo de recuperación de los servicios de TI se encuentran ya definidas en la política del plan de recuperación de desastres. El equipo de recuperación de servicios se encuentra conformado por las siguientes personas:

Tabla 44. Equipo de recuperación de servicios PRONACA.

Miembros del equipo de recuperación de servicios PRONACA					
Nombre	**Apellido**	**Cargo**	**Teléfono Oficina**	**Teléfono Celular**	**Ubicación**
RubXXX	RecXXX	Director Tecnología e Información	023976XXX ext XXXX	099901XXXX	Quito
HugXXX	SegXXX	Gerente de Operaciones	023976XXX ext XXXX	099427XXXX	Quito
FabXXX	GalXXX	Gerente de Mantenimiento	023976XXX ext XXXX	099973XXXX	Quito
OlgXXX	SilXXX	Gerente de Seguridad de la información	023976XXX ext XXXX	099927XXXX	Quito Bogotá
OmaXXX	GonXXX	Administrador de Base de Datos	023976XXX ext XXXX	099427XXXX	Quito
DavXXX	VinXXX	Administrador de Base de Datos	023976XXX ext XXXX	099398XXXX	Quito
PamXXX	MolXXX	Administrador de Base de Datos	023976XXX ext XXXX	098484XXXX	Quito
OscXXX	VitXXX	Administrador de Base de Datos	023976XXX ext XXXX	099471XXXX	Guayaquil
FabXXX	MorXXX	Analista de sistemas	023976XXX ext XXXX	098708XXXX	Quito
AndXXX	DelXXX	Coordinador de negocio	023976XXX ext XXXX	099261XXXX	Quito
EdwXXX	ValXXX	Analista de sistemas	023976XXX ext XXXX	099994XXXX	Quito
AlfXXX	CheXXX	Analista de sistemas	023976XXX ext XXXX	099434XXXX	Quito
WilXXX	CifXXX	Soporte usuarios	023976XXX ext XXXX	099804XXXX	Quito
ChrXXX	MorXXX	Arquitecto de aplicaciones	023976XXX ext XXXX	099427XXXX	Quito
RemXXX	CorXXX	Coordinador de proyectos	023976XXX ext XXXX	099581XXXX	Quito
OswXXX	AlvXXX	Coordinador de proyectos	023976XXX ext XXXX	098408XXXX	Quito

Adaptado de: (Gaspar, 2010)

Tabla 45. Equipo de recuperación de servicios Proveedores.

Miembros del equipo de recuperación de servicios Proveedores					
Nombre	**Apellido**	**Cargo**	**Teléfono Oficina**	**Teléfono Celular**	**Ubicación**
XimXXX	UtrXXX	Proveedor ERP	022447XXX ext XXXX	099774XXXX	Quito
EdgXXX	PirXXX	Proveedor Sistema de gestión de pedidos y cobros – PDA	571485XXXX	57320454XXXX	Bogotá
PatXXX	CasXXX	Proveedor Mensajería – Bus de integración	023976XXX ext XXXX	099565XXXX	Quito
FelXXX	PueXXX	Proveedor Sistema optimizador de rutas		5698378XXXX	Santiago
JosXXX	DelXXX	Proveedor Sistema de gestión de inventarios	900920XXX ext XXXX	94442XXXX	Bilbao
AleXXX	CarXXX	Proveedor Sistema de registro de pesos	023826XXX ext XXXX	096982XXXX	Quito
FauXXX	CanXXX	Proveedor Integración en nube	023976XXX ext XXXX	099345XXXX	Quito
AleXXX	AlmXXX	Proveedor Sistema de gestión de pedidos Plantas	023962XXX ext XXXX	098932XXXX	Quito
DanXXX	ChaXXX	Proveedor Sistema de impresión	023976XXX ext XXXX	099795XXXX	Quito
AndXXX	RodXXX	Proveedor Sistema de respaldos	023825XXX	099895XXXX	Quito
JosXXX MarXXX	ConXXX JarXXX	Proveedor Enlace de red externo	023963XXX 024005XXX	099909XXXX 099730XXXX	Quito Quito
CamXXX	PeñXXX	Proveedor *Firewall*	022440XXX	099581XXXX	Quito

Adaptado de: (Gaspar, 2010)

5. Capitulo V. Conclusiones y Recomendaciones

5.1. Conclusiones

Una vez finalizado el presente proyecto del Diseño de un Plan de Recuperación de Desastres para el departamento de Tecnología de Información se concluye lo siguiente:

El análisis de impacto en el negocio, permitió conocer de manera formal la afectación que tendría la organización en la parte económica, comercial, operacional, imagen y legal si se interrumpen los procesos de gestión de ventas o recaudaciones.

Mediante el análisis de impacto se logró determinar el tiempo máximo de inactividad tolerable que puede soportar los procesos críticos sin los servicios tecnológicos y establecer los RTO y RPO requeridos por el negocio.

Con el análisis de riegos se identificaron los activos más importantes para la empresa, las vulnerabilidades y amenazas que pueden causar incidentes o daños en la infraestructura.

La estrategia de continuidad de los servicios de TI permitió definir el tratamiento y los controles para mitigar los riesgos y la arquitectura de solución para garantizar la continuidad de los procesos de negocio ante un desastre.

Por medio del análisis costo-beneficio se determinó que el valor de la estrategia de continuidad de un sitio alterno en 3 años es menor que la pérdida de las ventas que genera la empresa en un día.

5.2. Recomendaciones

Como resultado del proyecto se realizan las siguientes recomendaciones:

Implementar el Diseño del Plan de Recuperación de Desastres propuesto en el presente proyecto el cual se encuentra elaborado a las necesidades de la empresa, aplicando como mejores prácticas los estándares de ITIL y la norma ISO 27005.

La empresa debe contar con un sitio alterno en una ciudad lejana a Quito, que no se vea afectada por un mismo desastre y que cuente con proveedores de servicios de centro de datos; el proyecto sugiere la ciudad de Guayaquil la cual cumple con lo antes mencionado.

Replicar los activos identificados como críticos e importantes para la empresa mediante soluciones especializadas para garantizar una pronta recuperación de los servicios tecnológicos ante un desastre.

Aplicar los controles de riesgos propuestos para los activos de acuerdo a la prioridad para reducir la probabilidad de que una amenaza pueda causar daños a los recursos tecnológicos de la organización.

Arrendar el sitio alterno a una empresa experta y con experiencia en brindar servicios de alojamiento y administración de centro de datos con altos estándares de calidad que avalen la disponibilidad de los servicios.

REFERENCIAS

Axelos. (2011). *Glosario y abreviaturas de ITIL.* TSO.

Axelos. (2011). *ITIL - Diseño del Servicio.* TSO.

BCE. (2016). *Banco Central del Ecuador.* Recuperado el 15 de Febrero de 2016, de Nuevas Publicaciones: http://www.bce.fin.ec/index.php/component/k2/item/755

Coss Bu, R. (2005). *Análisis y evaluación de proyectos de inversión.* Ciudad de México: Limusa.

Gaspar, J. (2010). *El plan de continuidad de negocio.* Madrid: Ediciones Díaz de Santos, S.A.

Guanoluisa, J., & Maldonado, I. (2015). *Análisis de riesgos y diseño de una plan de seguridad de la información para el consejo nacional de discapacidades "CONADIS".* Quito: Universidad Politecnica Nacional.

Hoffer, Jim. (2001). *Life & Health Library.* Recuperado el 27 de Noviembre de 2015, de CBS INTERACTIVE BUSINESS NETWORK RESOURCE LIBRARY: http://archive.is/20120629133345/findarticles.com/p/articles/mi_m0DUD/is_1_22/ai_68864006#selection-21.1-21.46

ISO. (2011). *ISO/IEC 27005:2011 Tecnología de la Información - Técnicas de seguridad - Gestión de riesgos de seguridad de la información.* ISO.

ISO. (2012). *ISO 22300:2012 Seguridad social - Terminología.* ISO.

ISO. (2013). *ISO/IEC 27002:2013 Tecnología de la Información - Técnicas de seguridad - Código de prácticas para los controles de seguridad de la información.* ISO.

Matos, M., Beriguete, M., & Reidy, P. (2015). *Diseño de un plan de recuperación ante desastre (DRP).* Editorial Académica Española.

Morales, R. (2015). *Diseño para la implementación de tres dominios de un sistema de gestión en la seguridad de la información basada en la norma ISO27001 e ISO27002, para el área de software de la procesadora nacional de alimentos PRONACA.* Quito: Universidad de las Fuerzas Armadas.

NIST. Contingency Planning Guide for Federal Information Systems. *NIST Special Publication 800-34 Rev. 1.* National Institute of Standards and Technology, Gaithersburg.

PRONACA. (2013). *Memoria 2013.* Recuperado el 08 de Diciembre de 2015, de Capítulo 1 Nuestra Compañía: https://view.ceros.com/pronaca/memoria-2013/p/2

Rodríguez, N., & William, M. (2006). *Planificación y evaluación de proyectos informáticos.* San José: EUNED.

Snedaker, S. (2007). *Business Continuity & Disaster Recovery.* Burlington: Syngress Publishing, Inc.

VisionSolutions. (2014). *Migrate, Portect & Recover Anywhere*. Recuperado el 08 de Febrero de 2016, de Recuperación sencilla para AIX , costo efectiva y en la que se puede confiar: http://world.visionsolutions.com/world/Espanol/Products/Disaster-Recovery-DT-RecoverNow.aspx

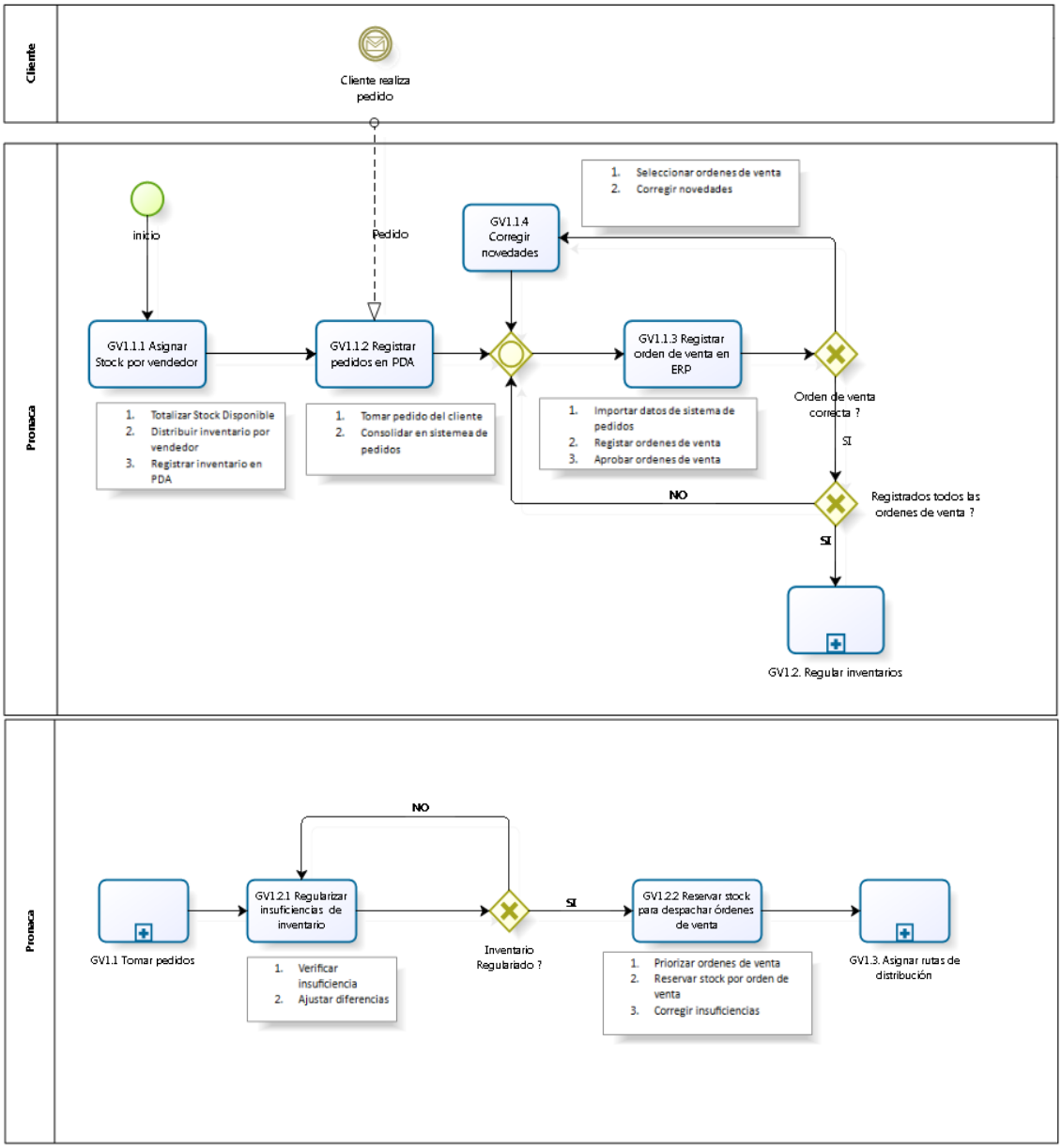
VMWARE. (2015). *Site Recovery Manager*. Recuperado el 07 de Febrero de 2016, de http://www.vmware.com/latam/products/site-recovery-manager/

ANEXOS

ANEXO A

DIAGRAMAS DE FLUJO DE LOSPROCESOS DE NEGOCIO DE PRONACA

Las figuras A1, A2, A3 y A4 muestran a detalle las actividades de cada proceso de negocio.



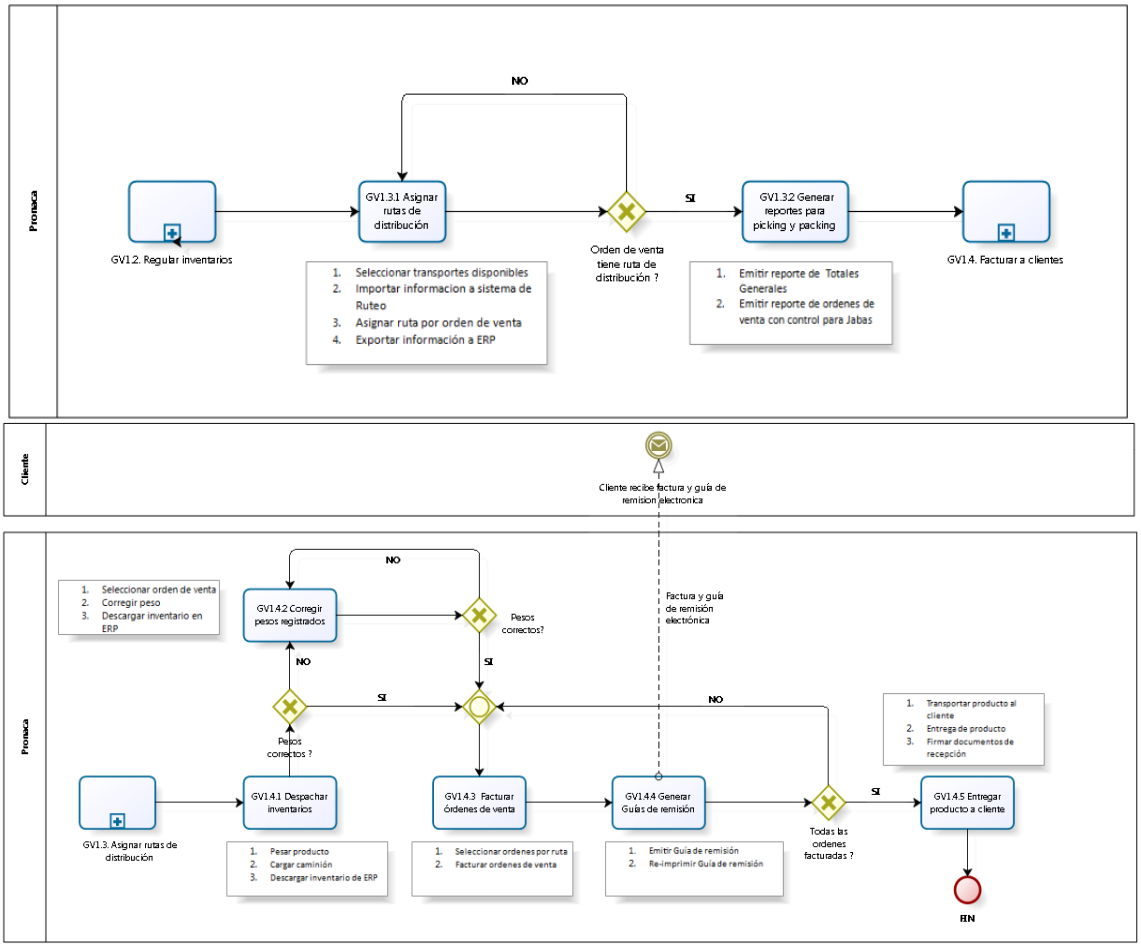


Figura A1. Proceso gestión de ventas consumo hogar.

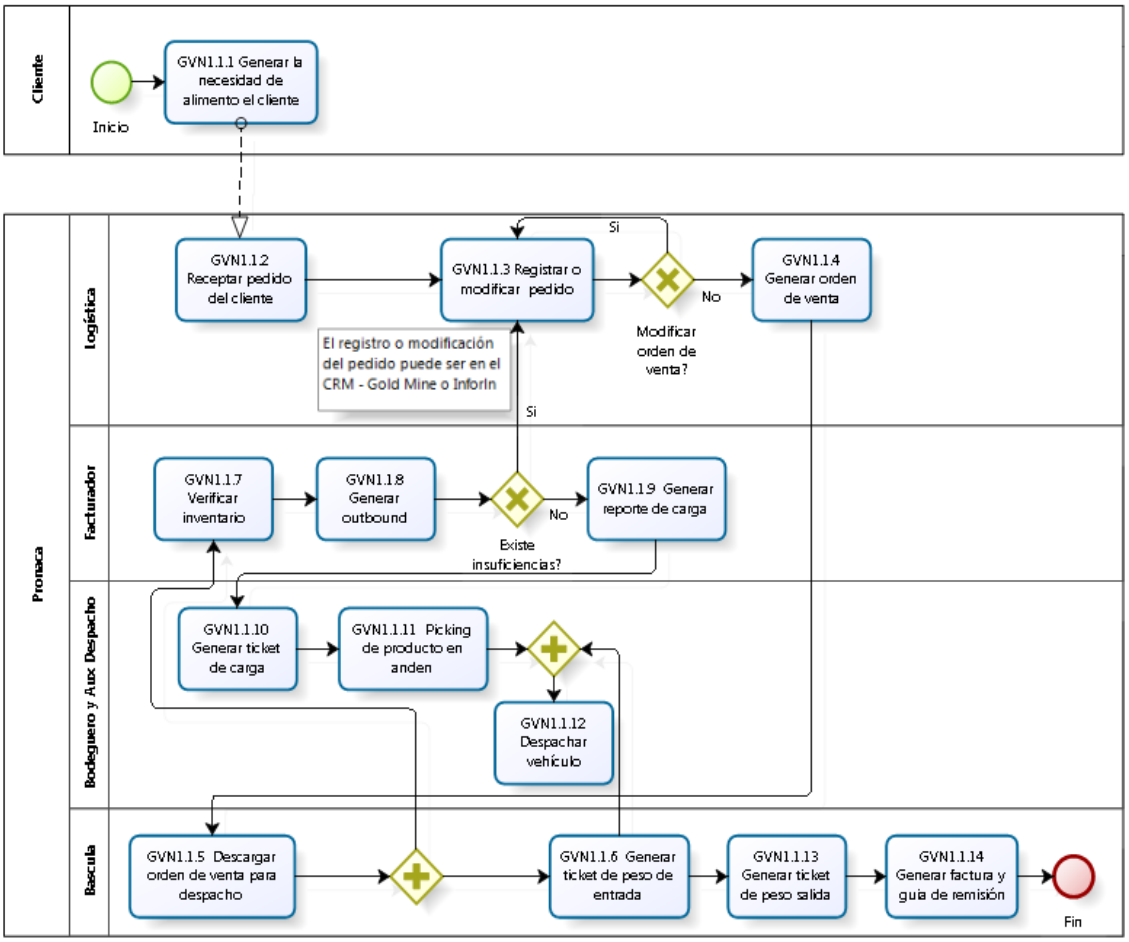
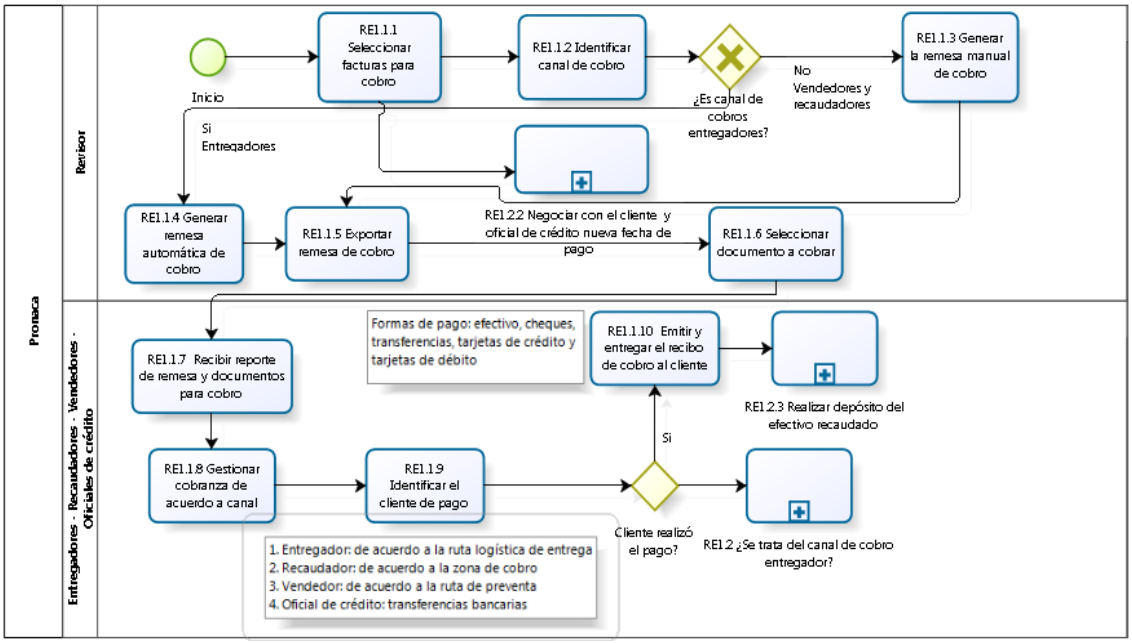


Figura A2. Proceso gestión de ventas nutrición & salud animal y negocio agrícola.



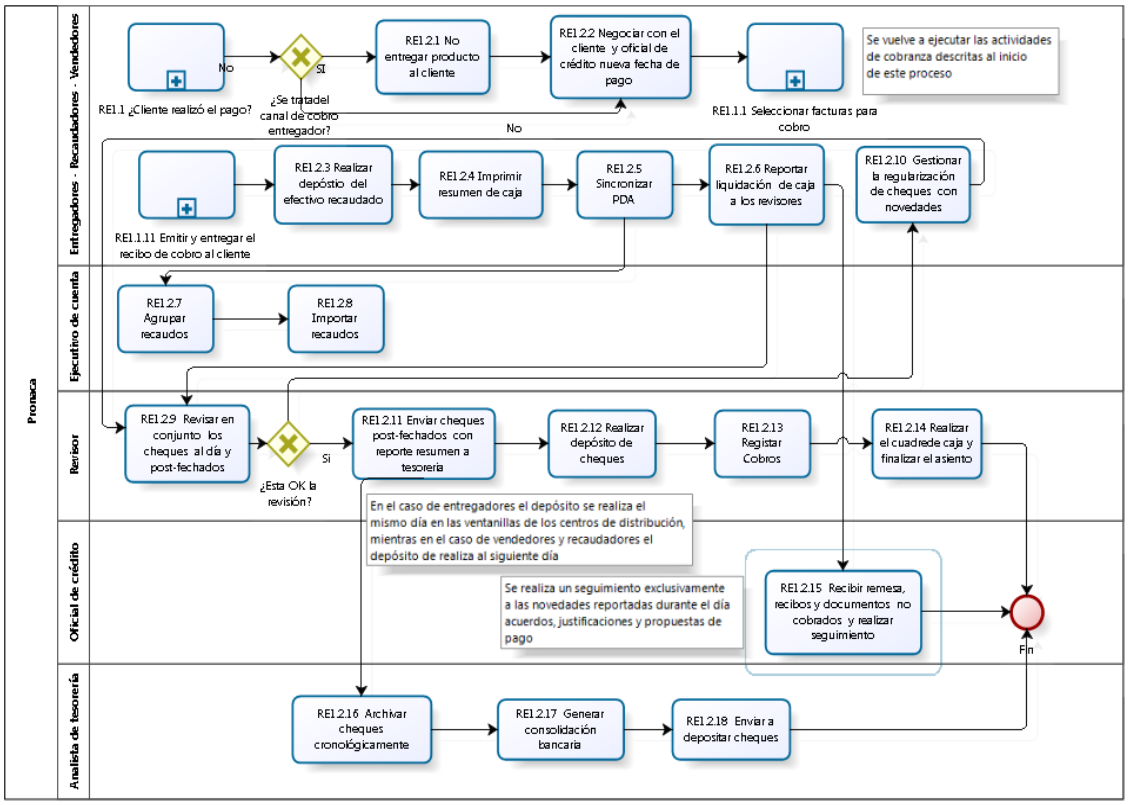


Figura A3. Proceso recaudaciones consumo hogar.

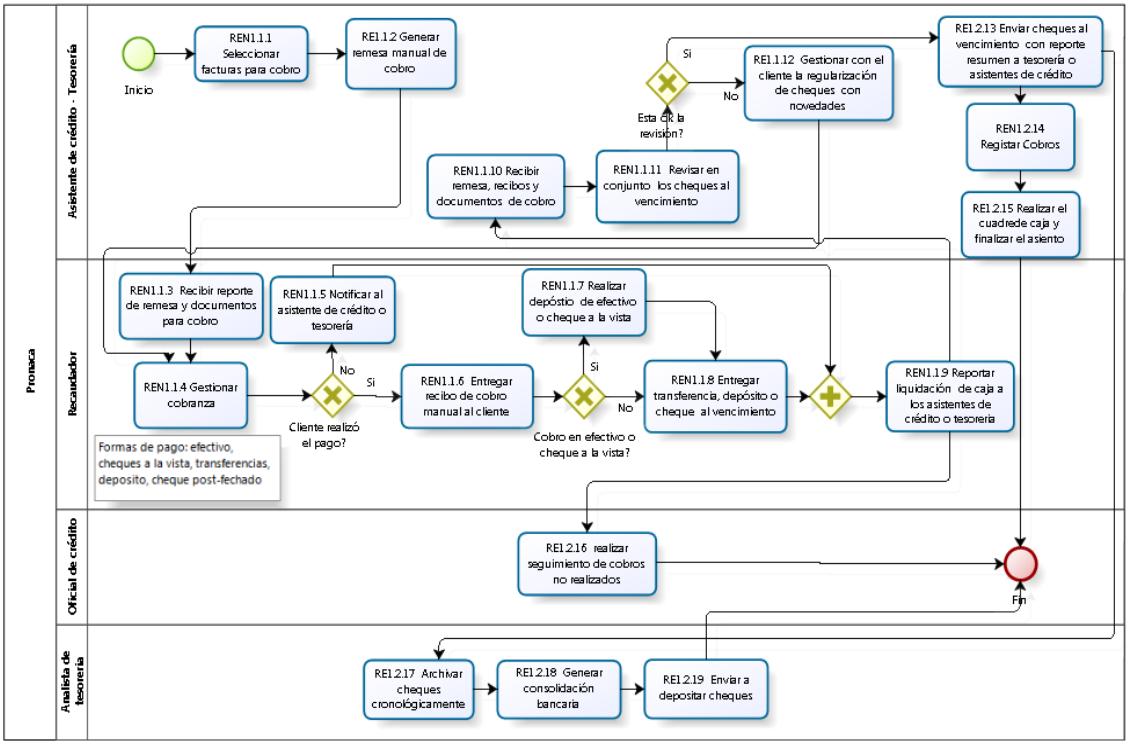


Figura A4. Proceso recaudaciones nutrición & salud animal y negocio agrícola.

ANEXO B

ELABORACIÓN Y/O ACTUALIZACIÓN DE POLÍTICAS Y/O PROCEDIMIENTOS

CATEGORIZACIÓN:		PROCEDIMIENTOS ADMINISTRATIVOS	
NEGOCIO:	CORPORATIVOS	**FECHA EMISIÓN:**	17/02/2014
PROCESO:	ADMINISTRACIÓN	**FECHA PUBLICACIÓN:**	17/02/2014
ÁREA:	ADMINISTRACIÓN GENERAL	**FECHA ÚLTIMA ACTUALIZACIÓN:**	
POLÍTICA:	ELABORACION Y/O ACTUALIZACIÓN DE POLITICAS Y/O PROCEDIMIENTOS	**CÓDIGO:**	CPADAGPR17

1. Objetivos

Definir los parámetros generales bajo los cuales se deben sujetar los responsables dueños de los procesos de la estandarización y centralización de la información tanto corporativa como de cada Negocio.

Documentar los pasos que tienen que seguir los Colaboradores y/o dueños de los procesos, ya sea para: documentar un nuevo documento o actualizar un documento existente.

2. Alcance

Aplicable a PRONACA y sus Compañías Relacionadas.

3. Exposición del procedimiento

3.1. Definiciones

3.1.1. Políticas: Conjunto de criterios generales que establecen el marco de referencia para el desempeño de los procesos o actividades.

3.1.2. Procedimientos: Es un documento que describe, claramente, los pasos secuenciales para iniciar, desarrollar y concluir una actividad (operación) relacionada con el proceso productivo (producto o servicio), los elementos técnicos a emplear, los requerimientos, el alcance y limitaciones fijadas, el número del personal que interviene, etc.

3.1.3. Instructivo: Describe de forma detallada el “cómo” desarrollar una actividad dentro de un procedimientos.

3.1.4. Fichas Técnicas, Métodos de Análisis, Guías de Trabajo, Hojas de Rendimiento: Documentos propios de cada negocio que especifican datos técnicos de cada producto o proceso.

3.2. Categorización de Documentos

3.2.1. Políticas Corporativas: Son aquellas que apoyan a los objetivos corporativos y que sirven de guía para organización, están alineados estrechamente con la planificación estratégica y la valoración del riesgo.

3.2.2. Políticas y Procesos Administrativos: Son documentos creados por las distintas áreas en función a la repetición de sus actividades, y que son relativamente estables.

3.2.3. Políticas y Procesos Operacionales: Son documentos donde se concentra la mayor cantidad de procedimientos comerciales y de producción con actividades que regulan el proceso productivo y de comercialización.

3.3. Nuevo Documento: Inicio – Elaboración

3.3.1. Se ha definido un documento estándar que cumple con todos los requisitos para la administración de la información. (Ver Anexo B1). Los centros de Operación que han tenido certificaciones mantendrán el formato definido para el efecto y la codificación se mantendrá (solo en el texto), a fin de facilitar la trazabilidad del documento.

3.3.2. Los Colaboradores responsables del manejo de documentos, deben hacer uso de este formato y enviar al Analista de Control Operacional para continuar con el proceso de ingreso al sistema.

3.3.3. Cada documento a crearse, deben tener obligatoriamente una persona responsable del proceso, que no es precisamente quién redacta dicho documento, con el fin de controlar el cumplimiento de los descrito en las políticas, procedimientos u otros documentos que se encuentran publicados en la base de la Intranet “Manual de Políticas Corporativas”.

3.3.4. Durante la documentación de las actividades administrativas y/o de control de un procedimiento, es importante indicar quién o quiénes son los responsables por ejecutar, revisar o aprobar una determinada actividad.

3.3.5. Así mismo, es importante considerar que durante la documentación de una actividad, para que ésta se encuentre apropiadamente documentada, se puede contestar las siguientes interrogantes: ¿qué?, ¿cómo?, ¿cuándo?, ¿dónde?, ¿por qué?, ¿quién?, etc.

3.3.6. Cada procedimiento debe contener los controles mínimos del proceso que contribuyan a mitigar los riesgos inherentes tales como: niveles de revisión y aprobación apropiados, segregación de funciones, seguimiento y monitoreo de las actividades, controles automáticos, etc. Estos controles serán validados o sugeridos por la

Unidad de Control Operacional durante su proceso de revisión, previo a la publicación de un nuevo documento.

3.4. Nuevo Documento y/o Actualización: Revisiones y Aprobaciones

3.4.1. A través de la Intranet o de forma manual, los documentos son enviados a las personas involucradas en el proceso para su revisión o aprobación, el tiempo de estas actividades son controladas automáticamente por el sistema o manualmente por medio del Analista de Control Operacional.

3.4.2. El sistema actualmente está parametrizado para tomar acción con tres (3) días laborables, si algún Colaborador asignado no realiza esta actividad, automáticamente el sistema continúa su proceso al siguiente nivel y será su responsabilidad en caso de existir inconvenientes luego de la publicación del documento. Estatus Feb. 2014: Al momento este control se lo encuentra realizando el Analista de Control Operacional de forma manual.

3.4.3. Si los Colaboradores encargados de la revisión y aprobación no pudieran avanzar con este proceso, el sistema permite delegar estas actividades a otras personas, o puede solicitar al Analista de Control Operacional una ampliación del plazo siendo este no más de siete (7) días calendario.

3.4.4. El Analista de Control Operacional será el responsable de realizar un seguimiento de la oportuna revisión y/o aprobación de los niveles correspondientes registrados en los documentos.

3.4.5. Las revisiones y aprobaciones sólo aplican para Políticas y Procedimientos, el resto de documentos se publican con la aprobación a través del e-mail del nivel correspondiente.

3.5. Nuevo Documento y/o Actualización: Niveles de Aprobación

3.5.1. Consúltese los siguientes niveles de revisión y aprobación para la publicación y/o actualización de documentos:

Tabla AnexoB1. Niveles de Revisión y Aprobación de Documentos

Niveles de Revisión y Aprobación de Documentos				
Tipo de Documento	**Aplicación**	**Revisión**	**Aprobación**	**Workflow**
Reglamentos	Corporativa	Directores	Directorio	NO
Manuales	Corporativa	Directores	Gerentes de Negocio	NO
Políticas	Corporativa		Director Finanzas y Planeación	SI
Políticas	Cias. Relacionadas	Gerente Adm. Financiero	Directorio	SI
Políticas	A Negocios	Gerente de Negocio	Directorio	SI
Políticas	A Departamentos	Directores	Director Finanzas y Planeación	SI
Políticas	A Áreas	Directores	Director Finanzas y Planeación y/o Directores	SI
Procedimientos	Corporativa	Directores	Director Finanzas y Planeación	SI
Procedimientos	A Negocios	Gerente Adm. Financiero	Gerente de Negocio	SI
Procedimientos	A Departamentos	Gerente Adm. Financiero	Directores	SI
Procedimientos	A Áreas	Directores	Gerente de Negocio	SI
Instructivos	Corporativa	Directores	Directores	NO
Fichas Técnicas	A Negocios	Gerentes	Gerentes de Negocio o Delegados	NO
Métodos de Análisis	A Negocios	Gerentes	Gerentes de Negocio o Delegados	NO
Otros doc. Propios del Negocio	A Negocios	Gerentes	Gerentes de Negocio o Delegados	NO

3.6. Nuevo Documento y/o Actualización: Publicación y Difusión

3.6.1. Concluidas las revisiones, modificaciones y aprobaciones, el sistema automáticamente ó a través del Analista de Control Operacional, se notificará que el documento ha sido publicado.

3.6.2. La difusión de la información se realizará a través del correo electrónico.

3.7. Funciones del Sistema Workflow

3.7.1. El flujo de procesos está encaminado a:

3.7.1.1. Promover el sistema de publicación de Documentos Corporativos y propios de cada Negocio.

3.7.1.2. Difundir esta información a través de la Intranet.

3.7.1.3. Registrar los revisores y aprobadores de los documentos.

3.7.1.4. Otorgar un valor agregado a los usuarios mediante el acceso individual a la información.

3.7.2. Este sistema es el único autorizado para revisar, aprobar, actualizar y publicar las políticas, procedimientos y demás documentos que sean de suma importancia para la organización.

3.8. Fortalezas del Sistema

3.8.1. Información actualizada y centralizada en una sola base; al alcance de todos los Colaboradores

3.8.2. No permite imprimir, editar ni copiar en medio magnéticos, reduciendo de esta manera los costos de impresión y la alteración de su contenido. Sólo de enviarán copias controladas a los Centros de Operación que no dispongan de la Intranet.

3.8.3. La información publicada en la base, es la única que regirá para efectos de control y auditoría.

3.9. Pasos para la Publicación de un Nuevo Documento o para la Actualización de uno ya existente

3.9.1. Publicación Nuevo Documento:

3.9.1.1. Enviar al Analista de Control Operacional la política y/o procedimiento con sus respectivos anexos, que se desea publicar.

3.9.1.2. Considerar si existe otro documento similar publicado en la Intranet que debería ser enviado al archivo histórico o complementado, para ello se deberá solicitar al Analista de Control Operacional un inventario de políticas y procedimientos colgados en la Intranet.

3.9.2. Actualización de un Documento Existente:

3.9.2.1. Solicitar al Analista de Control Operacional, un inventario de políticas y/o procedimientos actualmente publicados en la Intranet.

3.9.2.2. Identificar qué documentos necesitan ser actualizados.

3.9.2.3. Solicitar al Analista de Control Operacional el documento que desea actualizar en el formato de Word autorizado por la compañía.

3.9.2.4. Realice los cambios de rigor y solicite la debida revisión interna de su área o departamento de los niveles correspondientes. Se solicita activar la opción en Microsoft Word de control de cambio (opción: “Revisar” / “Control de cambios”).

3.9.3. Pasos en Común para la Publicación y/o Actualización:

3.9.3.1. Solicitar la revisión del Analista de Control Operacional al documento que desea publicar y/o actualizar a fin de obtener potenciales oportunidades de mejora.

3.9.3.2. Valide y/o acuerde las oportunidades de mejora sugeridas, si las hubiere.

3.9.3.3. Imprimir el documento final revisado y acordado, e incorpore las firmas de responsabilidad de quienes: elaboraron/actualizaron, revisaron y aprobaron.

3.9.3.4. Finalmente entregar el documento impreso firmado al Analista de Control Operacional para la actualización respectiva en la Intranet y su posterior socialización.

4. Anexos

- Formato para elaborar documentos

CATEGORIZACIÓN:		
NEGOCIO:	**FECHA EMISIÓN:**	17/02/2014
PROCESO:	**FECHA PUBLICACIÓN:**	Asigna el sistema
ÁREA:	**FECHA ÚLTIMA ACTUALIZACIÓN:**	Asigna el sistema
POLÍTICA O PROCEDIMIENTO:	**CÓDIGO:**	Asigna el sistema

1. Objetivo

Debe ser concreto y utilizar los verbos en infinitivo.

2. Alcance

Que áreas o negocios son los que están involucrados en el Proceso a documentarse.

3. Exposición de la política o procedimiento

3.1. Subtítulos

3.2. Párrafos con letra Tahoma, fuente 12, e interlineado 1.5.

4. Responsabilidades

Responsables de la aplicación del proceso (cargo formal según estructura de DO)

- Documentar en verbo infinitivo, las responsabilidades de cada cargo.

5. Anexos

Flujogramas, imágenes, formatos, formularios y otros; estos anexos pueden ser impresos o grabados en el disco.

Elaborado por:	Revisado por:	Aprobado por:

Nota 1: En el caso de que el documento se publicado con carácter de confidencial, para efectos de seguridad de la información, favor enviar el listado de los Colaboradores autorizados para la visualización y lectura en la Intranet de dicho documento.

Nota 2: Para la legalización de la publicación de los documentos en la base de la Intranet, deberán ser revisados y aprobados por los niveles correspondientes y validado por la Unidad de Control Operacional. Favor enviar documento impreso firmado por los responsables de su elaboración, revisión y aprobación.

5. Responsabilidades

Dueño del Proceso

- Redactar los procesos para formalizar su aplicación.
- Realizar evaluaciones respecto a la aplicación.
- Realizar cambios o modificaciones de acuerdo a las necesidades.
- Actualizar los documentos de acuerdo a las nuevas realidades de los procesos.

Revisor (es)

- Revisar y comentar acerca del documento.

Aprobador (es)

- Aprobar o rechazar los documentos y emitir sus comentarios y sugerencias en caso de existir.

Analista de Control Operacional

- Colaborar en el relevamiento de la información.
- Coordinar con el dueño del proceso la correcta redacción y codificación de los documentos.
- Coordinar la asignación de Revisores y Aprobadores.
- Controlar el flujo normal del proceso.
- Publicar y difundir todos los documentos.
- Coordinar las actualizaciones, modificaciones o reemplazo de los documentos.
- Dar soporte a los usuarios y al personal de Auditoría.

ANEXO C

ENCUESTAS DE VALORACIÓN DE ANÁLISIS DE IMPACTO

Resultado de la encuesta realizada al Gerente de consumo hogar logística dueño del proceso gestión de ventas consumo hogar.

- Impacto Económico

#	Cuestionario	Sí	No	Valoración Cualitativa			
				4 horas	1 día	2 días	1 semana
1	¿Varía el impacto en los ingresos en función del día o mes de año?	X					
2	Si es así, indique cuando se producen los picos	Más grave el impacto el día viernes y el último día laborable del mes					
3	En la fecha más crítica ¿cuál es el impacto en los ingresos si el proceso no puede finalizar?	X		1	2	2	3
4	¿Se perderían descuentos si, como consecuencia de la interrupción del proceso, no se realizaran los pagos en los plazos previstos? Si es así, ¿cuánto?		X				
5	¿Se perderían intereses si, como consecuencia de la interrupción del proceso? Si es así, ¿cuánto?		X				
6	¿Se incrementarían los costos como consecuencia de la interrupción del proceso? (salarios improductivos, pérdida de productividad, aumento de rechazos por pérdida de calidad, etc.) Si es así ¿cuánto?		X				
7	¿Aumentarían los costos de almacenamientos debido a la imposibilidad de enviar productos y mercancías? Si es así ¿cuánto?	X		1	2	3	4
8	¿Se producirían costos adicionales de operación (horas extra, reconstrucción de trabajos perdidos, etc.)? Si es así ¿cuánto?	X		1	1	2	3
	Impacto cualitativo máximo =			1	2	3	4

- Impacto Comercial

#	Cuestionario	Sí	No	Valoración Cualitativa			
				4 horas	1 día	2 días	1 semana
1	¿Habrá impacto en futuros negocios si este proceso se interrumpe?	X		0	1	2	3
2	¿Se producirán costos puntuales si se interrumpiera este proceso (publicidad, marketing, nuevos productos, etc.)?		X				
3	¿Se perderían inversiones ya hechas si se interrumpe este proceso? (publicidad, promociones, publicaciones, etc.)?		X				
4	¿Tendrá impacto en los clientes si queda interrumpido este proceso de negocio?	X		0	1	2	3
5	¿Tendrá un impacto negativo en los clientes si, como consecuencia de la interrupción del proceso no se puede emitir facturas?	X		0	1	1	2
6	¿Habrá un aumento en las reclamaciones de los clientes si se produce una interrupción que impida gestionar sus pedidos?	X		0	1	2	3
7	¿Habría incumplimiento de contratos con clientes con repercusiones legales?		X				
8	¿Podría la organización perder porcentaje de participación en el mercado debido a la interrupción de este proceso?	X		0	1	1	2
9	Si se retrasara el lanzamiento de nuevos productos como consecuencia de la interrupción de este proceso, ¿Se vería impactada la posición de mercado?		X				
10	¿Hay riesgo de cambio de proveedor si no se atienden las necesidades de los clientes?	X		0	1	1	2
	Impacto cualitativo máximo =			0	1	2	3

- Impacto Operacional

#	Cuestionario	Sí	No	Valoración Cualitativa			
				4 horas	1 día	2 días	1 semana
1	¿Se perderán descuentos si, como consecuencia de la interrupción del proceso, no se realizaran los pagos en los plazos previstos? Si es así, ¿Cuánto?		X				
2	¿Se produciría deterioro de productos por exceso de tiempo de almacenaje si la función queda interrumpida?		X				
3	¿Se incrementarían los costos como consecuencia de la interrupción del proceso? (salarios improductivos, pérdida de productividad, aumento de rechazos por pérdida de calidad, etc.) Si es así, ¿cuánto?		X				
4	¿Aumentarían los costos de almacenamiento debido a la imposibilidad de enviar productos y mercancías? Si es así, ¿cuánto?	X		1	2	3	4
5	¿Se producirían costos adicionales de operación (horas extra, reconstrucción de trabajos perdidos, etc.)? Si es así, ¿cuánto?	X		1	1	2	3
6	¿Sufriría algún impacto el flujo de trabajo si queda interrumpido el proceso de negocio?	X		1	1	2	3
7	¿Sufrirán impactos operacionales otras dependencias de la organización, nacionales o internacionales?		X				
8	¿Se causará un grave perjuicio a los proveedores si las facturas no se pagan a tiempo?		X				
9	¿Podría pararse la producción debido a la interrupción del proceso?		X				
10	¿Causa impacto la interrupción del proceso en la seguridad e higiene en el trabajo?		X				
	Impacto cualitativo máximo =			1	2	3	4

- Impacto Imagen

#	Cuestionario	Sí	No	Valoración Cualitativa			
				4 horas	1 día	2 días	1 semana
1	¿Sufrirá algún impacto la imagen de la organización en el exterior si el proceso se interrumpe?		X				
2	¿Sufrirá algún impacto la imagen de la organización antes los propios empleados que pueda dar lugar a desmoralización?		X				
3	¿Sufrirá algún impacto la imagen de la organización ante los propios empleados que pueda dar lugar a problemas laborables?		X				
4	¿Habrá algún impacto medio ambiental que afecte a la imagen de la organización ante la sociedad?		X				
5	Si como consecuencia de la interrupción del proceso, hay que variar las condiciones de presentación, embalaje, empaquetado, etc. Sin variar la calidad, ¿se vería impactada la imagen de la organización?		X				
6	Si como consecuencia de la interrupción del proceso, hay que variar los programas de entregas de los suministradores, ¿se vería impactada la credibilidad de la organización?		X				
7	Si como consecuencia la de interrupción del proceso, se retrasa la información financiera, ¿se vería impactada la credibilidad de la organización ante organismos externos? (Administración, mercado de valores, entidades financieras, auditores externos, etc.)	X		0	1	1	3
8	Si como consecuencia de la interrupción del proceso, se retrasa la información financiera, ¿se vería impactada la credibilidad de la organización ante estamentos superiores o inferiores de la propia organización? (Filiales, oficinas centrales, empresas		X				

	asociadas, etc.)						
9	¿Puede dar lugar la interrupción a que los medios de comunicación se hagan eco de sus consecuencias?		X				
10	¿Se debilitará la imagen de la organización ante los agentes sociales? (Organizaciones empresariales, centrales sindicales, colegios profesionales, etc.)		X				
	Impacto cualitativo máximo =			0	1	1	3

- Impacto Legal

#	Cuestionario	Sí	No	Valoración Cualitativa			
				4 horas	1 día	2 días	1 semana
1	¿Se incurriría en penalizaciones por retraso de pagos, si el proceso no finaliza?		X				
2	¿Habría multas si no se hicieran puntualmente los pagos de impuestos, seguridad social, etc.?	X		0	1	1	2
3	¿Se incumpliría alguna ley si el proceso no finaliza?		X				
4	¿Se produciría incumplimiento de alguna normativa laboral/sindical si el proceso no finaliza?		X				
5	¿Habría incumplimiento de contratos con repercusiones legales?		X				
6	¿Habrá responsabilidades legales por impacto medio ambiental si el proceso no finaliza?		X				
7	¿Puede haber responsabilidades legales frente a socios, accionistas, clientes, etc. Si el proceso no finaliza a tiempo?		X				
8	¿Habría responsabilidades legales si se perdieran archivos y documentación de soporte? (Por ejemplo por pérdida de datos personales ante la agencia de protección de datos)	X		1	1	2	3
9	¿Estaría la organización sujeta a penalizaciones por la incapacidad de suministrar a tiempo sus productos/servicios?		X				
10	Si los procedimientos de respuesta ante la crisis no son atendidos adecuadamente en el tiempo, ¿Se vería la organización sujeta a demandas relacionadas con la seguridad de las personas?		X				
	Impacto cualitativo máximo =			1	1	2	3

Resultado de la encuesta realizada al Gerente de logística agropecuaria dueño del proceso gestión de ventas nutrición & salud animal y negocio agrícola.

- Impacto Económico

#	Cuestionario	Sí	No	Valoración Cualitativa			
				4 horas	1 día	2 días	1 semana
1	¿Varía el impacto en los ingresos en función del día o mes de año?	X					
2	Si es así, indique cuando se producen los picos	Más grave el impacto en el mes de diciembre					
3	En la fecha más crítica ¿cuál es el impacto en los ingresos si el proceso no puede finalizar?	X		1	2	3	4
4	¿Se perderían descuentos si, como consecuencia de la interrupción del proceso, no se realizaran los pagos en los plazos previstos? Si es así, ¿cuánto?		X				
5	¿Se perderían intereses si, como consecuencia de la interrupción del proceso? Si es así, ¿cuánto?		X				
6	¿Se incrementarían los costos como consecuencia de la interrupción del proceso? (salarios improductivos, pérdida de productividad, aumento de rechazos por pérdida de calidad, etc.) Si es así ¿cuánto?	X		0	1	2	3
7	¿Aumentarían los costos de almacenamientos debido a la imposibilidad de enviar productos y mercancías? Si es así ¿cuánto?	X		0	0	1	2
8	¿Se producirían costos adicionales de operación (horas extra, reconstrucción de trabajos perdidos, etc.)? Si es así ¿cuánto?	X		0	1	2	3
	Impacto cualitativo máximo =			1	2	3	4

- Impacto Comercial

#	Cuestionario	Sí	No	Valoración Cualitativa			
				4 horas	1 día	2 días	1 semana
1	¿Habrá impacto en futuros negocios si este proceso se interrumpe?	X		0	1	2	3
2	¿Se producirán costos puntuales si se interrumpiera este proceso (publicidad, marketing, nuevos productos, etc.)?	X		0	0	1	3
3	¿Se perderían inversiones ya hechas si se interrumpe este proceso? (publicidad, promociones, publicaciones, etc.)?	X		0	0	1	3
4	¿Tendrá impacto en los clientes si queda interrumpido este proceso de negocio?	X		1	2	2	3
5	¿Tendrá un impacto negativo en los clientes si, como consecuencia de la interrupción del proceso no se puede emitir facturas?	X		1	2	2	3
6	¿Habrá un aumento en las reclamaciones de los clientes si se produce una interrupción que impida gestionar sus pedidos?	X		1	2	2	3
7	¿Habría incumplimiento de contratos con clientes con repercusiones legales?	X		1	2	2	3
8	¿Podría la organización perder porcentaje de participación en el mercado debido a la interrupción de este proceso?	X		1	2	2	3
9	Si se retrasara el lanzamiento de nuevos productos como consecuencia de la interrupción de este proceso, ¿Se vería impactada la posición de mercado?	X		1	2	2	3
10	¿Hay riesgo de cambio de proveedor si no se atienden las necesidades de los clientes?	X		1	2	2	3
	Impacto cualitativo máximo =			1	2	2	3

- Impacto Operacional

#	Cuestionario	Sí	No	Valoración Cualitativa			
				4 horas	1 día	2 días	1 semana
1	¿Se perderán descuentos si, como consecuencia de la interrupción del proceso, no se realizaran los pagos en los plazos previstos? Si es así, ¿Cuánto?		X				
2	¿Se produciría deterioro de productos por exceso de tiempo de almacenaje si la función queda interrumpida?	X		0	0	0	2
3	¿Se incrementarían los costos como consecuencia de la interrupción del proceso? (salarios improductivos, pérdida de productividad, aumento de rechazos por pérdida de calidad, etc.) Si es así, ¿cuánto?	X		0	1	2	3
4	¿Aumentarían los costos de almacenamiento debido a la imposibilidad de enviar productos y mercancías? Si es así, ¿cuánto?	X		0	0	1	2
5	¿Se producirían costos adicionales de operación (horas extra, reconstrucción de trabajos perdidos, etc.)? Si es así, ¿cuánto?	X		0	1	2	3
6	¿Sufriría algún impacto el flujo de trabajo si queda interrumpido el proceso de negocio?	X		1	1	2	3
7	¿Sufrirán impactos operacionales otras dependencias de la organización, nacionales o internacionales?	X		0	1	2	3
8	¿Se causará un grave perjuicio a los proveedores si las facturas no se pagan a tiempo?	X		0	1	2	3
9	¿Podría pararse la producción debido a la interrupción del proceso?	X		0	1	2	3
10	¿Causa impacto la interrupción del proceso en la seguridad e higiene en el trabajo?	X		0	0	1	2
	Impacto cualitativo máximo =			1	1	2	3

- Impacto Imagen

#	Cuestionario	Sí	No	Valoración Cualitativa			
				4 horas	1 día	2 días	1 semana
1	¿Sufrirá algún impacto la imagen de la organización en el exterior si el proceso se interrumpe?	X		0	0	1	2
2	¿Sufrirá algún impacto la imagen de la organización antes los propios empleados que pueda dar lugar a desmoralización?		X				
3	¿Sufrirá algún impacto la imagen de la organización ante los propios empleados que pueda dar lugar a problemas laborables?	X		0	0	0	1
4	¿Habrá algún impacto medio ambiental que afecte a la imagen de la organización ante la sociedad?		X				
5	Si como consecuencia de la interrupción del proceso, hay que variar las condiciones de presentación, embalaje, empaquetado, etc. Sin variar la calidad, ¿se vería impactada la imagen de la organización?		X				
6	Si como consecuencia de la interrupción del proceso, hay que variar los programas de entregas de los suministradores, ¿se vería impactada la credibilidad de la organización?	X		0	0	1	2
7	Si como consecuencia la de interrupción del proceso, se retrasa la información financiera, ¿se vería impactada la credibilidad de la organización ante organismos externos? (Administración, mercado de valores, entidades financieras, auditores externos, etc.)	X		0	0	1	3
8	Si como consecuencia de la interrupción del proceso, se retrasa la información financiera, ¿se vería impactada la credibilidad de la organización ante estamentos superiores o inferiores de la propia organización? (Filiales, oficinas centrales, empresas asociadas, etc.)	X		0	0	1	3

9	¿Puede dar lugar la interrupción a que los medios de comunicación se hagan eco de sus consecuencias?		X				
10	¿Se debilitará la imagen de la organización ante los agentes sociales? (Organizaciones empresariales, centrales sindicales, colegios profesionales, etc.)		X				
	Impacto cualitativo máximo =			0	0	1	3

- Impacto Legal

#	Cuestionario	Sí	No	Valoración Cualitativa			
				4 horas	1 día	2 días	1 semana
1	¿Se incurriría en penalizaciones por retraso de pagos, si el proceso no finaliza?	X		0	0	0	2
2	¿Habría multas si no se hicieran puntualmente los pagos de impuestos, seguridad social, etc.?	X		0	0	1	2
3	¿Se incumpliría alguna ley si el proceso no finaliza?	X		0	0	1	2
4	¿Se produciría incumplimiento de alguna normativa laboral/sindical si el proceso no finaliza?	X		0	0	1	2
5	¿Habría incumplimiento de contratos con repercusiones legales?	X		0	1	2	3
6	¿Habrá responsabilidades legales por impacto medio ambiental si el proceso no finaliza?		X				
7	¿Puede haber responsabilidades legales frente a socios, accionistas, clientes, etc. Si el proceso no finaliza a tiempo?	X		0	1	2	3
8	¿Habría responsabilidades legales si se perdieran archivos y documentación de soporte? (Por ejemplo por pérdida de datos personales ante la agencia de protección de datos)	X		0	1	2	3
9	¿Estaría la organización sujeta a penalizaciones por la incapacidad de suministrar a tiempo sus productos/servicios?	X		0	0	1	2
10	Si los procedimientos de respuesta ante la crisis no son atendidos adecuadamente en el tiempo, ¿Se vería la organización sujeta a demandas relacionadas con la seguridad de las personas?		X				
	Impacto cualitativo máximo =			0	1	2	3

Resultado de la encuesta realizada al Gerente crédito y cobranzas comercial dueño del proceso recaudaciones consumo hogar.

- Impacto Económico

#	Cuestionario	Sí	No	Valoración Cualitativa			
				4 horas	1 día	2 días	1 semana
1	¿Varía el impacto en los ingresos en función del día o mes de año?	X					
2	Si es así, indique cuando se producen los picos	Más grave el impacto los días jueves, viernes, sábado y todo el mes de diciembre					
3	En la fecha más crítica ¿cuál es el impacto en los ingresos si el proceso no puede finalizar?	X		1	2	3	4
4	¿Se perderían descuentos si, como consecuencia de la interrupción del proceso, no se realizaran los pagos en los plazos previstos? Si es así, ¿cuánto?		X				
5	¿Se perderían intereses si, como consecuencia de la interrupción del proceso? Si es así, ¿cuánto?		X				
6	¿Se incrementarían los costos como consecuencia de la interrupción del proceso? (salarios improductivos, pérdida de productividad, aumento de rechazos por pérdida de calidad, etc.) Si es así ¿cuánto?	X		1	1	1	1
7	¿Aumentarían los costos de almacenamientos debido a la imposibilidad de enviar productos y mercancías? Si es así ¿cuánto?	X		1	1	1	1
8	¿Se producirían costos adicionales de operación (horas extra, reconstrucción de trabajos perdidos, etc.)? Si es así ¿cuánto?	X		1	1	1	1
	Impacto cualitativo máximo =			1	2	3	4

- Impacto Comercial

#	Cuestionario	Sí	No	Valoración Cualitativa			
				4 horas	1 día	2 días	1 semana
1	¿Habrá impacto en futuros negocios si este proceso se interrumpe?	X		0	1	1	1
2	¿Se producirán costos puntuales si se interrumpiera este proceso (publicidad, marketing, nuevos productos, etc.)?		X				
3	¿Se perderían inversiones ya hechas si se interrumpe este proceso? (publicidad, promociones, publicaciones, etc.)?		X				
4	¿Tendrá impacto en los clientes si queda interrumpido este proceso de negocio?	X		1	1	1	1
5	¿Tendrá un impacto negativo en los clientes si, como consecuencia de la interrupción del proceso no se puede emitir facturas?	X		1	2	3	4
6	¿Habrá un aumento en las reclamaciones de los clientes si se produce una interrupción que impida gestionar sus pedidos?	X		1	1	1	1
7	¿Habría incumplimiento de contratos con clientes con repercusiones legales?	X		1	1	1	1
8	¿Podría la organización perder porcentaje de participación en el mercado debido a la interrupción de este proceso?		X				
9	Si se retrasara el lanzamiento de nuevos productos como consecuencia de la interrupción de este proceso, ¿Se vería impactada la posición de mercado?		X				
10	¿Hay riesgo de cambio de proveedor si no se atienden las necesidades de los clientes?		X				
	Impacto cualitativo máximo =			1	2	3	4

- Impacto Operacional

#	Cuestionario	Sí	No	Valoración Cualitativa			
				4 horas	1 día	2 días	1 semana
1	¿Se perderán descuentos si, como consecuencia de la interrupción del proceso, no se realizaran los pagos en los plazos previstos? Si es así, ¿Cuánto?		X				
2	¿Se produciría deterioro de productos por exceso de tiempo de almacenaje si la función queda interrumpida?	X		1	1	1	2
3	¿Se incrementarían los costos como consecuencia de la interrupción del proceso? (salarios improductivos, pérdida de productividad, aumento de rechazos por pérdida de calidad, etc.) Si es así, ¿cuánto?	X		1	1	1	1
4	¿Aumentarían los costos de almacenamiento debido a la imposibilidad de enviar productos y mercancías? Si es así, ¿cuánto?	X		1	1	1	1
5	¿Se producirían costos adicionales de operación (horas extra, reconstrucción de trabajos perdidos, etc.)? Si es así, ¿cuánto?	X		1	1	1	1
6	¿Sufriría algún impacto el flujo de trabajo si queda interrumpido el proceso de negocio?	X		1	1	1	1
7	¿Sufrirán impactos operacionales otras dependencias de la organización, nacionales o internacionales?	X		1	1	1	1
8	¿Se causará un grave perjuicio a los proveedores si las facturas no se pagan a tiempo?		X				
9	¿Podría pararse la producción debido a la interrupción del proceso?	X		1	1	2	3
10	¿Causa impacto la interrupción del proceso en la seguridad e higiene en el trabajo?		X				
	Impacto cualitativo máximo =			1	1	2	3

- Impacto Imagen

#	Cuestionario	Sí	No	Valoración Cualitativa			
				4 horas	1 día	2 días	1 semana
1	¿Sufrirá algún impacto la imagen de la organización en el exterior si el proceso se interrumpe?		X				
2	¿Sufrirá algún impacto la imagen de la organización antes los propios empleados que pueda dar lugar a desmoralización?	X		0	1	1	1
3	¿Sufrirá algún impacto la imagen de la organización ante los propios empleados que pueda dar lugar a problemas laborables?	X		0	1	1	1
4	¿Habrá algún impacto medio ambiental que afecte a la imagen de la organización ante la sociedad?		X				
5	Si como consecuencia de la interrupción del proceso, hay que variar las condiciones de presentación, embalaje, empaquetado, etc. Sin variar la calidad, ¿se vería impactada la imagen de la organización?		X				
6	Si como consecuencia de la interrupción del proceso, hay que variar los programas de entregas de los suministradores, ¿se vería impactada la credibilidad de la organización?	X		0	1	1	1
7	Si como consecuencia la de interrupción del proceso, se retrasa la información financiera, ¿se vería impactada la credibilidad de la organización ante organismos externos? (Administración, mercado de valores, entidades financieras, auditores externos, etc.)	X		0	1	1	1
8	Si como consecuencia de la interrupción del proceso, se retrasa la información financiera, ¿se vería impactada la credibilidad de la organización ante estamentos superiores o inferiores de la propia organización? (Filiales, oficinas centrales, empresas asociadas, etc.)		X				

9	¿Puede dar lugar la interrupción a que los medios de comunicación se hagan eco de sus consecuencias?		X				
10	¿Se debilitará la imagen de la organización ante los agentes sociales? (Organizaciones empresariales, centrales sindicales, colegios profesionales, etc.)		X				
	Impacto cualitativo máximo =			0	1	1	1

- Impacto Legal

#	Cuestionario	Sí	No	Valoración Cualitativa			
				4 horas	1 día	2 días	1 semana
1	¿Se incurriría en penalizaciones por retraso de pagos, si el proceso no finaliza?		X				
2	¿Habría multas si no se hicieran puntualmente los pagos de impuestos, seguridad social, etc.?		X				
3	¿Se incumpliría alguna ley si el proceso no finaliza?		X				
4	¿Se produciría incumplimiento de alguna normativa laboral/sindical si el proceso no finaliza?		X				
5	¿Habría incumplimiento de contratos con repercusiones legales?		X				
6	¿Habrá responsabilidades legales por impacto medio ambiental si el proceso no finaliza?		X				
7	¿Puede haber responsabilidades legales frente a socios, accionistas, clientes, etc. Si el proceso no finaliza a tiempo?		X				
8	¿Habría responsabilidades legales si se perdieran archivos y documentación de soporte? (Por ejemplo por pérdida de datos personales ante la agencia de protección de datos)	X		1	2	3	4
9	¿Estaría la organización sujeta a penalizaciones por la incapacidad de suministrar a tiempo sus productos/servicios?	X		1	1	1	1
10	Si los procedimientos de respuesta ante la crisis no son atendidos adecuadamente en el tiempo, ¿Se vería la organización sujeta a demandas relacionadas con la seguridad de las personas?		X				
	Impacto cualitativo máximo =			1	2	3	4

Resultado de la encuesta realizada al Gerente crédito y cobranzas pecuario dueño del proceso recaudaciones nutrición & salud animal y negocio agrícola.

- Impacto Económico

#	Cuestionario	Sí	No	Valoración Cualitativa			
				4 horas	1 día	2 días	1 semana
1	¿Varía el impacto en los ingresos en función del día o mes de año?	X					
2	Si es así, indique cuando se producen los picos	Más grave el impacto en los meses de mayo, junio y julio					
3	En la fecha más crítica ¿cuál es el impacto en los ingresos si el proceso no puede finalizar?	X		0	0	1	1
4	¿Se perderían descuentos si, como consecuencia de la interrupción del proceso, no se realizaran los pagos en los plazos previstos? Si es así, ¿cuánto?	X		0	0	1	1
5	¿Se perderían intereses si, como consecuencia de la interrupción del proceso? Si es así, ¿cuánto?		X				
6	¿Se incrementarían los costos como consecuencia de la interrupción del proceso? (salarios improductivos, pérdida de productividad, aumento de rechazos por pérdida de calidad, etc.) Si es así ¿cuánto?	X		0	1	1	2
7	¿Aumentarían los costos de almacenamientos debido a la imposibilidad de enviar productos y mercancías? Si es así ¿cuánto?	X		0	1	1	2
8	¿Se producirían costos adicionales de operación (horas extra, reconstrucción de trabajos perdidos, etc.)? Si es así ¿cuánto?	X		1	1	2	3
	Impacto cualitativo máximo =			1	1	2	3

- Impacto Comercial

#	Cuestionario	Sí	No	Valoración Cualitativa			
				4 horas	1 día	2 días	1 semana
1	¿Habrá impacto en futuros negocios si este proceso se interrumpe?	X		1	1	2	3
2	¿Se producirán costos puntuales si se interrumpiera este proceso (publicidad, marketing, nuevos productos, etc.)?		X				
3	¿Se perderían inversiones ya hechas si se interrumpe este proceso? (publicidad, promociones, publicaciones, etc.)?	X		0	1	1	2
4	¿Tendrá impacto en los clientes si queda interrumpido este proceso de negocio?	X		1	2	2	3
5	¿Tendrá un impacto negativo en los clientes si, como consecuencia de la interrupción del proceso no se puede emitir facturas?	X		0	1	1	2
6	¿Habrá un aumento en las reclamaciones de los clientes si se produce una interrupción que impida gestionar sus pedidos?	X		2	2	2	3
7	¿Habría incumplimiento de contratos con clientes con repercusiones legales?		X				
8	¿Podría la organización perder porcentaje de participación en el mercado debido a la interrupción de este proceso?	X		0	0	1	2
9	Si se retrasara el lanzamiento de nuevos productos como consecuencia de la interrupción de este proceso, ¿Se vería impactada la posición de mercado?		X				
10	¿Hay riesgo de cambio de proveedor si no se atienden las necesidades de los clientes?	X		0	0	2	3
	Impacto cualitativo máximo =			2	2	2	3

- Impacto Operacional

#	Cuestionario	Sí	No	Valoración Cualitativa			
				4 horas	1 día	2 días	1 semana
1	¿Se perderán descuentos si, como consecuencia de la interrupción del proceso, no se realizaran los pagos en los plazos previstos? Si es así, ¿Cuánto?		X				
2	¿Se produciría deterioro de productos por exceso de tiempo de almacenaje si la función queda interrumpida?	X		0	1	2	3
3	¿Se incrementarían los costos como consecuencia de la interrupción del proceso? (salarios improductivos, pérdida de productividad, aumento de rechazos por pérdida de calidad, etc.) Si es así, ¿cuánto?	X		1	1	1	2
4	¿Aumentarían los costos de almacenamiento debido a la imposibilidad de enviar productos y mercancías? Si es así, ¿cuánto?	X		0	1	1	2
5	¿Se producirían costos adicionales de operación (horas extra, reconstrucción de trabajos perdidos, etc.)? Si es así, ¿cuánto?	X		1	1	2	3
6	¿Sufriría algún impacto el flujo de trabajo si queda interrumpido el proceso de negocio?	X		1	1	2	3
7	¿Sufrirán impactos operacionales otras dependencias de la organización, nacionales o internacionales?	X		1	1	2	3
8	¿Se causará un grave perjuicio a los proveedores si las facturas no se pagan a tiempo?		X				
9	¿Podría pararse la producción debido a la interrupción del proceso?	X		0	1	2	3
10	¿Causa impacto la interrupción del proceso en la seguridad e higiene en el trabajo?		X				
	Impacto cualitativo máximo =			1	1	2	3

- Impacto Imagen

#	Cuestionario	Sí	No	Valoración Cualitativa			
				4 horas	1 día	2 días	1 semana
1	¿Sufrirá algún impacto la imagen de la organización en el exterior si el proceso se interrumpe?	X		0	0	1	2
2	¿Sufrirá algún impacto la imagen de la organización antes los propios empleados que pueda dar lugar a desmoralización?	X		0	1	2	2
3	¿Sufrirá algún impacto la imagen de la organización ante los propios empleados que pueda dar lugar a problemas laborables?	X		0	0	1	2
4	¿Habrá algún impacto medio ambiental que afecte a la imagen de la organización ante la sociedad?		X				
5	Si como consecuencia de la interrupción del proceso, hay que variar las condiciones de presentación, embalaje, empaquetado, etc. Sin variar la calidad, ¿se vería impactada la imagen de la organización?	X		0	1	1	2
6	Si como consecuencia de la interrupción del proceso, hay que variar los programas de entregas de los suministradores, ¿se vería impactada la credibilidad de la organización?	X		1	2	2	3
7	Si como consecuencia la de interrupción del proceso, se retrasa la información financiera, ¿se vería impactada la credibilidad de la organización ante organismos externos? (Administración, mercado de valores, entidades financieras, auditores externos, etc.)	X		0	1	1	3
8	Si como consecuencia de la interrupción del proceso, se retrasa la información financiera, ¿se vería impactada la credibilidad de la organización ante estamentos superiores o inferiores de la propia organización? (Filiales, oficinas centrales, empresas asociadas, etc.)	X		1	1	2	3

9	¿Puede dar lugar la interrupción a que los medios de comunicación se hagan eco de sus consecuencias?	X		0	0	0	2
10	¿Se debilitará la imagen de la organización ante los agentes sociales? (Organizaciones empresariales, centrales sindicales, colegios profesionales, etc.)	X		0	0	0	2
	Impacto cualitativo máximo =			1	2	2	3

- Impacto Legal

#	Cuestionario	Sí	No	Valoración Cualitativa			
				4 horas	1 día	2 días	1 semana
1	¿Se incurriría en penalizaciones por retraso de pagos, si el proceso no finaliza?	X		0	0	1	1
2	¿Habría multas si no se hicieran puntualmente los pagos de impuestos, seguridad social, etc.?	X		1	1	2	3
3	¿Se incumpliría alguna ley si el proceso no finaliza?		X				
4	¿Se produciría incumplimiento de alguna normativa laboral/sindical si el proceso no finaliza?		X				
5	¿Habría incumplimiento de contratos con repercusiones legales?	X		0	0	0	2
6	¿Habrá responsabilidades legales por impacto medio ambiental si el proceso no finaliza?		X				
7	¿Puede haber responsabilidades legales frente a socios, accionistas, clientes, etc. Si el proceso no finaliza a tiempo?	X		0	1	1	2
8	¿Habría responsabilidades legales si se perdieran archivos y documentación de soporte? (Por ejemplo por pérdida de datos personales ante la agencia de protección de datos)	X		0	0	0	2
9	¿Estaría la organización sujeta a penalizaciones por la incapacidad de suministrar a tiempo sus productos/servicios?		X				
10	Si los procedimientos de respuesta ante la crisis no son atendidos adecuadamente en el tiempo, ¿Se vería la organización sujeta a demandas relacionadas con la seguridad de las personas?		X				
	Impacto cualitativo máximo =			1	1	2	3

ANEXO D

PROCEDIMIENTO DE ALMACENAMIENTO Y CUSTODIA DE RESPALDOS

CATEGORIZACIÓN:		PROCEDIMIENTOS ADMINISTRATIVOS	
NEGOCIO:	CORPORATIVOS	**FECHA EMISIÓN:**	30/06/2010
PROCESO:	TECNOLOGÍA INFORMÁTICA	**FECHA PUBLICACIÓN:**	07/07/2010
ÁREA:	TECNOLOGÍA INFORMÁTICA	**FECHA ÚLTIMA ACTUALIZACIÓN:**	28/12/2015
POLÍTICA:	ALMACENAMIENTO Y CUSTODIA DE RESPALDOS	**CÓDIGO:**	TICPSSPTPRC5

1. Objetivo

Definir el proceso y los responsables de su cumplimiento en el manejo y control de los medios (cintas) utilizados con la herramienta Tivoly Storage Manager en la toma de respaldos del Data Center de la compañía.

2. Alcance

Aplicable a la Gerencia de Operaciones de Tecnologías de Información y Administradores de Bases de Datos de Pronaca y sus Compañías Relacionadas.

3. Exposición del procedimiento

3.1. Generalidades

3.1.1. La Compañía utiliza como herramienta de respaldos y recuperación *Tivoly Storage Manager* TSM de IBM, herramienta de clase y alcance mundial.

3.1.2. TSM mantiene una base de datos interna en la cual se registra detalladamente la información contenida en cada una de las cintas utilizadas

en los procesos de respaldo. Dicha base de datos es respaldada automáticamente una vez por día.

3.1.3. Diariamente el respaldo de la base de datos es copiado mediante un script automático hacia un servidor ftp y las cintas son enviadas a un sitio externo (Ecuadasa Guayaquil).

3.1.4. La base de datos de TSM es el principal medio de obtención del inventario de cintas utilizadas en los procesos de respaldo. Como complemento a este, se mantiene la bitácora de registro de envió de cintas a sitio externo, en donde se registrara el código de cinta(s) correspondiente que se envía en cada paquete, una vez al mes.

3.1.5. En los casos que se requiera recuperar información, mediante la línea de comandos y aplicación gráfica de TSM, se obtiene la identificación de la(s) cintas(s) necesarias para la ejecución exitosa de dicho proceso.

3.1.6. En resumen, el inventario de cintas de TSM se lo obtiene de dos fuentes: la base de datos de TSM y la bitácora de envió de respaldos a sitio alterno.

4. Responsabilidades
    - Administradores de bases de datos
        - Mantener las claves de acceso al servidor TSM y su ubicación física.
        - Definir la ubicación de la caja de seguridad en el subsuelo del edificio y su respectiva combinación (código de seguridad).
        - Custodia de la bitácora de envió de cintas a sitio externo.
        - Almacenamiento de cintas en la caja de seguridad y que se han llenado en el robot.
        - Envió de cintas a sitio alterno.

        - Recepción de cintas de sitio externo y almacenamiento de las mismas en la caja de seguridad del edificio Inverna.
    - Gerente de Operaciones
        - Autorizar cambios en las políticas de respaldos y recuperación implementadas en TSM.
        - Llevar registro y control acerca de cambio de políticas de respaldos, en claves de acceso en TSM y combinación de la caja fuerte.
    - Sitio alterno Ecuadasa Guayaquil
        - Ser custodio de las cintas que son enviadas desde el edificio Inverna.
        - Realizar el almacenamiento en la planta en la caja de seguridad de la misma.
    - Director de TI
        - Verificar el cumplimiento de este procedimiento.

5. Anexos

N/A

Elaborado por:	Revisado por:	Aprobado por:
Administrador de Base de datos	Supervisor Control Interno Gerente Auditor	Director Tecnología e Información

GLOSARIO

Activo

Es cualquier recurso o competencia. Los activos de un proveedor de servicio incluyen todo aquello que pueda contribuir a la prestación de un servicio. Los activos pueden ser de alguno de los siguientes tipos: gestión, organización, procesos, conocimientos, personas, información, aplicaciones, infraestructura o el capital financiero.

Acuerdo de niveles de servicio

Es un acuerdo entre el proveedor de servicios de TI y un cliente. Un acuerdo de niveles de servicio describe los servicios de TI, documenta los objetivos de nivel de servicio, y especifica las responsabilidades del proveedor de servicios de TI y el cliente. Un acuerdo único puede cubrir múltiples servicios de TI o varios clientes.

Amenaza

Una amenaza es cualquier cosa que podría aprovechar una vulnerabilidad. Cualquier causa potencial de un incidente puede ser considerada una amenaza. Por ejemplo, un incendio es una amenaza que podría aprovechar la vulnerabilidad por lo inflamable de los revestimientos del piso. Comúnmente, este término se utiliza en la gestión de seguridad de la información y la gestión de continuidad de los servicios de TI, pero también se aplica a otros ámbitos, como la gestión de disponibilidad y de problemas.

Análisis costo beneficio

Es una actividad que analiza y compara los costos y los beneficios involucrados en uno o más cursos de acción alternativos.

Análisis de Impacto al Negocio

(Business Impact Analysis) o Análisis de Impacto al Negocio es la actividad en la gestión de la continuidad del negocio que identifica las funciones vitales de negocios y sus dependencias. Estas dependencias pueden incluir a proveedores, personas, otros procesos del negocio, servicios de TI, etc. El análisis de impacto al negocio define los requisitos de recuperación de los servicios de TI. Estos requisitos incluyen tiempos de recuperación objetivos, puntos de recuperación objetivos y los objetivos mínimos de nivel de servicio para cada servicio de TI.

Cadena de valor

Es una secuencia de procesos que crean un producto o servicio que es de valor para un cliente. Cada paso en la secuencia se basa en los pasos anteriores y contribuye con el producto o servicio global.

Confidencialidad

Es un principio de seguridad que requiere que solo las personas autorizadas puedan tener acceso a los datos.

Disponibilidad

Es la habilidad de un servicio de TI u otro elemento de configuración para realizar la función acordada cuando sea requerido. La disponibilidad está determinada por la confiabilidad, capacidad de dar mantenimiento, capacidad de dar servicio, desempeño y seguridad. Generalmente la disponibilidad se calcula como un porcentaje. A menudo, este cálculo se basa en el tiempo de servicio acordado y el tiempo de inactividad. La mejor práctica para calcular la disponibilidad de un servicio de TI es utilizando las mediciones de los resultados de negocios.

Economía de escala

Es la reducción que se puede lograr en el costo promedio al aumentar el uso de un servicio o activo de TI.

Escalabilidad

Es la capacidad de un servicio de TI, procesos, elemento de configuración, etc., para llevar a cabo su función acordada cuando hay un cambio en la carga de trabajo o alcance.

Evento

Es un cambio de estado que tiene importancia para la gestión de servicios de TI u otro elemento de configuración. El término también se utiliza en el sentido de una alerta o notificación creada por cualquier servicio de TI, elemento de configuración o herramienta de monitoreo. Típicamente, los eventos requieren que el personal de operaciones de TI tome acciones, y a menudo conllevan a que se registren incidentes.

Externalización

Es el uso de un proveedor de servicios externos de TI para gestionar los servicios de TI.

Gestión de cambio

Es el proceso responsable de controlar el ciclo de vida de todos los cambios, permitiendo que se realicen cambios que son beneficiosos, minimizando la interrupción de servicios de TI.

Gestión de continuidad de servicios de TI

Es el proceso responsable de gestionar los riesgos que podría afectar seriamente los servicios de TI. La gestión de continuidad de servicios de TI garantiza que el proveedor de servicios de TI siempre puede entregar niveles mínimos de servicio que hayan sido acordados, al reducir los riesgos a un nivel aceptable y planifica para la recuperación de los servicios de TI. La gestión de continuidad de servicios de TI da soporte a la gestión de continuidad del negocio.

Gestión de riesgos

Incluye todas las actividades requeridas para identificar y controlar la exposición al riesgo, que pueden tener un impacto en el logro de los objetivos del negocio de una organización.

Infraestructura de TI

Es todo el hardware, software, redes, instalaciones, etc., que se necesitan para desarrollar, probar, entregar, monitorear, controlar o dar soporte a servicios de TI y a aplicaciones. El término incluye toda la tecnología de información, pero no a las personas, procesos y documentación asociadas.

Integridad

Es un principio de seguridad que garantiza que los datos y elementos de configuración solo puedan ser modificados por personas y actividades autorizadas. La integridad considera todas las posibles causas de modificación, incluyendo averías en el software y hardware, eventos ambientales, y la intervención humana.

ITIL

Es un conjunto de publicaciones de mejores prácticas para la gestión de servicios de TI. Es propiedad de la Oficina del Gabinete (parte del Gobierno de Su Majestad), ITIL proporciona guías de calidad para la prestación de servicios de TI y los procesos, las funciones y otras competencias necesarios para sustentarlas. El marco de trabajo ITIL se basa en el ciclo de vida de servicio y dicho ciclo consta de cinco etapas (estrategia del servicio, diseño del servicio, transición del servicio, operación del servicio y mejora continua del servicio), cada una de ellas tiene su propia publicación de apoyo. También hay una serie de publicaciones complementarias de ITIL que proporcionan orientación específica para sectores de la industria, tipos de organización, modelos operativos y arquitecturas de tecnología.

Negocio

Es una entidad corporativa u organización global formada por un número de unidades de negocio. En el contexto de ITSM, el término incluye al sector público y organizaciones sin fines de lucro, así como a compañías. Un proveedor de servicios de TI proporciona servicios de TI a un cliente dentro de un negocio. El proveedor de servicios de TI puede ser parte del mismo negocio que su cliente (proveedor de servicios internos), o parte de otro negocio (proveedor de servicios externos).

Plan de Continuidad de Negocio

(Business Continuity Plan) o Plan de Continuidad de Negocio es un plan que define los pasos necesarios para restaurar los procesos de negocio después de la ocurrencia de una interrupción. El plan también establece las condiciones que determinan los disparadores para la invocación, la gente a involucrar, comunicaciones, etc. los planes de continuidad del servicio de TI constituyen una parte importante de los planes de la continuidad del negocio.

Política

Son expectativas e intenciones de la gerencia, formalmente documentadas. Las políticas se utilizan para guiar las decisiones, y para asegurar el desarrollo e implementación consistente y apropiado de procesos, normas, roles, actividades, infraestructura de TI, etc.

Presupuesto

Es una lista de todo el dinero que una organización o unidad del negocio planea recibir y pagar, durante un período determinado de tiempo.

Proceso

Es un conjunto estructurado de actividades diseñadas para lograr un objetivo específico. Un proceso tiene una o más entradas definidas y las transforma en salidas definidas. Puede valerse de cualquier rol, responsabilidad, herramientas y controles de gestión que sean necesarios para entregar de forma confiable los resultados. Un proceso puede definir, si son necesarios, políticas, normas, directrices, actividades e instrucción de trabajo.

Proceso de negocio

Es un proceso que es propiedad y está siendo operado por el negocio. Un proceso de negocio contribuye a la entrega de un producto o servicio a un cliente del negocio. Por ejemplo, un minorista puede tener un proceso de compra que ayuda a prestar servicios a sus clientes del negocio. Muchos procesos de negocio dependen de los servicios de TI.

Punto objetivo de recuperación

(Recovery point objective) o punto objetivo de recuperación es la cantidad máxima de datos que se pueden perder cuando se restablece el servicio después de una interrupción. Los puntos de recuperación objetivo para cada servicio de TI deben ser negociados, acordados y documentados, y se utilizan como requisitos para el diseño de servicios de TI y los planes de continuidad del servicio.

Recuperación

Es devolver a un elemento de configuración o un servicio de TI a un estado de funcionamiento. A menudo, la recuperación de un servicio de TI incluye la recuperación de datos a un estado consistente conocido. Después de la recuperación, puede ser necesario ejecutar otros pasos antes de poner el servicio de TI a disposición de los usuarios (restauración).

Respaldo

Es una copia de los datos que sirve de protección en caso de pérdida de la integridad o la disponibilidad de los originales.

Riesgo

Es un posible evento que podría causar daños o pérdidas, o afectar la capacidad de alcanzar objetivos. Un riesgo se mide por la probabilidad de una amenaza, la vulnerabilidad de los activos a esa amenaza, y el impacto que tendría si ocurre. El riesgo también puede ser definido como la incertidumbre en el resultado, y puede ser utilizado en el contexto de la medición de la probabilidad de resultados positivos, así como de resultados negativos.

Servicio

Es un medio de entregar valor a los clientes, al facilitar los resultados que los clientes quieren lograr sin apropiarse de los costos y riesgos específicos. A veces se utiliza el término ‘Servicio’ como sinónimo de servicio base, servicio de TI o paquete de servicios. Véase también utilidad; garantía.

Servicio de TI

Es un servicio proporcionado por un proveedor de servicios de TI. Un servicio de TI se compone de una combinación de tecnología de información, personas y procesos. Los servicios de TI de cara-al-cliente dan soporte directo a los procesos del negocio de uno o más clientes y sus objetivos de niveles de servicio deben definirse en un acuerdo de nivel de servicio. Otros servicios de TI, llamados servicios de soporte, no son utilizados directamente por el negocio, pero el proveedor de servicios los requiere para entregar los servicios de cara-al-cliente. Véase también servicio base, servicio habilitante, servicio suplementario; servicio; paquete de servicios.

Tiempo objetivo de recuperación

(Recovery time objective) o tiempo objetivo de recuperación es el tiempo máximo permitido para la recuperación de un servicio de TI después de una interrupción. El nivel de servicio que debe prestarse podrá ser inferior al objetivo de nivel de servicio normal. Los tiempos de recuperación objetivo para cada servicio de TI deben ser negociados, acordados y documentados.

Umbral

Es el valor de una métrica que podría causar que se genere una alerta o se tome una acción de gestión.

Valor presente neto

Es una técnica utilizada para ayudar a tomar decisiones sobre los gastos de capital. Se comparan las entradas de efectivo con las salidas de efectivo. Un valor presente neto positivo indica que la inversión vale la pena.

Vulnerabilidad

Es una debilidad que podría ser aprovechada por una amenaza.