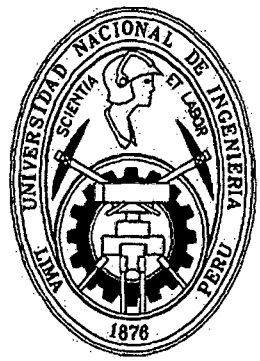
UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS

Sección de Posgrado



"METODOLOGÍA BASADA EN UN ENFOQUE SOA, DE UN PLAN DE RECUPERACIÓN DE DESASTRES PARA UNA PLATAFORMA DE INTEROPERABILIDAD"

TESIS

PARA OPTAR EL GRADO ACADÉMICO DE MAESTRO EN CIENCIAS CON MENCIÓN EN INGENIERÍA DE SISTEMAS

ELABORADO POR EL

ING. CARLOS ALFREDO TRIGO PÉREZ

ASESOR

MAG. JOSUE ANGULO PÉREZ

LIMA – PERÚ

2012

ÍNDICE

DEDICATORIA

A MIS PADRES: IRMA Y ALFREDO

EJEMPLO DE LUCHA Y SACRIFICIO

POR EL BIEN DE SUS HIJOS

A MIS HIJOS CARLOS Y LORENA.

A MI ESPOSA ANA CARMEN POR SU

COMPRENSIÓN

RESUMEN

El trabajo de investigación consiste en desarrollar una Metodología basada en un enfoque SOA (arquitectura orientada a servicios) para la implementación del Plan de Recuperación de Desastres aplicada a una Plataforma de Interoperabilidad en cuya configuración se encuentran dos Data Centers o Centros de Datos uno como principal y el otro de contingencia con software SOA y componentes de alta disponibilidad.

Para este estudio se va a tomar como muestra un grupo empresarial donde se está aplicando esta tecnología de información, para poder desarrollar una metodología, basada en el enfoque SOA, para el Plan de Recuperación de Desastres (PRD) o Disaster Recovery Planning (DRP), la que va estar compuesta de una serie de procedimientos que van a generar productos parciales que al final servirán de fundamento para el Plan propiamente dicho.

Adicionalmente, se tiene el propósito de demostrar esta investigación, manipulando la variable independiente: **Metodología basada en un enfoque SOA, del Plan de Recuperación de Desastres (PRD)** y verificando su incidencia en la variable dependiente: **Servicio de la Plataforma de Interoperabilidad**, además mediante la formulación de indicadores e índices, dichas variables podrán ser medidas y demostrarse en el análisis de los resultados, el valor agregado que brinda esta metodología en el desarrollo del PRD para esta plataforma de interoperabilidad.

ABSTRACT

The disaster recovery plans have increased their dominance, after 11 September 2001, in which thousands of international organizations based in the Twin Towers were forced to put in test plans, most of which failed with different impacts ranging from their disappearance to the affectation in their operation, with recovery periods that took months and years, in some cases, to reach the same level of operation they had before the disaster.

Large business groups in the first decade of the XXI century have been looking greater flexibility in their IT services through the called "Service Oriented Architecture" (SOA), which has given them, in general:

• Greater interoperability between existing applications, external and future applications

• Agility in business processes that enable faster time implementation of required changes in the business processes of the company.

• Lower maintenance costs to ensure the business capabilities (software components) are consolidated in a small amount of shared services.

Service-oriented architectures (SOAs), based on Web service standards, have emerged as the leading industry wide enabler for interoperability with mechanisms to exchange processes and / or data between heterogeneous systems. In the web environment, interoperability is a necessary condition to have full access to the information available. Companies that are embracing SOAs are finding huge benefits, but could be lost if we don´t have an effective Disaster Recovery Plan, based on SOA`s approach.

This research is for business groups using SOA, that have an Interoperability Platform with high availability hardware and software in two data centers, (principal and contingency one) but that need a framework in order to use for developing a Disaster Recovery Plan. The methodology, as a result of this investigation has 4 proposal steps for developing the plan and includes the maintenance of this plan for any changes in the Platform.

With this DRP based on SOA`s approach, Business groups, after a disaster, can have their contingency´s data center operative in minutes, as well as, once recovered its main data center, return its operations in less than an hour.

INTRODUCCIÓN

Hablar hoy de "Seguridad de información" es partir de la historia de la Seguridad de las Computadoras, aquellas conocidas como Mainframes. Esta historia se inicia gracias a los grupos de científicos que desarrollaron la computación para romper los códigos durante la Segunda Guerra Mundial, ellos fueron los que crearon los primeros computadores modernos.

En aquella época la necesidad principal estribaba en asegurar al Mainframe de cualquier amenaza externa, es decir la seguridad física del hardware. Al poco tiempo la necesidad se amplió en asegurar la integridad de sus datos contra espionaje y sabotaje.

A fines de los años 60´s apareció ARPANET (lo que hoy es INTERNET), como un programa para desarrollar Redes y compartir recursos, incluyéndose la seguridad de los accesos remotos y la vulnerabilidad de las contraseñas. Todo esto nos llevó a la denominada seguridad de las redes.

Por otro lado, a diferencia de la seguridad de las computadoras, en aquella época, la seguridad de la información solo consideraba esquemas de clasificación de documentos, pero sin ayuda de las computadoras, es decir no existían proyectos para tal fin.

Durante los años 80´s siguió la evolución hasta transformarse en seguridad de la Información. Ya en los 90´s con el impulso de la INTERNET se vive lo que es la red global de las redes, al alcance del público en general, es decir desde cualquier computador, sin embargo, dentro de estos estándares de facto para la interconexión no se consideró la seguridad de la información como un factor crítico o nunca fue de

información lo hagan sin interferencia u obstrucción por eventos denominados Desastres. Obtener una mejorada disponibilidad, traducida en el mínimo tiempo sin servicio se puede lograr como lo demostraremos en los siguientes capítulos, a través de una Metodología basada en un enfoque SOA, de un Plan de Recuperación de Desastres para una Plataforma de Interoperabilidad.

primera prioridad, de ahí por ejemplo el origen de los problemas con el correo electrónico.

Ya en el siglo 21. La INTERNET ha traído consigo la comunicación entre millones de redes de computadoras inseguras. La seguridad de la información almacenada en dichas computadoras está influenciada por la seguridad en cada uno de los otros equipos de cómputo con los que están conectados.

Es así que podemos darnos cuenta, a través de la historia de la seguridad de la información, que el concepto de la seguridad de la computadora no es mas el principal objetivo para asegurar los sistemas de cómputo. La Seguridad de la computadora ha evolucionado hacia componentes complejos y de entornos con múltiples facetas, los que hoy se definen como Seguridad de la Información[1].

Seguridad de la Información es la protección de la información y de los sistemas y hardware que usan, almacenan y transmiten dicha información. Para proteger la información y sus sistemas relacionados de diversos peligros, es necesario que la Alta Dirección de las empresas fije políticas de seguridad, así como programas de concientización, entrenamiento y educación para el personal, complementado con tecnología de seguridad de información.

Dentro de los modelos de Seguridad de la Información destaca el denominado triángulo de la seguridad **CID** (Confidencialidad, Integridad y Disponibilidad), desarrollado por la industria de la seguridad informática, la cual describe tres características de la utilidad de la información: Confidencialidad, Integridad y Disponibilidad. La seguridad de la información ha ampliado este modelo con otros conceptos como Precisión, Autenticidad, etc.

En el presente trabajo nos concentramos, dado el ambiente en el cual hoy los grupos empresariales y gobiernos buscan interoperar bajo el enfoque SOA, exclusivamente en la característica denominada Disponibilidad, es decir permitir que los usuarios que necesitan acceder a diversos servicios de intercambio de

[1] M. Whitman and Herbert Mattord, (2003). Principles of Information Security, Course Technology.

CAPÍTULO I

PROTOCOLO DE LA INVESTIGACIÓN

El crecimiento económico ha implicado un reto para los centros de datos de las organizaciones, es así que empresas de gran envergadura propician la creación de otras entidades con especializaciones que fortalecen a la empresa inicial multiplicando los negocios de dicha corporación o grupo empresarial. Esto trae consigo que la información también vaya incrementándose y por lo tanto se hace necesario contar con una plataforma tecnológica que utilice, transfiera e intercambie la información requerida para los servicios ofrecidos.

Para ello se necesita contar con un Data Center Principal y otro de Contingencia para fortalecer la continuidad de los servicios bajo la modalidad tecnológica de Service Oriented Architecture (SOA) en una Plataforma de Interoperabilidad muy particular y que como tal existen muy pocas en nuestro medio. Es por esta razón que se consideró implementar un Plan de Recuperación de Desastres (PRD) o Disaster Recovery Planning (DRP) que normalmente se aplica a un Centro de Cómputo convencional sin las características especiales de alta disponibilidad e intercambio de servicios de información bajo enfoque SOA que exige una Plataforma de Interoperabilidad.

El presente trabajo de investigación consistirá en adecuar y alinear, desarrollando nuevas técnicas para la construcción del Plan de Recuperación de Desastres, bajo el enfoque SOA para una Plataforma de Interoperabilidad, tomando como muestra un grupo empresarial que utiliza este tipo de plataforma tecnológica.

1.1. EL PROBLEMA A INVESTIGAR

1.1.1. ANTECEDENTES DEL PROBLEMA

Durante la evolución de la Tecnología de la Información, en sus inicios, la infraestructura utilizada en la décadas de los 60, 70 y 80 era una configuración centralizada en los grandes mainframes que procesaban la información con un sistema de seguridad que era suficiente para proteger la información que requerían las empresas, la elaboración del plan de contingencias daba sus primeros pasos para posteriormente tener mayor importancia en las décadas de los 90 y 2000 desarrollándose el sistema distribuido en red que hizo mas funcional esta plataforma pero con altos riesgos de seguridad. Sin embargo, el Plan de Contingencias cubría, en forma general escenarios de interrupción de los servicios de sistemas, con procedimientos muy limitados, no estando debidamente preparados para situaciones extremas hoy catalogadas como Desastres[2]. Mas aun considerando que en la actualidad las empresas cuentan con las denominadas "aplicaciones críticas de negocio", los planes de contingencia sin un componente de Recuperación de Desastres, se vuelven inefectivos para esta realidad.

Por otra parte, en la actualidad han surgido diversas topologías y una de las más interesantes es la Plataforma de Interoperabilidad (PI) complementada con la Arquitectura orientada a Servicios o Service Oriented Architecture (SOA) generando un Hub que administra un complejo Data Center con una granja de servidores y considerando un Data Center alternativo, siendo éste último de contingencia, considerando componentes redundantes que aseguran la alta disponibilidad de su servicio.

Esta es la configuración en estudio y que mediante una metodología basada en un enfoque SOA[3], que se va a elaborar, se generará uno de

[2] Neaga, Gregor; Winters, Bruce; Laufman Pat (1998) S.O.S. en su Sistema de Computación. Prentice Hall Hispanoamérica, S.A.

[3] Erl, Thomas (2005) Service-Oriented Architecture. Concepts, Technology and Design. Pearson Education

los planes de contingencia más importantes: el Plan de Recuperación de Desastres (PRD) o Disaster Recovery Planning (DRP), objeto de este estudio de investigación.

El no contar con dicho Plan, en esta clase de tecnología, significa maximizar el riesgo de perder la información y la infraestructura que la soporta al optar por una alternativa equivocada o simplemente no poder tomar acción ante un desastre de esta magnitud.

Por lo tanto este trabajo de investigación para desarrollar el PRD para la PI orientada a SOA tendrá un beneficio importante al contar con un procedimiento efectivo en la mitigación de un siniestro de esta naturaleza.

1.1.2. FORMULACIÓN DEL PROBLEMA

Para plantear el problema se mencionará como se va a desarrollar el trabajo de investigación y mediante que recursos de las área de conocimiento comprometidas en el estudio

Con el propósito de cumplir con el objetivo de la investigación, formularemos un problema principal y tres problemas secundarios.

1.1.2.1. PROBLEMA PRINCIPAL

¿En qué medida una metodología basada en un enfoque SOA, que desarrolle el Plan de Recuperación de Desastres (PRD), mejora la disponibilidad del servicio de la Plataforma de Interoperabilidad (PI) en un Grupo Empresarial?

1.1.2.2. PROBLEMAS SECUNDARIOS

1.- ¿De qué manera el Análisis de Riesgos e Impacto de TI determina las vulnerabilidades, niveles de ocurrencia e impacto en la PI?

2.- ¿De qué forma el Plan de Crisis minimiza el proceso de recuperación de desastres en la Plataforma de Interoperabilidad?

3.- ¿En qué medida el Plan de Recuperación de desastres asegura la continuidad del servicio de la PI.?

1.2. OBJETIVOS

Los objetivos están delimitados al desarrollo de una metodología basada en un enfoque SOA, para la implementación de un PRD para un Grupo Empresarial que utilice una Plataforma de Interoperabilidad con un Data Center Principal (DCP) y otro Data Center de Contingencia (DCC).

1.2.1. OBJETIVO GENERAL

Cuantificar el nivel de mejora generado por la aplicación de la metodología basada en un enfoque SOA, del PRD a una PI.

1.2.2. OBJETIVOS ESPECÍFICOS

1.- Determinar las vulnerabilidades, niveles de ocurrencia e impacto mediante el Análisis de Riesgos y de Impacto de TI en la PI.

2.- Minimizar el proceso de recuperación de desastres por medio del Plan de Crisis en la PI.

3.- Asegurar la continuidad de los servicios de la PI mediante el Plan de Recuperación de desastres.

1.3. JUSTIFICACIÓN O IMPORTANCIA

Esta Investigación justifica su realización, ya que asegurará la continuidad de las operaciones de la PI en entidades que utilicen esta tecnología, brindando alta disponibilidad y confiabilidad de la información que se transfiere, utiliza e intercambia en esta plataforma. La interrupción de las operaciones en la PI debido a no tener un PRD debidamente desarrollado, puede ocasionar pérdidas económicas en la producción del grupo empresarial LAGOS S.A. que pueden ser irrecuperables.

La omisión del PRD puede ocasionar pérdidas económicas por inoperatividad del negocio por días, semanas, las que también podrían

repercutir en la pérdida definitiva de proveedores, clientes y por ende de negocios futuros, si se excede el tiempo de tolerancia máxima de inactividad por falla de la PI. En el caso del grupo empresarial, han estimado que sus pérdidas por inoperatividad llegarían a los US $ 240,000 diarios, sin considerar los demás aspectos mencionados.

1.4. HIPÓTESIS Y VARIABLES

1.4.1. HIPÓTESIS GENERAL

Si se desarrolla una metodología basada en un enfoque SOA, para el Plan de Recuperación de Desastres para la Plataforma de Interoperabilidad, entonces mejorará la disponibilidad del servicio de transferencia, utilización e intercambio de información en el Grupo Empresarial.

1.4.2. HIPÓTESIS ESPECÍFICAS

- Si se aplica el Análisis de Riesgo y de Impacto de TI entonces se determinarán las vulnerabilidades, niveles de ocurrencia e impacto a la PI.
- Si se implementa el Plan de Crisis entonces se minimizará el proceso de recuperación de desastres en la PI.
- Si se desarrolla el Plan de Recuperación de desastres se asegurará la continuidad del servicio de información en la PI.

1.4.3. IDENTIFICACIÓN DE VARIABLES, INDICADORES E INDICES

A continuación se identificará cada una de las variables, además se indicará su operacionalización y los posibles indicadores que deban aplicarse.

1.4.3.1. VARIABLE INDEPENDIENTE X:

Metodología basada en un enfoque SOA, del Plan de Recuperación de Desastres (PRD) se determina mediante una metodología que implica el Análisis de Riesgo y el Análisis de

Impacto de TI, realizando un tratamiento de los riesgos para desarrollar los Planes de Crisis, Contingencia y Recuperación.

Se estudia a partir del siguiente indicador:

Indicador X_1

Nivel de cumplimiento de pruebas del PRD

Es un indicador que demuestra la efectividad del PRD según el porcentaje de pruebas exitosas que debe estar entre el 70% y 100% según juicio experto

Índices:

$X_{1.1}$: Nro. de pruebas exitosas de Contexto / Nro. de pruebas totales de Contexto.

Las Pruebas de contexto consisten en la realización de actividades con los empleados que les permitan estar en contacto permanente con la recuperación del servicio evitando los contactos erróneos.

Son pruebas que Notifican una Emergencia, brindando un método seguro y de bajo costo, para detectar omisiones generales, causadas por cambios en el personal designado en los Equipos de Recuperación. Consiste en verificar que la información de las Listas de Llamada esté vigente, estableciendo contactos verificados tanto dentro como fuera de la organización.

Métricas → Contactos verificados por prueba (* los cuales pueden ser exitosos o no)

*No debe existir ningún contacto verificado erróneo de lo contrario la prueba de Contexto no es exitosa

$X_{1.2}$: Nro. de pruebas exitosas de Organización / Nro. de pruebas totales de Organización.

Esta prueba se focaliza en verificar la integridad y veracidad de las actividades y tareas asignadas a los Equipos de Recuperación de la Organización, a la vez que brinda una oportunidad para entrenar a sus integrantes, sin tener que interrumpir las operaciones o incurrir en gastos de traslado al Data Center de Contingencia.

El objetivo principal de esta modalidad de prueba es asegurar que el Plan ha definido todas las funciones y sus responsabilidades, y que se ha incluido toda la documentación de soporte. También puede ser utilizado para identificar el hardware, el software de base o las aplicaciones que pudieran haber sufrido cambios últimamente.

Métricas → Actividades verificadas por prueba (** las cuales pueden ser exitosas o no)

**No debe existir ninguna actividad verificada errónea de lo contrario la prueba de Organización no es exitosa

$X_{1.3}$: Nro. de pruebas exitosas de Operación / Nro. de pruebas totales de Operación.

Una Prueba de Operación es un ejercicio planificado que incluye la habilitación de los sistemas, subsistemas y aplicaciones de la PI, mediante el traslado de recursos humanos y tecnológicos de Contingencia, en el cual se ejecutarán los procedimientos de recuperación contenidos en este Plan.

El objetivo principal de este tipo de pruebas es asegurar que la plataforma de recuperación y los enlaces de comunicaciones requeridos para restablecer las aplicaciones críticas estén disponibles, y que el personal está entrenado en la ejecución de los procedimientos documentados en este Plan.

También sirve para verificar que la infraestructura comprometida está totalmente operativa para aplicar los procedimientos de la prueba de Operación.

Esta categoría de pruebas podría tener un alcance parcial (por ejemplo, validación de los procedimientos técnicos de recuperación) o total, al incluir a la totalidad de los componentes del Plan, pero en nuestro caso para ser más exigentes, se ha determinado un alcance total.

Para la medición existen parámetros cada uno de los cuales tienen condiciones que deben de cumplirse totalmente para que las pruebas sean exitosas. Los parámetros con sus respectivas condiciones son las siguientes:

- Parámetro: Alcance de la Prueba.
  Cuyas condiciones son la consideración de:
  - Participantes
  - Notificación
  - Infraestructura
  - Aplicaciones
- Parámetro: Definición de Objetivos de la Prueba.
  Siendo sus condiciones:
  - Objetivos y resultados esperados
  - Límite de tiempo
- Parámetro: Medición de la Prueba.
  Cuyas condiciones son:
  - Registro de tiempo durante la prueba
  - Documentación del problema / desviación de la prueba
- Parámetro: Evaluación de la Prueba.
  Cuya condición es el:
  - Cumplimiento de Objetivos

Métricas → Parámetros verificados por prueba (*** los cuales pueden ser exitosos o no)

***No debe existir ningún parámetro verificado erróneo de lo contrario la prueba de Operación no es exitosa. Además para que el Parámetro verificado sea exitoso, se debe cumplir todas sus condiciones en forma correcta.

1.4.3.2. VARIABLE INDEPENDIENTE Y:

Servicio de la Plataforma de Interoperabilidad se determina mediante mediciones de alta disponibilidad y continuidad del servicio.

Se estudia a partir de los siguientes indicadores:

Indicador Y_1:

Continuidad del servicio

Este indicador va a expresar el tiempo de recuperación desde que ocurre el evento del desastre hasta que el servicio pueda operar razonablemente (todos los servidores transaccionales operativos), cabe precisar, levantando los dispositivos del servicio de TI que soportan los procesos principales del negocio.

Índice:

$Y_{1.1}$: Tiempo objetivo de recuperación (TOR) o RTO (Recovery Time Objective)

El TOR está compuesto por el Failover (Conmutación por falla), que es el tiempo de recuperación cuando el Data Center Principal (DCP) falla y tiene que operar el Data Center de Contingencia (DCC) operando razonablemente, teniendo luego que considerar un tiempo de ejecución de los servicios de emergencia (TESE), en el DCC apoyando la operatividad del negocio (Se asume que el TESE tiene el mismo valor con o sin el PRD), hasta que se da el Failback (Restauración por falla) que involucra el tiempo de restauración al transferir el rol del DCC al DCP y actualizando la información perdida

hasta que la totalidad de servicios sean recuperados en dicho Data Center.

Métrica → Minutos

Por lo tanto, en este caso el TOR no considerará el TESE (ya que este tiempo depende del tipo de evento o desastre que origina la interrupción) siendo finalmente la suma de los tiempos de estos dos procesos:

TOR = Tiempo de Failover + Tiempo de Failback

Indicador Y_2:

Disponibilidad del servicio

Índice:

$Y_{2.1}$: Punto objetivo de recuperación (POR) o RPO (Recovery Point Objective)

Se refiere a la magnitud de pérdida de datos que puede ser tolerado por un proceso que sea interrumpido.

Métrica → Datos perdidos

Indicador Y_3:

Riesgo de TI

Índices:

$Y_{3.1}$: Nivel de Impacto de las amenazas

Es la magnitud del daño causado a los procesos durante la ocurrencia de una amenaza o evento (Ejemplo: Inundaciones, terremoto, fuego, incendio, sabotaje, ataques terroristas, vandalismo, falla general en el sistema de energía, falla en la seguridad física, falta de personal para las operaciones y soporte de los servicios que brinda la PI.) que origine perjuicios de algún tipo y desencadene otras amenazas.

Se ha calificado en forma cualitativa en los siguientes niveles:

Grave, Severo, Moderado, Bajo y Muy Bajo

Métrica → Puntuación

$Y_{3.2}$: Nivel de ocurrencia de las amenazas

Es la probabilidad de que se presente la amenaza tabulando niveles de frecuencia que se dan a continuación:

Muy frecuente, Probable, Posible, Improbable y Raro

Métrica → Puntuación

$Y_{3.3}$: Nivel de vulnerabilidad de la PI

Siendo la debilidad que puede ser explotada por una amenaza, la que también se califica con los niveles siguientes:

Muy alto, Alto, Medio, Bajo

Métrica → Puntuación

1.4.4. OPERACIONALIZACIÓN DE VARIABLES

Variable Independiente X: Metodología basada en un enfoque SOA, del Plan de Recuperación de Desastres (PRD).- Esta metodología se

determina mediante una combinación de procedimientos que van desde el Análisis de Riesgos e Impacto de TI terminando con un Plan de Crisis y un Plan de Contingencias que sería el producto final del PRD.

Se mide mediante el Indicador Nivel de cumplimiento de las pruebas del PRD, siendo los índices relativos a las pruebas de contexto, organización y operación siendo los responsables de medir esta variable independiente, determinando su grado de incidencia en la variable dependiente.

Variable Dependiente Y: Servicio de la Plataforma de Interoperabilidad.- El servicio en mención debe calcularse mediante factores que incidan en la seguridad que son consecuencia de la aplicación del PRD, una forma es desarrollar el experimento con la presencia de la variable independiente y los efectos que ella causa y luego con la ausencia y comparar el efecto que esta metodología basada en el enfoque SOA, del PRD puede producir.

Esta variable dependiente es medida mediante indicadores de Continuidad de Servicio, Disponibilidad de Servicio y Riesgo de TI, determinando el impacto que tiene la variable independiente sobre ella.

La Matriz de Consistencia respectiva se encuentra en el ANEXO 4

1.5. ALCANCE DE LA TESIS

Esta Tesis está delimitada a Empresas Corporativas o Grupos Empresariales que deseen implementar una PI con una configuración de un Data Center Principal (DCP) y otro Data Center de Contingencia (DCC) bajo el enfoque SOA que les ayude a intercambiar información entre las entidades involucradas

CAPÍTULO II

MARCO TEÓRICO

2.1. MARCO CONCEPTUAL

2.1.1. PLATAFORMA DE INTEROPERABILIDAD Y SOA

La plataforma de interoperabilidad representa el resultado del esfuerzo de los grupos empresariales y los organismos multilaterales que les apoyan para desarrollar un conjunto de soluciones tecnológicas de alta disponibilidad y confiabilidad, de la información que se transfiere, utiliza e intercambia en esta plataforma entre las empresas de la corporación o grupo empresarial. De acuerdo con los determinantes básicos a ser tenidos en cuenta en la conceptualización de la arquitectura propuesta en este documento, la existencia de un solo componente central es inadecuada, razón por la cual, se define como fundamental para la plataforma de interoperabilidad la existencia de un conjunto de elementos tecnológicos que serán denominados, de forma genérica, como el enrutador transaccional, cuya labor principal es parte de la solución que se propone para optimizar la interoperabilidad entre las entidades.

El enrutador transaccional corresponde a una solución tecnológica suficientemente flexible para reflejar los acuerdos logrados en los espacios de diálogo (tipologías de gobernanza y organizacional) reflejando las diversas definiciones y estándares establecidos (tipología semántica); así mismo, implementa las diferentes decisiones que en materia tecnológica se establezcan como estándares (tipología técnica).

El objetivo del enrutador consiste en hacer óptima la relación entre agencias de diferentes empresas, pues son estas últimas las que cuentan con los sistemas de información y bases de datos desde donde se extrae la información a ser intercambiada en la interoperabilidad. Así mismo, son estas agencias las que reciben la información requerida en cada servicio de gobierno electrónico. No obstante, no se establece un único sistema centralizado, sino por el contrario el modelo plantea que se puede interactuar con un conjunto de enrutadores, que operan al interior de la corporación y enrutador que actúa como interface de la PI.

La Plataforma de Interoperabilidad (PI) forma parte de la Plataforma de Gobierno Electrónico y tiene como objetivo general facilitar y promover la implementación de servicios de Gobierno Electrónico. Para esto, la PI brinda mecanismos que apuntan a simplificar la integración entre entidades y a posibilitar un mejor aprovechamiento de sus activos.

La PI provee infraestructura (hardware y software) y servicios utilitarios, que reducen la complejidad de implementar servicios al usuario y/o accesibles dentro del Grupo Empresarial. Asimismo, la PI aporta los mecanismos técnicos idóneos para implementar servicios compuestos, basados en los ofrecidos por diferentes organismos, normalizando e integrando la información proveniente de éstos.

A nivel tecnológico, la PI posibilita que los organismos provean sus funcionalidades de negocio a través de servicios de software de forma independiente a la plataforma en la que fueron implementados. Esto corresponde a la implementación de una SOA a nivel de todo el Grupo Empresarial, en la cual los servicios ofrecidos por los organismos son descritos, publicados y descubiertos, invocados y combinados a través de interfaces y protocolos estandarizados.

De esta forma, al facilitarse la reutilización de servicios, se promueve la construcción de nuevos servicios en base a otros ya existentes, reduciéndose los tiempos de implementación de nuevos requerimientos. Por otro lado, el "acoplamiento débil" entre servicios promovido por la SOA,

permite la evolución autónoma de los servicios de software implementados en los organismos.

2.1.2. GRUPOS EMPRESARIALES

Grupo de empresas, **grupo empresarial**, **grupo industrial**, **conglomerado empresarial** o **conglomerado industrial** es, en derecho y economía, el conglomerado de empresas que dependen todas de una misma empresa matriz, porque ésta tiene una participación económica suficiente en su capital como para tomar las decisiones.

Si bien en derecho cada empresa es una persona jurídica diferente, en ocasiones se tienen en cuenta regulaciones especiales para los grupos de empresas para evitar fraudes a la ley, que provoquen perjuicios a terceros.

Específicamente *conglomerado* o **empresa multi-industria** suele referirse a la combinación de dos o más empresas que realizan negocios completamente diferentes. Los conglomerados suelen ser grandes y pueden ser formados por la fusión de más de tres empresas.

Concentración empresarial o **concentración industrial** es la agrupación de empresas a través de acuerdos, fusiones o la dependencia de participaciones accionariales a una empresa matriz (holding, trust, cártel, etc.), lo que disminuye o incluso elimina la libre competencia en un sector de la economía, produciendo alteraciones del mercado libre que se denominan situaciones de competencia imperfecta, oligopolio o incluso monopolio.

La concentración de empresas del mismo sector (o de la misma etapa de un proceso de producción) se denomina concentración horizontal; mientras que la de empresas de distintos sectores (vinculadas por ser clientes unas de otras) se denomina concentración vertical (la que intenta concentrar todas o la mayor parte de las fases de un mismo proceso productivo, lo que también se aplica a empresas de la misma industria pero que operan en

diferentes etapas del proceso de producción). Las concentraciones, al superar los efectos negativos del denominado minifundismo empresarial, suelen generar sinergias y economías de escala; aunque, en algunos casos, sobrepasar ciertos límites de dimensiones o complejidad organizativa produce efectos disfuncionales (des economías de escala).

Por otro lado, el grupo empresarial es el conjunto de una o más sociedades independientes jurídicamente entre sí, pero que se encuentran bajo un control o subordinación ejercido por una matriz o controlante y sometidas a una dirección unitaria que determina los lineamientos de cada una de ellas. Conformándose el grupo empresarial únicamente cuando concurran los dos elementos de su esencia; 1. El control o subordinación y 2. La unidad de propósito y dirección; sin que signifique esto, que se esté dando nacimiento a un nuevo ente autónomo e independiente, pues se mantiene intacta la personalidad jurídica de cada una de las sociedades vinculadas al grupo[4].

2.1.3. SEGURIDAD EN EL CENTRO DE PROCESAMIENTO DE DATOS Y EL PLAN DE RECUPERACION DE DESASTRES

Centro de Procesamiento de datos o Data Center (CPD):

Definición: Se denomina como CPD al lugar (edificio, oficina, site, etc.) donde se concentra todos los recursos necesarios para el procesamiento, explotación o almacenaje de la información de una organización.

Necesidad: Se crean y se mantienen debido a la necesidad que tienen las medianas y grandes empresas esto para poder tener la información necesaria para sus operaciones en un mismo lugar.

Factores de Creación de CPD:

• Garantizar la continuidad del servicio (clientes, empleados, ciudadanos, proveedores y empresas colaboradoras).

• Protección física de los equipos electrónicos (informáticos).

• Almacenar datos de información crítica.

[4] Concepción Muñoz Delgado *Geografía*, Anaya.

Funciones del CPD:

• Tratar los Datos (compilar, almacenar, y proteger los datos de una compañía).

• Ofrecer Servicios (Hosting, Intranet, telecomunicaciones, CMBD, bases de datos).

Como se mencionó, respecto a la Seguridad en el CPD, uno debe desplegar una serie de medidas para minimizar los diversos riesgos a los cuales está expuesto, sin embargo, a pesar de todo, el CPD no está exento de una falla en la seguridad que podría detener las operaciones de la organización, afectando sobretodo la imagen de la empresa. Por lo tanto, ante esta posibilidad debe de desarrollar un Plan de Recuperación de Desastres.

Anteriormente sólo los sistemas de nómina, contabilidad, almacén, etc., estaban soportados y algunas empresas no sufrían un gran impacto si tenían interrupciones prolongadas de servicio (más de 4 días). Una recaptura de los datos solucionaba los problemas, sólo era cuestión de tiempo.

Sin embargo, las organizaciones en la actualidad dependen cada vez más de sus servicios de información ya que han buscado mejorar su servicio al ciudadano y hacer eficientes sus operaciones. Un desastre en sus oficinas evitaría la continuidad del negocio.

El gobierno electrónico es el mandatario para que toda organización tenga planes de recuperación en casos de desastres, para evitar que un evento de ese tipo afecte los resultados financieros.

Las instituciones que ofrezcan servicios usando Internet no se pueden dar el lujo de dejar de proporcionar los servicios debido a las fallas en su centro de cómputo.

Un ejemplo muy claro es el área de protección civil, donde los servicios de información a la población durante un fenómeno meteorológico son tan importantes que en caso de fallas podrían significar hasta pérdidas de vidas.

Otro ejemplo es el abastecimiento de medicinas. En caso de que una

institución de seguridad social no tuviera la disponibilidad de reportar por medio de los servicios de cómputo conectados a las grandes empresas farmacéuticas, la escasez de algunas medicinas, sería crítica para la atención de los pacientes.

No olvidemos de las empresas que dependen del gobierno para proporcionar servicios de energía eléctrica o de abastecimiento de petróleo. En estos casos, los servicios de cómputo y telecomunicaciones son críticos y deben estar disponibles las 24 horas del día, los 7 días de la semana, durante los 365 días del año.

¿Qué es un desastre?

Podríamos definir un desastre como la pérdida total o parcial de la información crítica para la institución, durante un período considerable de tiempo, durante el cual la organización puede verse seriamente afectada en su operación y en su imagen de servicio.

Esto se traduciría en alguna de las siguientes situaciones:

• Imposibilidad de producir bienes o servicios

• No poder vender

• Imposibilidad de cobrar impuestos

• Incremento de cartera vencida

• Información crítica no disponible para toma de decisiones

• Incumplimiento de compromisos (legales, con clientes, con proveedores, sindicatos, etc.)

• Impacto negativo en el precio de la acción

• Pérdida de imagen y votos ante la ciudadanía

Los desastres sí ocurren

Aunque la posibilidad de que ocurra un desastre es menor, siempre existe y un administrador profesional y honesto no podrá negar que existe posibilidad

de que suceda en cualquier momento, por ello debemos estar preparados para que el impacto sea mínimo.

A continuación los desastres más populares que nos recuerdan que la realidad puede ser diferente.

- Torres Gemelas de Nueva York, EUA 2001; terrorismo
- Ataques por Internet a Hotmail 2000; negación de servicios
- Deslaves en Venezuela 2000; meteorológico
- Bomba en el World Trade Center de Nueva York, EUA 1993; terrorismo
- Incendio en edificio del Banco Confía en Monterrey, México. 1987; negligencia
- Huracán Gilberto en Monterrey, México 1988: meteorológico
- Terremoto en la Cd. de México 1985; geológico

Algunos datos estadísticos

- El 30 por ciento de las empresas de Estados Unidos que tuvieron un desastre en sus oficinas corporativas (Head Quarters), se declararon en quiebra durante los siguientes 3 años (Computer Security Institute,)
- En algunos lugares existen reglamentos legales que obligan a los dueños de empresas a apoyar el desarrollo de un plan de recuperación en caso de desastres, sin embargo en la mayoría de los casos no ocurre así, por lo que es difícil justificar el proyecto, ya que la mentalidad de la mayoría de la gente hace que se piense que no pasará nada.
- Sin embargo en algunos casos empresas aseguradoras o bancos requieren saber y auditar los planes de recuperación de desastre con el propósito de evaluar el riesgo de la empresa, así como la probabilidad de que se siga operando en caso de desastres.

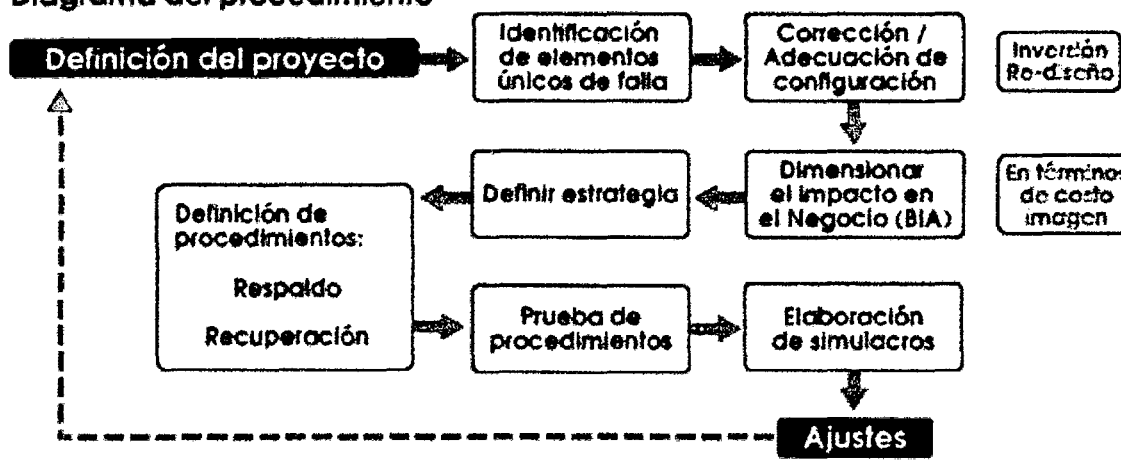
Proceso de planeación de la recuperación en caso de desastre

- El objetivo del proceso de planeación de la recuperación en caso de desastre es disminuir el impacto de un desastre en las operaciones de la institución.
- En ocasiones no es posible evitar un desastre natural, sin embargo sí podemos disminuir su impacto y definir las actividades de recuperación que permitan reanudar las actividades normales en el tiempo más corto

posible.

- Es mejor tener un procedimiento preestablecido que improvisar en caso de un desastre porque cuando se actúa bajo presión se cometen más errores. En la siguiente figura mostramos un diagrama del procedimiento que puede establecerse:

Diagrama del procedimiento



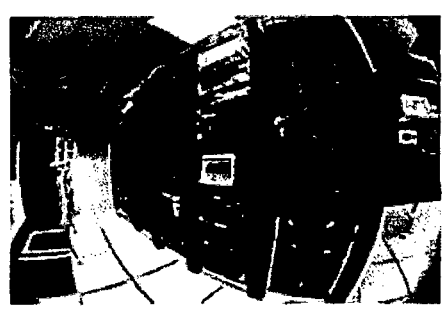
Fuente: BCP The Need and Approach, by Carl Jackson; BCP Testing Strategies, By Carl Jackson.

2.2. MARCO DE TECNOLOGÍAS BÁSICAS

2.2.1. TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

HARDWARE

Centro de procesamiento de datos[5]



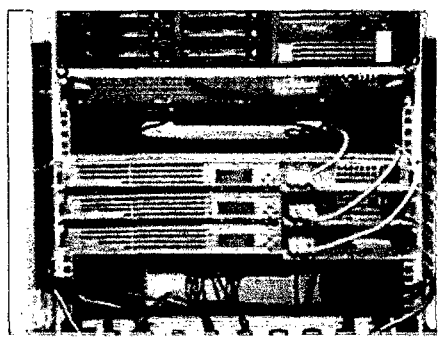
[5] WIKIPEDIA, La enciclopedia libre. [en línea].

Equipamiento de comunicaciones en un CPD.

Se denomina **centro de procesamiento de datos** (CPD) a aquella ubicación donde se concentran los recursos necesarios para el procesamiento de la información de una organización. También se conoce como *centro de cómputo* en Latinoamérica, o *centro de cálculo* en España o **centro de datos** por su equivalente en inglés *data center*.

Dichos recursos consisten esencialmente en unos ambientes debidamente acondicionados, computadoras y redes de comunicaciones.

Ubicación



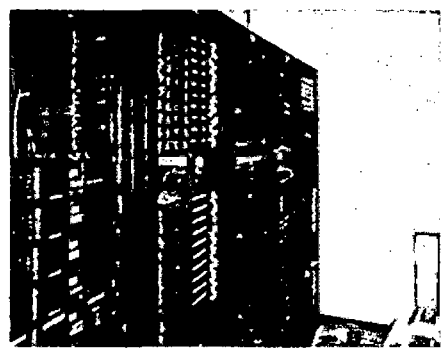
Servidores *enrackados*

Un CPD es un edificio o sala de gran tamaño usada para mantener en él una gran cantidad de equipamiento electrónico. Suelen ser creados y mantenidos por grandes organizaciones con objeto de tener acceso a la información necesaria para sus operaciones. Por ejemplo, un banco puede tener un data center con el propósito de almacenar todos los datos de sus clientes y las operaciones que estos realizan sobre sus cuentas. Prácticamente todas las compañías que son medianas o grandes tienen algún tipo de CPD, mientras que las más grandes llegan a tener varios.

Entre los factores más importantes que motivan la creación de un CPD se puede destacar el garantizar la continuidad del servicio a clientes, empleados, ciudadanos, proveedores y empresas colaboradoras, pues en estos ámbitos

es muy importante la protección física de los equipos informáticos o de comunicaciones implicados, así como servidores de bases de datos que puedan contener información crítica.

Diseño



Servidores

El diseño de un centro de procesamiento de datos comienza por la elección de su ubicación geográfica, y requiere un equilibrio entre diversos factores:

- Coste económico: coste del terreno, impuestos municipales, seguros, etc.
- Infraestructuras disponibles en las cercanías: energía eléctrica, carreteras, acometidas de electricidad, centralitas de telecomunicaciones, bomberos, etc.
- Riesgo: posibilidad de inundaciones, incendios, robos, terremotos, etc.

Una vez seleccionada la ubicación geográfica es necesario encontrar unas dependencias adecuadas para su finalidad, ya se trate de un local de nueva construcción u otro ya existente a comprar o alquilar. Algunos requisitos de las dependencias son:

- Doble acometida eléctrica.
- Muelle de carga y descarga.
- Montacargas y puertas anchas.
- Altura suficiente de las plantas.

- Medidas de seguridad en caso de incendio o inundación: drenajes, extintores, vías de evacuación, puertas ignífugas, etc.
- Aire acondicionado, teniendo en cuenta que se usará para la refrigeración de equipamiento informático.
- Almacenes.
- Orientación respecto al sol (si da al exterior).
- Etc.

Aún cuando se disponga del local adecuado, siempre es necesario algún despliegue de infraestructuras en su interior:

- Falsos pisos y falsos techos.
- Cableado de red y teléfono.
- Doble cableado eléctrico.
- Generadores y cuadros de distribución eléctrica.
- Acondicionamiento de salas.
- Instalación de alarmas, control de temperatura y humedad con avisos SNMP o SMTP.
- Facilidad de acceso (pues hay que meter en él aires acondicionados pesados, muebles de servidores grandes, etc.).
- Etc.

Una parte especialmente importante de estas infraestructuras son aquellas destinadas a la seguridad física de la instalación, lo que incluye:

- Cerraduras electromagnéticas.
- Torniquetes.
- Cámaras de seguridad.
- Detectores de movimiento.
- Tarjetas de identificación.
- Etc.

Una vez acondicionado el habitáculo se procede a la instalación de las computadoras, las redes de área local, etc. Esta tarea requiere un diseño

lógico de redes y entornos, sobre todo en áreas a la seguridad. Algunas actuaciones son:

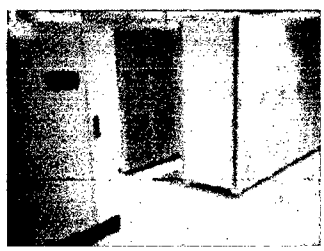
- Creación de zonas desmilitarizadas (DMZ).
- Segmentación de redes locales y creación de redes virtuales (VLAN).
- Despliegue y configuración de la electrónica de red: pasarelas, ruteadores, conmutadores, etc.
- Creación de los entornos de explotación, pre-explotación, desarrollo de aplicaciones y gestión en red.
- Creación de la red de almacenamiento.
- Instalación y configuración de los servidores y periféricos.
- Etc.

Site

Generalmente, todos los grandes servidores se suelen concentrar en una sala denominada "sala fría", "nevera", "pecera" (o *site*). Esta sala requiere un sistema específico de refrigeración para mantener una temperatura baja (entre 21 y 23 grados centígrados*), necesaria para evitar averías en las computadoras a causa del sobrecalentamiento.

- Según las normas internacionales la temperatura exacta debe ser 22,3 grados centígrados.

La "pecera" suele contar con medidas estrictas de seguridad en el acceso físico, así como medidas de extinción de incendios adecuadas al material eléctrico, tales como extinción por agua nebulizada o bien por gas INERGEN, dióxido de carbono o nitrógeno, aunque una solución en auge actualmente es usar sistemas de extinción por medio de agentes gaseosos, como por ejemplo Novec 1230.



Pecera de un CPD.

Consumo

El consumo de un CPD es elevado, por ello se están desarrollando iniciativas para controlar su consumo, como la EU Code of Conduct for Data Centres o uso de recursos naturales limpios para refrigerar

SOFTWARE

Se conoce como *software*[6] *al equipamiento lógico o soporte lógico* de un sistema informático, comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas, en contraposición a los componentes físicos, que son llamados hardware.

componentes Los lógicos incluyen, entre muchos otros, las aplicaciones informáticas; tales como el procesador de texto, que permite al usuario realizar todas las tareas concernientes a la edición de textos; el software de sistema, tal como el sistema operativo, que, básicamente, permite al resto de los programas funcionar adecuadamente, facilitando también la interacción entre los componentes físicos y el resto de las aplicaciones, y proporcionando una interfaz con el usuario.

El anglicismo "software" es el más ampliamente difundido, especialmente en la jerga técnica, el término sinónimo *"logical"*, derivado del término francés *"logiciel"*, es utilizado en países y zonas de habla francesa.

Existen varias definiciones similares aceptadas para software, pero probablemente la más formal sea la siguiente:

[6] Diccionario de la lengua española 2005 (2010). wordreference.com (ed.): «software» (diccionario). Espasa-Calpe.

Es el conjunto de los programas de cómputo, procedimientos, reglas, documentación y datos asociados que forman parte de las operaciones de un sistema de computación.[7]

Considerando esta definición, el concepto de software va más allá de los programas de computación en sus distintos estados: código fuente, binario o ejecutable; también su documentación, los datos a procesar e incluso la información de usuario forman parte del software: es decir, *abarca todo lo intangible*, todo lo «no físico» relacionado.

El término «software» fue usado por primera vez en este sentido por John W. Tukey en 1957. En la ingeniería de software y las ciencias de la computación, el software es toda la información procesada por los sistemas informáticos: programas y datos.

El concepto de leer diferentes secuencias de instrucciones (programa) desde la memoria de un dispositivo para controlar los cálculos fue introducido por Charles Babbage como parte de su máquina diferencial. La teoría que forma la base de la mayor parte del software moderno fue propuesta por Alan Turing en su ensayo de 1936, «Los números computables», con una aplicación al problema de decisión.

CLASIFICACION DE SOFTWARE[8]

Si bien esta distinción es, en cierto modo, arbitraria, y a veces confusa, a los fines prácticos se puede clasificar al software en tres grandes tipos:

- **Software de sistema**: Su objetivo es desvincular adecuadamente al usuario y al programador de los detalles del sistema informático en particular que se use, aislándolo especialmente del procesamiento referido a las características internas de: memoria, discos, puertos y dispositivos de comunicaciones, impresoras, pantallas, teclados, etc. El

[7] IEEE Std, IEEE Software Engineering Standard: Glossary of Software Engineering Terminology. IEEE Computer Society Press, 1993

[8] Haeberer, A. M.; P. A. S. Veloso, G. Baum (1988) (en Español). *Formalización del proceso de desarrollo de software* (Ed. preliminar edición). Buenos Aires: Kapelusz

software de sistema le procura al usuario y programador, adecuadas interfaces de alto nivel, controladores, herramientas y utilidades de apoyo que permiten el mantenimiento del sistema global. Incluye entre otros:

- Sistemas operativos
- Controladores de dispositivos
- Herramientas de diagnóstico
- Herramientas de Corrección y Optimización
- Servidores
- Utilidades

- **Software de programación:** Es el conjunto de herramientas que permiten al programador desarrollar programas informáticos, usando diferentes alternativas y lenguajes de programación, de una manera práctica. Incluyen básicamente:
  - Editores de texto
  - Compiladores
  - Intérpretes
  - Enlazadores
  - Depuradores
  - Entornos de Desarrollo Integrados (IDE): Agrupan las anteriores herramientas, usualmente en un entorno visual, de forma tal que el programador no necesite introducir múltiples comandos para compilar, interpretar, depurar, etc. Habitualmente cuentan con una avanzada interfaz gráfica de usuario (GUI).
- **Software de aplicación**[9]: Es aquel que permite a los usuarios llevar a cabo una o varias tareas específicas, en cualquier campo de actividad susceptible de ser automatizado o asistido, con especial énfasis en los negocios. Incluye entre muchos otros:
  - Aplicaciones para Control de sistemas y automatización industrial
  - Aplicaciones ofimáticas
  - Software educativo
  - Software empresarial
  - Bases de datos
  - Telecomunicaciones (por ejemplo Internet y toda su estructura lógica)

[9] Sommerville, Ian (2005) Ingeniería del software (7ma. edición). Madrid: Pearson Educación S.A

- Videojuegos
- Software médico
- Software de cálculo Numérico y simbólico.
- Software de diseño asistido (CAD)
- Software de control numérico (CAM)

Servicio web[10]

Un servicio web (en inglés, *Web services*) es una tecnología que utiliza un conjunto de protocolos y estándares que sirven para intercambiar datos entre aplicaciones. Distintas aplicaciones de software desarrolladas en lenguajes de programación diferentes, y ejecutadas sobre cualquier plataforma, pueden utilizar los servicios web para intercambiar datos en redes de ordenadores como Internet. La interoperabilidad se consigue mediante la adopción de estándares abiertos. Las organizaciones OASIS y W3C son los comités responsables de la arquitectura y reglamentación de los servicios Web. Para mejorar la interoperabilidad entre distintas implementaciones de servicios Web se ha creado el organismo WS-I, encargado de desarrollar diversos perfiles para definir de manera más exhaustiva estos estándares. Es una maquina que atiende las peticiones de los clientes web y les envía los recursos solicitados.

Estándares empleados

- Web Services Protocol Stack: Así se denomina al conjunto de servicios y protocolos de los servicios Web.
- XML (Extensible Markup Language): Es el formato estándar para los datos que se vayan a intercambiar.
- SOAP (Simple Object Access Protocol) o XML-RPC (XML Remote Procedure Call): Protocolos sobre los que se establece el intercambio.
- Otros protocolos: los datos en XML también pueden enviarse de una aplicación a otra mediante protocolos normales como HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol), o SMTP (Simple Mail Transfer Protocol).
- WSDL (Web Services Description Language): Es el lenguaje de la interfaz

pública para los servicios Web. Es una descripción basada en XML de los requisitos funcionales necesarios para establecer una comunicación con los servicios Web.

- UDDI (Universal Description, Discovery and Integration): Protocolo para publicar la información de los servicios Web. Permite comprobar qué servicios web están disponibles.
- WS-Security (Web Service Security): Protocolo de seguridad aceptado como estandar por OASIS (Organization for the Advancement of Structured Information Standards). Garantiza la autenticación de los actores y la confidencialidad de los mensajes enviados.

Ventajas de los servicios web

- Aportan interoperabilidad entre aplicaciones de software independientemente de sus propiedades o de las plataformas sobre las que se instalen.
- Los servicios Web fomentan los estándares y protocolos basados en texto, que hacen más fácil acceder a su contenido y entender su funcionamiento.
- Permiten que servicios y software de diferentes compañías ubicadas en diferentes lugares geográficos puedan ser combinados fácilmente para proveer servicios integrados.

Inconvenientes de los servicios Web

- Para realizar transacciones no pueden compararse en su grado de desarrollo con los estándares abiertos de computación distribuida como CORBA (Common Object Request Broker Architecture).
- Su rendimiento es bajo si se compara con otros modelos de computación distribuida, tales como RMI (Remote Method Invocation), CORBA o DCOM (Distributed Component Object Model). Es uno de los inconvenientes derivados de adoptar un formato basado en texto. Y es que entre los objetivos de XML no se encuentra la concisión ni la eficacia de procesamiento.
- Al apoyarse en HTTP, pueden esquivar medidas de seguridad basadas en *firewall* cuyas reglas tratan de bloquear o auditar la comunicación entre programas a ambos lados de la barrera.

Razones para crear servicios Web

La principal razón para usar servicios Web es que se pueden utilizar con HTTP sobre TCP (Transmission Control Protocol) en el puerto 80. Dado que las organizaciones protegen sus redes mediante *firewalls* -que filtran y bloquean gran parte del tráfico de Internet-, cierran casi todos los puertos TCP salvo el 80, que es, precisamente, el que usan los navegadores. Los servicios Web utilizan este puerto, por la simple razón de que no resultan bloqueados. Es importante señalar que los servicios web se pueden utilizar sobre cualquier protocolo, sin embargo, TCP es el más común.

Otra razón es que, antes de que existiera SOAP, no había buenas interfaces para acceder a las funcionalidades de otros ordenadores en red. Las que había eran *ad hoc* y poco conocidas, tales como EDI (Electronic Data Interchange), RPC (Remote Procedure Call), u otras APIs.

Una tercera razón por la que los servicios Web son muy prácticos es que pueden aportar gran independencia entre la aplicación que usa el servicio Web y el propio servicio. De esta forma, los cambios a lo largo del tiempo en uno no deben afectar al otro. Esta flexibilidad será cada vez más importante, dado que la tendencia a construir grandes aplicaciones a partir de componentes distribuidos más pequeños es cada día más utilizada.

Se espera que para los próximos años mejoren la calidad y cantidad de servicios ofrecidos basados en los nuevos estándares.

Plataformas

Servidores de aplicaciones para servicios Web:

- JBoss servidor de aplicaciones J2EE Open Source de Red Hat inc.
- Oracle Fusion Middleware
- IBM Lotus Domino a partir de la versión 7.0
- Axis y el servidor Jakarta Tomcat (de Apache)
- ColdFusion MX de [[Macromedia]httpd]
- Java Web Services Development Pack (JWSDP) de Sun Microsystems (basado en Jakarta Tomcat)

- JOnAS (parte de *ObjectWeb* una iniciativa de código abierto)
- Microsoft .NET
- Novell exteNd (basado en la plataforma J2EE)
- WebLogic
- WebSphere
- JAX-WS con GlassFish
- Zope es un servidor de aplicaciones Web orientado a objetos desarrollado en el lenguaje de programación Python
- VERASTREAM de AttachmateWRQ para modernizar o integrar aplicaciones host IBM y VT
- PHP

Cómo funcionan los servicios Web

El siguiente gráfico muestra cómo interactúa un conjunto de Servicios Web:

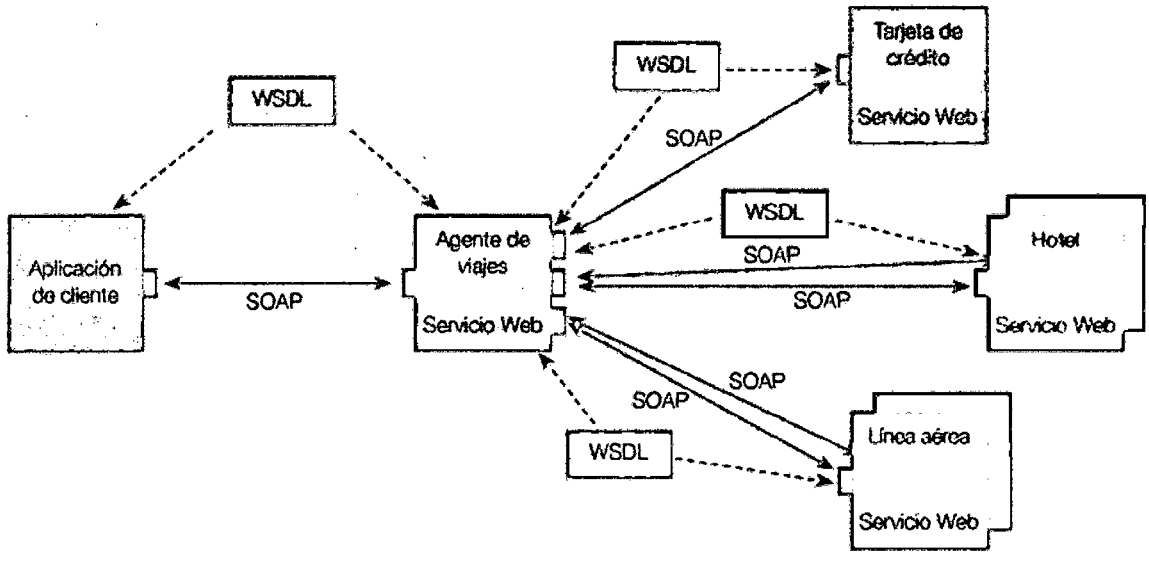


Figura 1 - Los servicios Web en Funcionamiento

Según el ejemplo del gráfico, un usuario (que juega el papel de cliente dentro de los Servicios Web), a través de una aplicación, solicita información sobre un viaje que desea realizar haciendo una petición a una agencia de viajes que ofrece sus **servicios** a través de Internet. La

agencia de viajes ofrecerá a su cliente (usuario) la información requerida. Para proporcionar al cliente la información que necesita, esta agencia de viajes solicita a su vez información a otros recursos (otros Servicios Web) en relación con el hotel y la compañía aérea. La agencia de viajes obtendrá información de estos recursos, lo que la convierte a su vez en cliente de esos otros Servicios Web que le van a proporcionar la información solicitada sobre el hotel y la línea aérea. Por último, el usuario realizará el pago del viaje a través de la agencia de viajes que servirá de intermediario entre el usuario y el servicio Web que gestionará el pago.

En todo este proceso intervienen una serie de tecnologías que hacen posible esta circulación de información. Por un lado, estaría SOAP (Protocolo Simple de Acceso a Objetos). Se trata de un protocolo basado en XML, que permite la interacción entre varios dispositivos y que tiene la capacidad de transmitir información compleja. Los datos pueden ser transmitidos a través de HTTP , SMTP , etc. SOAP especifica el formato de los mensajes. El mensaje SOAP está compuesto por un envelope (sobre), cuya estructura está formada por los siguientes elementos: header (cabecera) y body (cuerpo).

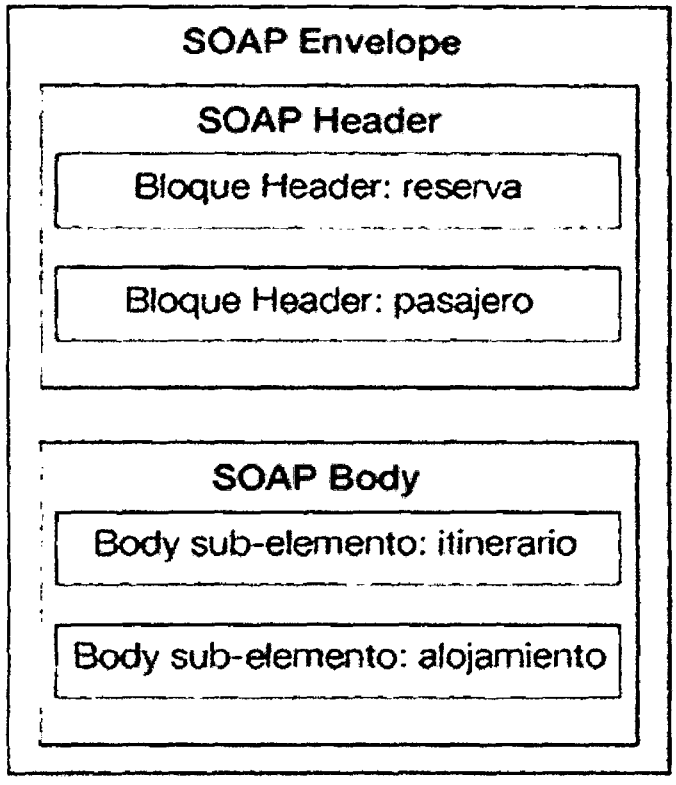


Figura 2 - Estructura de los mensajes

Para optimizar el rendimiento de las aplicaciones basadas en Servicios Web, se han desarrollado tecnologías complementarias a SOAP, que agilizan el envío de los mensajes (MTOM) y los recursos que se transmiten en esos mensajes (SOAP-RRSHB).

Por otro lado, WSDL (Lenguaje de Descripción de Servicios Web), permite que un servicio y un cliente establezcan un acuerdo en lo que se refiere a los detalles de transporte de mensajes y su contenido, a través de un documento procesable por dispositivos. WSDL representa una especie de contrato entre el proveedor y el que solicita. WSDL especifica la sintaxis y los mecanismos de intercambio de mensajes.

Durante la evolución de las necesidades de las aplicaciones basadas en Servicios Web de las grandes organizaciones, se han desarrollado mecanismos que permiten enriquecer las descripciones de las operaciones que realizan sus servicios mediante anotaciones semánticas y con directivas que definen el comportamiento. Esto permitiría encontrar los Servicios Web

que mejor se adapten a los objetivos deseados. Además, ante la complejidad de los procesos de las grandes aplicaciones empresariales, existe una tecnología que permite una definición de estos procesos mediante la composición de varios Servicios Web individuales, lo que se conoce como coreografía.

COMUNICACIONES[11]

La telecomunicación («comunicación a distancia», del prefijo griego *tele*, "distancia" y del latín *communicare*) es una técnica consistente en transmitir un mensaje desde un punto a otro, normalmente con el atributo típico adicional de ser bidireccional. El término telecomunicación cubre todas las formas de comunicación a distancia, incluyendo radio, telegrafía, televisión, telefonía transmisión de datos e interconexión de computadoras a nivel de enlace. El Día Mundial de las Telecomunicaciones se celebra el 17 de mayo. Según la Unión Internacional de Telecomunicaciones (UIT), las telecomunicaciones son «toda transmisión, emisión o recepción de signos, señales, datos, imágenes, voz, sonidos o información de cualquier naturaleza que se efectúa a través de cables, medios ópticos, físicos u otros sistemas electromagnéticos».

La base matemática sobre la que se desarrollan las telecomunicaciones fue desarrollada por el físico escocés James Clerk Maxwell. Maxwell, en el prefacio de su obra *Treatise on Electricity and Magnetism* (1873), declaró que su principal tarea consistía en justificar matemáticamente conceptos físicos descritos hasta ese momento de forma únicamente cualitativa, como las leyes de la inducción electromagnética y de los campos de fuerza, enunciadas por Michael Faraday. Con este objeto, introdujo el concepto de onda electromagnética, que permitió una descripción matemática adecuada de la interacción entre electricidad y magnetismo mediante sus célebres ecuaciones que describen y cuantifican los campos de fuerzas. Maxwell predijo que era posible propagar ondas por el espacio libre utilizando descargas eléctricas, hecho que corroboró Heinrich Hertz en 1887, ocho años después de la muerte de Maxwell, y que, posteriormente, supuso el inicio de la era de la

[11] Huidobro Moya, José Manuel. Redes y servicios de telecomunicaciones. Madrid: Thomson, 2006

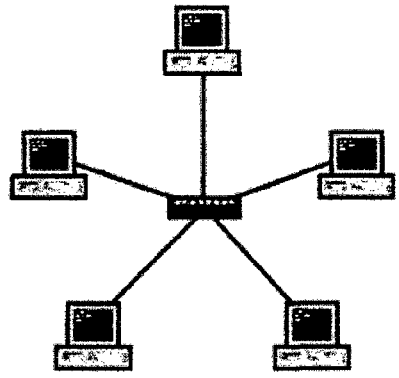
comunicación rápida a distancia. Hertz desarrolló el primer transmisor de radio generando radiofrecuencias entre 31 MHz y 1,25 GHz.

La serie de ondas y pulsos eléctricos que representan la información conforman lo que se denomina la señal, la cual atraviesa por un camino conductor de electricidad para el caso de los alámbricos; en el caso de la fibra óptica, los pulsos no son eléctricos sino luminosos y el medio es conductor de la luz. En el caso de los medios inalámbricos, la señal viaja a través del aire o el vacío, sin requerir un medio físico. El medio que se extiende desde el transmisor hasta el receptor conforma el citado enlace entre los dos extremos. En algunos casos este se forma de diversos tramos sobre medios diferentes, ejemplo de ello se da cuando tenemos un enlace total entre cable cobre y de fibra óptica en la red telefónica local. Existen varios términos que también se refieren al enlace, tales como canal y circuito los cuales son usados de forma indistinta. Sin embargo, se puede estrechar un poco más en su definición diciendo que canal tiene que ver principalmente con el enlace lógico, y que circuito se refiere al enlace físico que tiene canal de ida y canal de regreso

SWITCH[12]

Un **conmutador** o ***switch*** es un dispositivo digital lógico de interconexión de redes de computadoras que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red.

[12] Stallings, William (2004). *Comunicaciones y Redes de Computadores.* Prentice Hall



Un conmutador en el centro de una red en estrella.

Los conmutadores se utilizan cuando se desea conectar múltiples redes, fusionándolas en una sola. Al igual que los puentes, dado que funcionan como un filtro en la red, mejoran el rendimiento y la seguridad de las redes de área local.

ROUTER[13]

El primer dispositivo que tenía fundamentalmente la misma funcionalidad que lo que al día de hoy entendemos por router, era el Interface Message Processor o IMP. Los IMPs eran los dispositivos que formaban la ARPANET, la primera red de conmutación de paquetes. La idea de un router (llamado por aquel entonces gateway o compuerta) vino inicialmente de un grupo internacional de investigadores en redes de computadoras llamado el International Network Working Group (INWG). Creado en 1972 como un grupo informal para considerar las cuestiones técnicas que abarcaban la interconexión de redes diferentes, se convirtió ese mismo año en un subcomité del International Federation for Information Processing.

Esos dispositivos se diferenciaban de los conmutadores de paquetes que existían previamente en dos características. Por una parte, conectaban tipos de redes diferentes, mientras que por otra parte, eran dispositivos sin conexión, que no aseguraban fiabilidad en la entrega de tráfico, dejando este

[13] Comer, Douglas (2000). *Redes Globales de Información con Internet y TCP/ IP*. Prentice HalL

rol enteramente a los hosts. Esta última idea había sido ya planteada en la red CYCLADES.

La idea fue investigada con más detalle, con la intención de crear un sistema prototipo como parte de dos programas. Uno era el promovido por DARPA, programa que creó la arquitectura TCP/IP que se usa actualmente, y el otro era un programa en Xerox PARC para explorar nuevas tecnologías de redes, que produjo el sistema llamado PARC Universal Packet. Debido a la propiedad intelectual que concernía al proyecto, recibió poca atención fuera de Xerox durante muchos años.

Un tiempo después de 1974, Xerox consiguió el primer router funcional, aunque el primer y verdadero router IP fue desarrollado por Virginia Stazisar en BBN, como parte de ese esfuerzo promovido por DARPA, durante 1975-76. A finales de 1976, tres routers basados en PDP-11 entraron en servicio en el prototipo experimental de Internet.

El primer router multiprotocolo fue desarrollado simultáneamente por un grupo de investigadores del MIT y otro de Stanford en 1981. El router de Stanford se le atribuye a William Yeager y el del MIT a Noel Chiappa. Ambos estaban basados en PDP-11s. Como ahora prácticamente todos los trabajos en redes usan IP en la capa de red, los ruteadores multiprotocolo son en gran medida obsoletos, a pesar de que fueron importantes en las primeras etapas del crecimiento de las redes de ordenadores, cuando varios protocolos distintos de TCP/IP eran de uso generalizado. Los ruteadores que manejan IPv4 e IPv6 son multiprotocolo, pero en un sentido mucho menos variable que un ruteador que procesaba AppleTalk, DECnet, IP, y protocolos de XeroX. Desde mediados de los años 70 y en los años 80, los miniordenadores de propósito general servían como ruteadores.

Actualmente, los ruteadores de alta velocidad están altamente especializados, ya que se emplea un hardware específico para acelerar las funciones de ruteo más específicas, como son el encaminamiento de paquetes y funciones especiales como la encriptación IPsec.

En un ruteador se pueden identificar cuatro componentes:

- *Puertos de entrada*: realiza las funciones de la capa física consistentes en la terminación de un enlace físico de entrada a un router; realiza las funciones de la capa de enlace de datos necesarias para interoperar con las funciones de la capa de enlace de datos en el lado remoto del enlace de entrada; realiza también una función de búsqueda y reenvío de modo que un paquete reenviado dentro del entramado de conmutación del router emerge en el puerto de salida apropiado.

- *Entramado de conmutación*: conecta los puertos de entrada del router a sus puertos de salida.

- *Puertos de salida*: almacena los paquetes que le han sido reenviados a través del entramado de conmutación y los transmite al enlace de salida. Realiza entonces la función inversa de la capa física y de la capa de enlace que el puerto de entrada.

- *Procesador de enrutamiento*: ejecuta los protocolos de enrutamiento, mantiene la información de enrutamiento y las tablas de reenvío y realiza funciones de gestión de red dentro del router.

Conectividad Small Office, Home Office (SOHO)

Los ruteadores se utilizan con frecuencia en los hogares para conectar a un servicio de banda ancha, tales como IP sobre cable o ADSL. Un ruteador usado en una casa puede permitir la conectividad a una empresa a través de una red privada virtual segura.

Si bien son funcionalmente similares a los ruteadores, los residenciales usan traducción de dirección de red en lugar de direccionamiento.

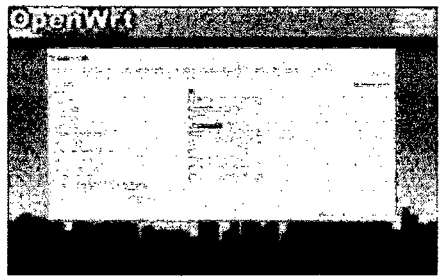
En lugar de conectar ordenadores locales a la red directamente, un ruteador residencial debe hacer que los ordenadores locales parezcan ser un solo equipo.

Ruteador de empresa

En las empresas se pueden encontrar ruteadores de todos los tamaños. Si bien los más poderosos tienden a ser encontrados en ISPs, instalaciones académicas y de investigación, pero también en grandes empresas.

El modelo de tres capas es de uso común, no todos de ellos necesitan estar presentes en otras redes más pequeñas.

Acceso



Una captura de pantalla de la interfaz web de LuCI OpenWrt.

Los ruteadores de acceso, incluyendo SOHO, se encuentran en sitios de clientes como sucursales que no necesitan de enrutamiento jerárquico de los propios. Normalmente, son optimizados para un bajo costo.

Distribución

Los ruteadores de distribución agregan tráfico desde ruteadores de acceso múltiple, ya sea en el mismo lugar, o de la obtención de los flujos de datos procedentes de múltiples sitios a la ubicación de una importante empresa. Los ruteadores de distribución son a menudo responsables de la aplicación de la calidad del servicio a través de una WAN, por lo que deben tener una memoria considerable, múltiples interfaces WAN, y transformación sustancial de inteligencia.

También pueden proporcionar conectividad a los grupos de servidores o redes externas. En la última solicitud, el sistema de funcionamiento del ruteador debe ser cuidadoso como parte de la seguridad de la arquitectura global. Separado del ruteador puede estar un cortafuegos o VPN concentrador, o el ruteador puede incluir estas y otras funciones de seguridad. Cuando una empresa se basa principalmente en un campus, podría no haber una clara distribución de nivel, que no sea tal vez el acceso fuera del campus.

En tales casos, los ruteadores de acceso, conectados a una red de área local (LAN), se interconectan a través del *Core routers*.

Núcleo

En las empresas, el *core routers* puede proporcionar una "columna vertebral" interconectando la distribución de los niveles de los ruteadores de múltiples edificios de un campus, o a las grandes empresas locales. Tienden a ser optimizados para ancho de banda alto.

Cuando una empresa está ampliamente distribuida sin ubicación central, la función del *core router* puede ser asumido por el servicio de WAN al que se suscribe la empresa, y la distribución de ruteadores se convierte en el nivel más alto.

Borde

Los ruteadores de borde enlazan sistemas autónomos con las redes troncales de Internet u otros sistemas autónomos, tienen que estar preparados para manejar el protocolo BGP y si quieren recibir las rutas BGP, deben poseer una gran cantidad de memoria.

Ruteadores inalámbricos[14]

A pesar de que tradicionalmente los ruteadores solían tratar con redes fijas (Ethernet, ADSL, RDSI...), en los últimos tiempos han comenzado a aparecer ruteadores que permiten realizar una interfaz entre redes fijas y móviles (Wi-Fi,

[14] Comer, Douglas (2000). *Redes Globales de Información con Internet y TCP/ IP.* Prentice Hall

GPRS, Edge, UMTS, Fritz!Box, WiMAX...) Un ruteador inalámbrico comparte el mismo principio que un ruteador tradicional. La diferencia es que éste permite la conexión de dispositivos inalámbricos a las redes a las que el ruteador está conectado mediante conexiones por cable. La diferencia existente entre este tipo de ruteadores viene dada por la potencia que alcanzan, las frecuencias y los protocolos en los que trabajan.

En Wi-Fi estas distintas diferencias se dan en las denominaciones como clase a/b/g/ y n.

Fabricantes

Uno de los fabricantes que más cuota de mercado tiene (a nivel profesional sobretodo) en lo que a venta de hardware para redes se refiere es Cisco Systems. Dentro de su amplia gama de productos enfocada al manejo y administración de redes de conmutación de paquetes, se distinguen dos tipos:

- *Equipos de configuración fija*: son routers o switches.

- *Equipos modulares o configurables*: constan de un chasis al que se le pueden añadir módulos con diversos tipos de interfaces, módulos de switching... y además, cuentan con un módulo interno de routing denominado Route Switch Module (RSM).

  Es interesante saber las posibilidades de configuración que ofrece el sistema operativo IOS de Cisco para entender mejor las posibilidades de funcionamiento de los routers.

En IOS se distinguen dos tipos de interfaces:

- *Interfaces enrutadas*: son interfaces de nivel 3, accesibles por IP. Cada una se corresponde con una dirección subred distinta. En IOS se denominan "IP interface". Se distinguen a su vez dos subtipos:

- *Interfaces físicas*: aquellas accesibles directamente por IP.

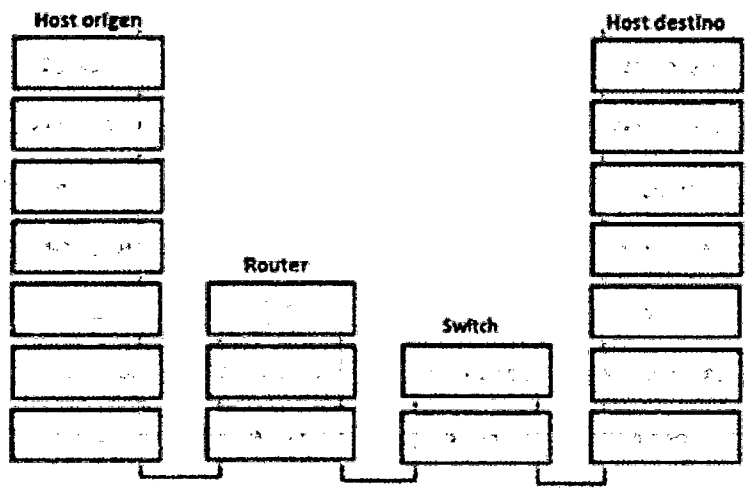
- *Interfaces virtuales*: aquellas que se corresponden con una VLAN o un CV. Si dicha interfaz se corresponde con una única VLAN se denomina Switch Virtual Interfaz (SVI), mientras que si se corresponde con un enlace trunk o con un CV, actúan como subinterfaces.

- *Interfaces conmutadas*: se trata de interfaces de nivel 2 accesibles solo por el módulo de switching. En IOS reciben el nombre de "switch port". Las hay de dos tipos:

- *Puertos de acceso*: soportan únicamente tráfico de una VLAN.
- *Puertos trunk*: soportan tráfico de varias VLANs distintas.

Por supuesto, estas posibilidades de configuración están únicamente disponibles en los equipos modulares, ya que en los de configuración fija, los puertos de un router actúan siempre como interfaces enrutadas, mientras que los puertos de un switch como interfaces conmutadas. Además, la única posible ambigüedad en los equipos configurables se da en los módulos de switching, donde los puertos pueden actuar de las dos maneras, dependiendo de los intereses del usuario.

Conmutadores frente a routers



Routers y switches en el modelo OSI

Un conmutador, al igual que un router es también un dispositivo de conmutación de paquetes de almacenamiento y reenvío. La diferencia fundamental es que el conmutador opera en la capa 2 (capa de enlace) del modelo OSI, por lo que para enviar un paquete se basa en una dirección MAC, al contrario de un router que emplea la dirección IP.

Un **concentrador** o ***hub*** es un dispositivo que permite centralizar el cableado de una red y poder ampliarla. Esto significa que dicho dispositivo recibe una señal y repite esta señal emitiéndola por sus diferentes puertos.

En la actualidad, la tarea de los concentradores la realizan, con frecuencia, los conmutadores o *switchs*.

Información técnica

Una red Ethernet se comporta como un medio compartido, es decir, sólo un dispositivo puede transmitir con éxito a la vez y cada uno es responsable de la detección de colisiones y de la retransmisión. Con enlaces 10BASE-T y 100Base-T (que generalmente representan la mayoría o la totalidad de los puertos en un concentrador) hay parejas separadas para transmitir y recibir, pero que se utilizan en modo *half duplex* el cual se comporta todavía como un medio de enlaces compartidos (véase 10BASE-T para las especificaciones de los pines).

Un concentrador, o repetidor, es un dispositivo de emisión bastante sencillo. Los concentradores no logran dirigir el tráfico que llega a través de ellos, y cualquier paquete de entrada es transmitido a otro puerto (que no sea el puerto de entrada). Dado que cada paquete está siendo enviado a través de cualquier otro puerto, aparecen las colisiones de paquetes como resultado, que impiden en gran medida la fluidez del tráfico. Cuando dos dispositivos intentan comunicar simultáneamente, ocurrirá una colisión entre los paquetes transmitidos, que los dispositivos transmisores detectan. Al detectar esta colisión, los dispositivos dejan de transmitir y hacen una pausa antes de volver a enviar los paquetes.

La necesidad de *hosts* para poder detectar las colisiones limita el número de centros y el tamaño total de la red. Para 10 Mbit/s en redes, de hasta 5 segmentos (4 concentradores) se permite entre dos estaciones finales. Para 100 Mbit/s en redes, el límite se reduce a 3 segmentos (2 concentradores) entre dos estaciones finales, e incluso sólo en el caso de que los concentradores fueran de la variedad de baja demora. Algunos concentradores tienen puertos especiales (y, en general, específicos del fabricante) les permiten ser combinados de un modo que consiente encadenar a través de los cables Ethernet los concentradores más sencillos, pero aun así una gran red Fast Ethernet es probable que requiera conmutadores para evitar el encadenamiento de concentradores.

La mayoría de los concentradores detectan problemas típicos, como el exceso de colisiones en cada puerto. Así, un concentrador basado en Ethernet, generalmente es más robusto que el cable coaxial basado en Ethernet. Incluso si la partición no se realiza de forma automática, un concentrador de solución de problemas la hace más fácil ya que las luces pueden indicar el posible problema de la fuente. Asimismo, elimina la necesidad de solucionar problemas de un cable muy grande con múltiples tomas.

Concentradores de doble velocidad

Los concentradores sufrieron el problema de que como simples repetidores sólo podían soportar una única velocidad. Mientras que los PC normales con ranuras de expansión podrían ser fácilmente actualizados a Fast Ethernet con una nueva tarjeta de red, máquinas con menos mecanismos de expansión comunes, como impresoras, pueden ser costosas o imposibles de actualizar. Por lo tanto, un punto medio entre concentrador y conmutador es conocido como **concentrador de doble velocidad**.

Este tipo de dispositivos consisten fundamentalmente en dos concentradores (uno de cada velocidad) y dos puertos puente entre ellos. Los dispositivos se conectan al concentrador apropiado automáticamente, en función de su velocidad. Desde el puente sólo se tienen dos puertos, y sólo uno de ellos necesita ser de 100 Mb/s.

2.2.2. SEGURIDAD DE LA INFORMACIÓN

Recuperación de desastres[15]

La recuperación de desastres es la habilidad de recuperarse de un evento que impacta el funcionamiento del centro de datos de su organización lo más rápido y completo posible. El tipo de desastre puede variar, pero el objetivo final es siempre el mismo.

Los pasos relacionados con la recuperación a partir de un desastre son numerosos y con un rango bien amplio. A continuación se muestra una descripción general a un nivel alto del proceso, junto con los puntos claves a tener en mente.

2.2.3.1. Creación, Evaluación e Implementación de un Plan de Recuperación de Desastres

Un sitio de respaldo es vital, sin embargo es inútil sin un plan de recuperación de desastres. Un plan de recuperación de desastres indica cada faceta del proceso de recuperación, incluyendo (pero no limitado) a:

- Los eventos que denotan posibles desastres
- Las personas en la organización que tienen la autoridad para declarar un desastre y por ende, colocar el plan en efecto
- La secuencia de eventos necesaria para preparar el sitio de respaldo una vez que se ha declarado un desastre
- Los papeles y responsabilidades de todo el personal clave con respecto a llevar a cabo el plan
- Un inventario del hardware necesario y del software requerido para restaurar la producción
- Un plan listando el personal a cubrir el sitio de respaldo, incluyendo un horario de rotación para soportar las operaciones continuas sin quemar a los miembros del equipo de desastres

[15] Jim Hoffer, "Backing Up Business - Industry Trend or Event", Health Management Technology, Jan 2001

- La secuencia de eventos necesaria para mover las operaciones desde el sitio de respaldo al nuevo/restaurado centro de datos

  Los planes de recuperación de desastres a menudo llenan múltiples carpetas de hojas sueltas. Este nivel de detalle es vital porque en el evento de una emergencia, el plan quizás sea lo único que quede de su centro de datos anterior (además de los otros sitios de respaldo, por supuesto) para ayudarlo a reconstruir y restaurar las operaciones.

Un documento de tal importancia merece una consideración bien seria (y posiblemente asistencia profesional para su creación).

Una vez que este documento es creado, el conocimiento que contiene debe ser evaluado periódicamente. Evaluar un plan de recuperación de desastres implica seguir los pasos del plan: ir al sitio de respaldo y configurar el centro de datos temporal, ejecutar las aplicaciones temporalmente y reactivar las operaciones normales después de que el "desastre" termine. La mayoría de las pruebas no tratan de llevar a cabo un 100% de las tareas del plan; en cambio, se selecciona un sistema y una aplicación representativa para reubicarlos en el sitio de respaldo, se coloca en producción por un período de tiempo y se lleva a operación normal al final de la prueba.

2.2.3.2. Sitios de respaldo: frío, templado y caliente

Uno de los aspectos más importantes del plan de recuperación de desastres es tener una ubicación desde la cual este puede ser ejecutado. Esta ubicación se conoce como sitio de respaldo. En el evento de un desastre, el sitio de respaldo es donde se recreará su centro de datos y desde donde usted operará, durante el mismo.

Hay tres tipos diferentes de sitios de respaldo:

- Sitios de respaldo fríos
- Sitios de respaldo templado
- Sitios de respaldo calientes

Obviamente estos términos no se refieren a la temperatura del sitio de respaldo. Se refieren en realidad al esfuerzo requerido para comenzar las operaciones en el sitio de respaldo en el evento de un desastre.

Un sitio de respaldo frío es simplemente un espacio en un edificio configurado apropiadamente. Todo lo que se necesite para restaurar el servicio a sus usuarios se debe conseguir y entregar a este sitio antes de comenzar el proceso de recuperación. Como se puede imaginar, el retraso de ir desde un sitio frío a uno en operación completa puede ser sustancial.

Los sitios de respaldo frío son los menos costosos.

Un sitio tibio ya está equipado con el hardware representando una representación fiel de lo encontrado en su centro de datos. Para restaurar el servicio, se deben despachar los últimos respaldos desde sus instalaciones de almacenamiento fuera del sitio y completar un restauración a metal pelado, antes de que pueda comenzar el trabajo real de recuperación.

Los sitios de respaldo calientes tienen una imagen espejo virtual de su centro de datos, con todos los sistemas configurados y esperando solamente por los últimos respaldos de los datos de sus usuarios desde las facilidades de almacenamiento fuera del sitio. Como se puede imaginar, un sitio de respaldo caliente se puede poner en funcionamiento completo en unas pocas horas.

Un sitio de respaldo caliente comprende el enfoque más costoso para una recuperación de desastres.

Los sitios de respaldo pueden provenir de tres fuentes diferentes:

- Compañías especializadas en suministrar servicios de recuperación de desastres
- Otras ubicaciones que pertenecen y son operadas por la organización
- Un acuerdo mutuo con otra organización para compartir las facilidades del centro de datos en el evento de un desastre

Cada enfoque tiene sus puntos buenos y malos. Por ejemplo, haciendo un contrato con una firma de recuperación de desastres a menudo trae consigo el acceso a profesionales con la experiencia necesaria para guiar a las organizaciones a través del proceso de creación, evaluación e implementación de un plan de recuperación de desastres. Como se puede imaginar, estos servicios tienen su costo.

El uso de otras instalaciones que pertenecen y son operadas por su organización, pueden ser esencialmente una opción de costo cero, pero el surtir el sitio de respaldo y mantener su disponibilidad inmediata es una proposición costosa.

Preparar un acuerdo para compartir centros de datos con otra organización puede ser extremadamente económico, pero usualmente las operaciones a largo plazo bajo estas condiciones no son posibles, pues probablemente el centro de datos anfitrión todavía continúa su producción normal, haciendo la situación incómoda en el mejor de los casos.

Por otro lado, la selección del sitio de respaldo es un acuerdo entre los costos y la necesidad de su organización por la continuación de las operaciones.

2.2.3.3. Disponibilidad del Hardware y Software

Su plan de recuperación de desastres debe incluir métodos para conseguir el hardware y software necesarios para las operaciones en el sitio de respaldo. Un sitio de respaldo manejado profesionalmente quizás ya tenga todo lo que

usted necesita (o quizás tenga que organizar la adquisición y entrega de materiales especializados que el sitio no tiene disponibles); por otro lado, un sitio de respaldo frío implica que se tienen identificadas las fuentes para cada ítem requerido. A menudo las organizaciones trabajan directamente con los fabricantes para establecer acuerdos para la entrega inmediata de hardware y/o software en el evento de un desastre.

2.2.3.4. Disponibilidad de los respaldos

Cuando se declara un desastre, es necesario notificarlo a sus instalaciones de almacenamiento fuera de sitio por dos razones:

- Para enviar los últimos respaldos al sitio de respaldo
- Para coordinar entregas de respaldos regulares al sitio de respaldo (en soporte a los respaldos normales en el sitio de respaldo)

2.2.3.5. Conectividad de red al sitio de respaldo

Un centro de datos no es de mucha ayuda si se encuentra desconectado del resto de la organización que está sirviendo. Dependiendo del plan de recuperación de desastres y de la naturaleza del mismo, su comunidad de usuarios puede estar ubicada a kilómetros de distancia del sitio de respaldo. En estos casos, una buena conectividad es vital para restaurar la producción.

Otro tipo de conectividad a tener en mente es la conectividad telefónica. Debe asegurarse de que existen suficientes líneas telefónicas disponibles para manejar todas las comunicaciones verbales con sus usuarios. Lo que antes podía ser un grito por encima de la pared de un cubículo ahora implica una conversación telefónica de larga distancia; por lo tanto, planee para tener más conectividad telefónica de la que pudiera parecer necesaria en un principio.

2.2.3.6. Personal del sitio de respaldo

El problema sobre conseguir el personal para su sitio de respaldo es multidimensional. Un aspecto del problema es determinar el personal requerido para poner a funcionar el centro de datos de respaldo por el tiempo

que sea necesario. Mientras que un equipo esquelético puede mantener las cosas en funcionamiento por un corto período de tiempo, a medida que el desastre se extiende se necesitará más y más gente para continuar el esfuerzo necesario para funcionar bajo las circunstancias extraordinarias que rodean un desastre.

Esto implica asegurarse de que el personal tiene tiempo suficiente para descansar y posiblemente viajar de regreso a sus hogares. Si el desastre fuese tan extendido que afecte también los hogares y familias de la gente, se necesitará tiempo adicional para permitirles manejar su propia recuperación de desastre. Se necesita alojamiento temporal cerca del sitio de respaldo, junto con el transporte requerido para movilizar a la gente entre el sitio de respaldo y su alojamiento.

A menudo un plan de recuperación de desastres incluye que trabaje en el sitio un personal representativo de todas las partes de la comunidad de usuarios de la organización. Esto depende en la habilidad de su organización de operar con un centro de datos remoto. Si los usuarios representantes deben trabajar en el sitio de respaldo, también deben estar disponibles facilidades similares para ellos.

2.2.3.7. Regreso a la normalidad

Eventualmente todos los desastres terminan. El plan de recuperación de desastres debe tomar en cuenta esta fase también. El nuevo centro de datos debe ser equipado con todo el software y hardware necesario; mientras que esta fase a menudo no tiene la naturaleza crítica de las preparaciones efectuadas cuando se declaró inicialmente el desastre, los sitios de respaldo cuestan dinero cada día que son utilizados, por lo que las preocupaciones económicas dictarán que el cambio se lleve a cabo lo más pronto posible.

Se deben hacer y entregar los últimos respaldos desde el sitio de respaldo al nuevo centro de datos. Después de almacenarlos en el nuevo hardware, se puede reactivar la producción en el nuevo centro de datos.

En este punto se puede desarmar el centro de datos de respaldo, con la sección final del plan indicando la disposición de todo el hardware temporal.

Finalmente, se hace una revisión de la efectividad del plan, integrando cualquier cambio recomendado por el comité de revisión en una versión actualizada del plan.

Seguridad Informática[16]

La infraestructura de conectividad para interconectar entidades debe garantizar el flujo e intercambio de información segura entre entidades participantes. Al utilizar redes públicas como Internet, la información pasa a través de muchos puntos que no están bajo control, y existe el riesgo de que la información pueda llegar a ser interceptada por terceros. Para garantizar el flujo seguro de datos, es necesario contar con una red privada virtual, en la cual viajen exclusivamente datos de las entidades, y que estos datos viajen cifrados para reducir al máximo la posibilidad de que la información pueda ser interceptada e interpretada por terceros.

Seguridad en centros de procesamiento de datos

Debido a la evolución de las tecnologías, de los servicios y de los entornos empresariales en general, la información se ha convertido quizás en el primer patrimonio de las empresas. De ahí que se pueda asegurar que la Seguridad en los

Centros de Procesamientos de Datos (C.P.D.) es una necesidad impuesta a toda entidad o empresa de cualquier rango.

La seguridad constituye, por consiguiente, uno de los principales problemas en todo sistema de procesamiento de datos; la expansión de los sistemas informáticos hace que sea imprescindible la implantación de nuevos elementos de seguridad que protejan de una forma adecuada estos entornos.

1 RIESGOS DE LOS CENTROS DE PROCESAMIENTOS DE DATOS

La seguridad del Centro de Procesamiento de Datos hace referencia a los riesgos que afectan a las instalaciones donde se encuentra el mismo y a las

[16] WIKIPEDIA, La enciclopedia libre. [en línea]

soluciones que han de adoptarse para su protección. La clasificación general de estos riesgos contemplados desde la posibilidad de que ocurra un evento/siniestro en función

de los recursos y el entorno, es la siguiente:

Siniestros en:

Recintos y edificio; Instalaciones auxiliares; Equipos o hardware; Software

Mapa de riesgos:

Incendio; Gases; Explosión/implosión; Daños por agua; Rayo. Tensión inducida:

Sobretensiones/cortocircuitos; Robo. Hurto; Actos vandálicos; Avería de componentes; Cambio de condiciones ambientales; Virus informático; Modificaciones o espionaje de datos; Pérdidas de datos/copias de seguridad

Algunos de estos riesgos representan una problemática diferente, que debe ser tratada individualmente y de acuerdo con las peculiaridades de cada instalación.

Incendio

Todos los incidentes producidos a causa del fuego en un C.P.D. pueden causar un daño significante y graves pérdidas incluso cuando se trata de fuegos pequeños. Los gases corrosivos y el humo desprendido por el PVC y otros plásticos en

combustión pueden dañar las placas del circuito electrónico. Además el calor generado puede destruir la sensibilidad del equipo y dañar el disco duro.

Causas de incendio

La experiencia ha demostrado que los fuegos se producen principalmente

por:

- Inflamación del aislante del cableado por aumento del calor.
- Negligencia provocada por fumadores o trabajos con fuegos abiertos

incontrolados, como puede ser la soldadura.

- Defectos de los componentes eléctricos del equipo, especialmente fuentes de alimentación.
- Cortocircuitos.
- Incendios exteriores a las instalaciones.

Daños producidos.- Los daños producidos en el C.P.D. en caso de incendio son fundamentalmente:

- Derrumbamientos.
- Deformaciones parciales y totales de los equipos.
- Oxidaciones en los componentes microelectrónicos producidas por los humos de las
- combustiones y el agua y humedad relativa elevada, proveniente de las tareas de extinción, como de los gases generados en incendio.

Medidas para limitar los daños después del incendio.- Los daños de incendio comprenden los daños directos e indirectos consecuentes del incendio.

Desde el momento de la concepción del incendio en el C.P.D., se deben estudiar las medidas para minimizar las consecuencias del mismo.

El C.P.D. puede contar con los siguientes sistemas de protección contra incendios de funcionamiento automático, cuya sucesiva implantación aumentará considerablemente su nivel de seguridad:

- Detección automática de incendios.
- Rociadores automáticos de acción previa.
- Sistema de extinción automática por CO2.
- Sistemas de nebulización de agua.
- Detección automática de incendios

La instalación de detección de incendios tiene una doble misión:

1. Avisar del inicio de un incendio al encargado del área de informática, o responsable de seguridad.

2. Desconectar la corriente eléctrica al ordenador, el sistema de ventilación,

cerrar de las compuertas cortafuego y disparar el sistema de extinción automática.

Para la detección en la propia sala también puede emplearse un sistema de fuegos incipientes que muestra y analiza en continuo el aire del local protegido. El aire se aspira por conductos mediante un ventilador y a través de una red de tuberías es conducido a un detector de alta sensibilidad.

Se instalará un sistema de detección automática de incendios de tipo "puntual-analógica-inteligente", en falso techo, falso suelo y ambiente. Este sistema de detección será el encargado del disparo del sistema de CO2 de inundación total del falso suelo y del llenado de las tuberías del sistema de rociadores, si existiesen tales instalaciones.

Se utilizarán detectores iónicos de humos para detectar fuegos abiertos, como pueden ser lugares donde se almacene papel.

Por regla general, el conducto de ventilación también debe protegerse mediante sistemas de aspiración con detectores iónicos de humo.

- **Sistemas de Extinción Automática por CO2**

  Los rociadores automáticos se justifican cuando el edificio no dispone de las garantías suficientes contra incendio o cuando el C.P.D. se encuentra ubicado en un edificio con cobertura de rociadores automáticos y la separación del centro con el edificio no tiene suficiente resistencia al fuego.

  Además se instalarán sistemas independientes de aplicación local de CO2 dentro de las carcasas de las C.P.U.

  Este sistema de detección de puntual da la alarma y señala el armario donde posteriormente se producirá descarga del CO2 en su interior. Análogamente puede explicarse en los falsos techos y falsos suelos.

- **Sistemas de Protección Contra Incendios:**

  CO2 en ambiente:

La función de esta instalación, es la extinción de un fuego cuando está todavía en estado incipiente y si es necesario, mantener la precisa concentración de CO2 durante el tiempo concreto para minimizar el peligro de una reignición.

Rociadores:

Standard

Tubería seca

Nebulización de agua: El agua nebulizada basa su principio extintor y de control de fuego en tres acciones diferentes:

- Enfriamiento.
- Desplazamiento del oxígeno por vapor de agua.
- Atenuación del a transmisión de calor por radiación.

El efecto de enfriamiento se optimiza al máximo, por la división del agua aplicada en gotas extremadamente pequeñas (80-200m), lo que resulta en un incremento de la superficie de absorción de calor y maximización de la producción de vapor. El proceso de vaporización extrae calor de la llama y de los vapores inflamables, produciendo la extinción.

El vapor de agua al expandirse desplaza el aire y reduce consecuentemente la cantidad de oxígeno que alimenta la combustión. Si este vapor puede quedar confinado en la proximidad del incendio, caso de recinto cerrado, o puede ser proyectado directamente a la base de las llamas, el oxígeno libre queda reducido consiguiéndose el cese de la

combustión. Por otro lado las pequeñísimas gotas de agua quedan suspendidas en el aire, reduciendo la transmisión de calor, por radiación, entre las llamas y el combustible no volatilizado, impidiendo su contribución a la continuidad del incendio.

Gases

- Causas de desprendimiento de humos: Centrándonos en los daños posteriores al incendio producidos por gases, están los producidos por HCl,

  sobre todo cuando se ha quemado PVC. El HCl se encuentra en forma de materiales de aislamiento, cables eléctricos, pavimentos plastificados, puertas plegables, etc. El HCl comienza a desprenderse del PVC a partir de una temperatura de 120ºC, y al llegar a 300ºC, ya se puede desprender en su totalidad de cualquier tipo de PVC. Otros gases de combustión se desprenden de productos de limpieza o disolventes.

- Daños producidos: La acción de los gases se puede detectar a simple vista debido:
  - El hierro es coloreado de marrón oscuro.
  - En el acero inoxidable las superficies se vuelven mates, apareciendo manchas de color marrón
  - oscuro con puntos negros en el centro.
  - En el cobre comienzan a aparecer manchas rojas y a continuación de un color verde claro.
- Medidas para limitar los daños después del siniestro
  - Se evacuarán lo antes posible, con permiso de los bomberos, los gases provenientes de la combustión al exterior abriendo ventanas y puertas, por efecto Venturi o mediante equipos de evacuación de humos.
  - Se desconectarán lo antes posible los equipos de aire acondicionado y ventilación.
  - Se cerrarán todas las puertas y ventanas que comuniquen con el resto del edificio.

Agua

- Causas de los daños por agua
  - Los daños producidos por el agua se entienden como inundaciones debidas a diversas causas, como son la rotura de conducciones, de agua sanitaria o de los equipos acondicionadores de aire, las extinciones de incendios y las

inundaciones propiamente dichas.

- Medidas de prevención
  - Se tendrá en cuenta que no pase ninguna conducción de agua o desagüe por la vertical del Centro de Procesamiento de Datos.
  - Será necesario que la impermeabilización de las cubiertas se haga contemplando normas más estrictas para otros edificios, poniendo especial cuidado tanto en la calidad de los materiales utilizados como en la ejecución de la mamo de obra.
  - Deberá existir una impermeabilización al agua de todos los conductos que penetren dentro del C.P.D.
  - No deberán existir bandejas de condensación en el falso suelo **ni en el falso techo.**

Modificación o espionaje de datos[17]

- Causas
  - En los entornos del C.P.D. se incluyen como errores y omisiones, los problemas de organización, los montajes incorrectos de soportes de datos, la liberación de ficheros no caducados, la distribución incorrecta de información confidencial, los trabajos realizados con versiones de programas incorrectas, etc.
  - El espionaje de datos es causado generalmente por empleados insatisfechos o descontentos. La utilización fraudulenta de datos o software puede dar lugar a pérdidas importantes en la empresa.
- Control de riesgos

Las medidas para el control de riesgos se centran básicamente en el control de accesos al C.P.D. y las medidas de seguridad para la utilización de aplicaciones y datos.

[17] Feenberg, Daniel (14 de mayo de 2004). «Can Intelligence Agencies Read Overwritten Data? A response to Gutmann. ». National Bureau of Economic Research.

CAPÍTULO III

REVISIÓN DEL ESTADO DEL ARTE

3.1. TAXONOMÍA DEL TEMA DE INVESTIGACIÓN

El tema de investigación se encuentra dentro del objetivo de Seguridad Informática de una organización, lo cual se define como una "declaración de intenciones para contrarrestar las amenazas identificadas y / o satisfacer las políticas de seguridad de la organización".

A estos Objetivos de seguridad también se les denomina propiedades de seguridad, aspectos de seguridad, o estados de la seguridad. La literatura existente las categoriza de acuerdo a varias taxonomías. Por ejemplo, Bishop [18] identifica 3 aspectos básicos de seguridad: Confidencialidad, Integridad y Disponibilidad, cuya interpretación varía de acuerdo al contexto del que proceden. Menezes [19].lista hasta diecisiete objetivos básicos para la seguridad informática, entre los que se observa algunos comunes como la confidencialidad, la integridad, identificación y autorización. También identifica firmas, marcas de tiempo y recibos como objetivos de seguridad, que en términos convencionales son más bien vistos como mecanismos o medios para alcanzar un objetivo específico. Sin embargo estos objetivos de seguridad se derivan de las cuatro metas de la criptografía: confidencialidad,

[18] M. Bishop. Computer Security: Art and Science, chapter 25. Addison-Wesley, December 2002.

[19] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone. Handbook of Applied Cryptography. CRC, 1996.

integridad, autenticación y no repudio. Eckert[20] identifica seis objetivos básicos de seguridad (autenticidad, Confidencialidad, Integridad, Disponibilidad, rendición de cuentas y el anonimato) .

Para nuestro propósito, podemos identificar tres categorías generales de objetivos genéricos de seguridad de acuerdo con el objetivo que persigue una organización en cuanto a la seguridad de los activos informáticos. Nosotros nos basaremos en la taxonomía propuesta por Bishop[21] y en consecuencia definimos los tres objetivos de seguridad informática:

1. La confidencialidad cuya meta es que los datos deben ser legibles a los actores que cuenten con los permisos correspondientes.

2. La integridad cuya meta es que los datos y la información no debe ser modificada si no está explícitamente permitido.

3. La disponibilidad cuya meta es que los activos informáticos tienen que estar disponibles para las personas autorizadas y autenticadas cuando sea necesario,

De estos tres objetivos de seguridad, nos centramos en el aspecto de "Disponibilidad", por cuanto un Plan de Recuperación de Desastres es una medida de contingencia que debe desarrollarse con el fin de minimizar el impacto en la continuidad de los servicios de una Plataforma de Interoperabilidad bajo el enfoque SOA.

La taxonomía o clasificación que incluye al PRD, se encuentra dentro de los llamados Planes de Contingencia del Negocio, los cuales son usados para crear y validar planes logísticos como una buena práctica de cómo una organización debe recuperar y restaurar sus funciones críticas parcial o totalmente interrumpidas dentro de un tiempo predeterminado después de una interrupción no deseada o desastre.

[20] C. Eckert. IT-Sicherheit. Oldenbourg, Manunchen [u.a.], 2004.

[21] M. Bishop. Computer Security: Art and Science, chapter 25. Addison-Wesley, December 2002.

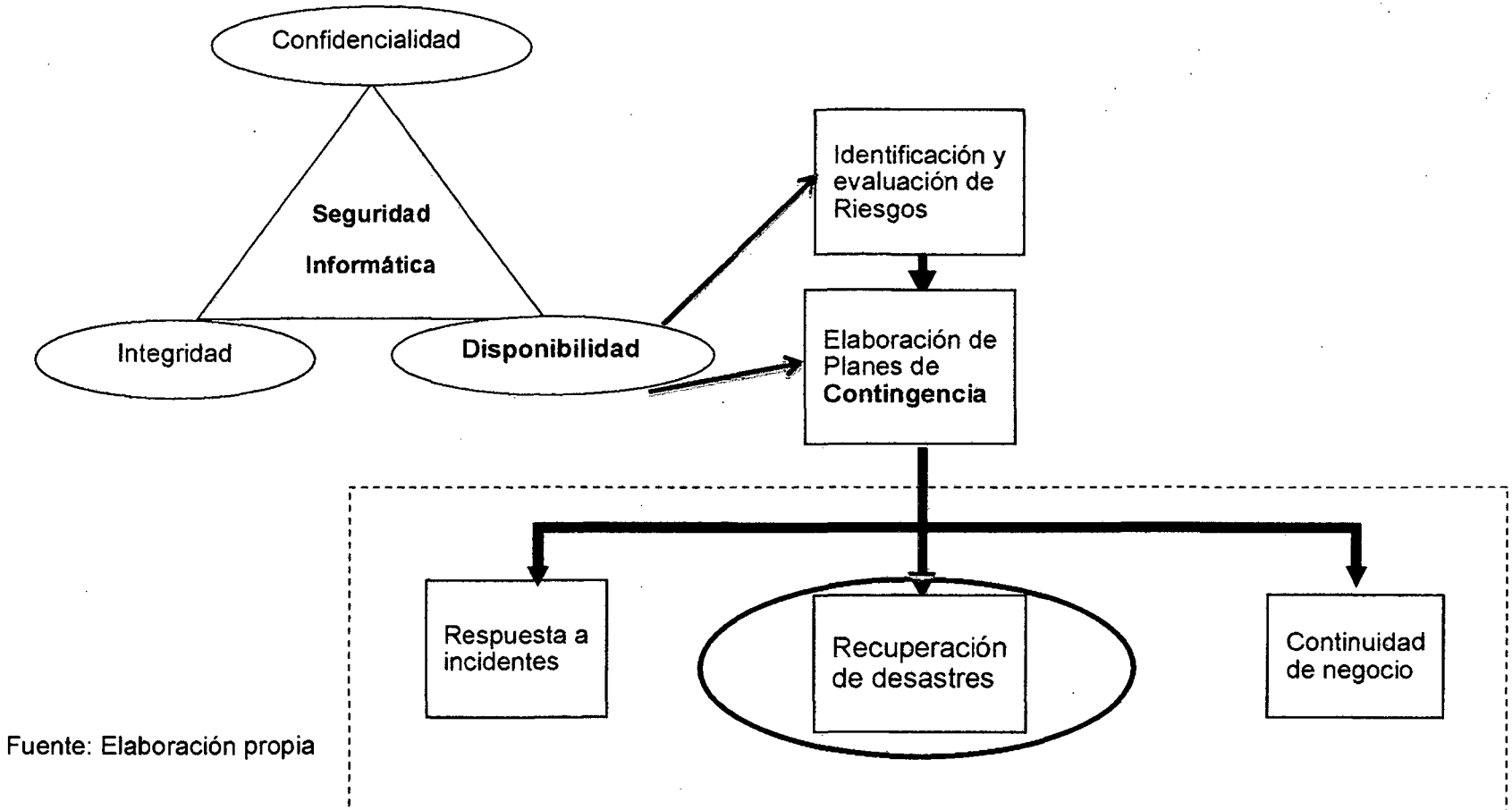
Dentro de los llamados Planes de Contingencia de negocio[22] se encuentran los 3 siguientes:

- *Plan de respuesta a incidentes (IRP).*- **se enfoca en la respuesta inmediata**, pero si el ataque escala o es un desastre, el proceso cambia a una Recuperación de desastres (PRD) y Plan de Continuidad del Negocio (BCP)
- Plan de recuperación de desastres (DRP).- **se enfoca típicamente en restaurar los sistemas en el local original después que ocurre un desastre** y así es como está cercanamente asociado con el BCP
- *Plan de Continuidad del negocio (BCP).* **BCP ocurre en forma conjunta o concurrentemente con el DRP,** cuando el daño es mayor o a largo plazo, cuando se requiere más que una simple restauración de información y recursos de información. Reestablece funciones críticas en sitio alterno.

Todos los planes de recuperación de desastres pasan por una identificación de los riesgos en los activos de información, continuando con el análisis, evaluación y tratamiento de los mismos, diferenciándose en la estrategia que se sigue para la recuperación que en algunos casos podría no necesariamente usarse un data center de contingencia propio de la organización (ver 2.2.2). Aquí reside la diferencia principal ya que los Planes de recuperación de desastres bajo el enfoque SOA obligan a tener un data center propio de contingencia con alta disponibilidad.

En el gráfico adjunto se resume el tema de investigación ubicando el Plan de recuperación de desastres como parte de la estrategia y Política de seguridad informática de un grupo empresarial:

[22] M. Whitman and Herbert Mattord; Principles of Information Security, Chapter 7. Course Technology, 2003

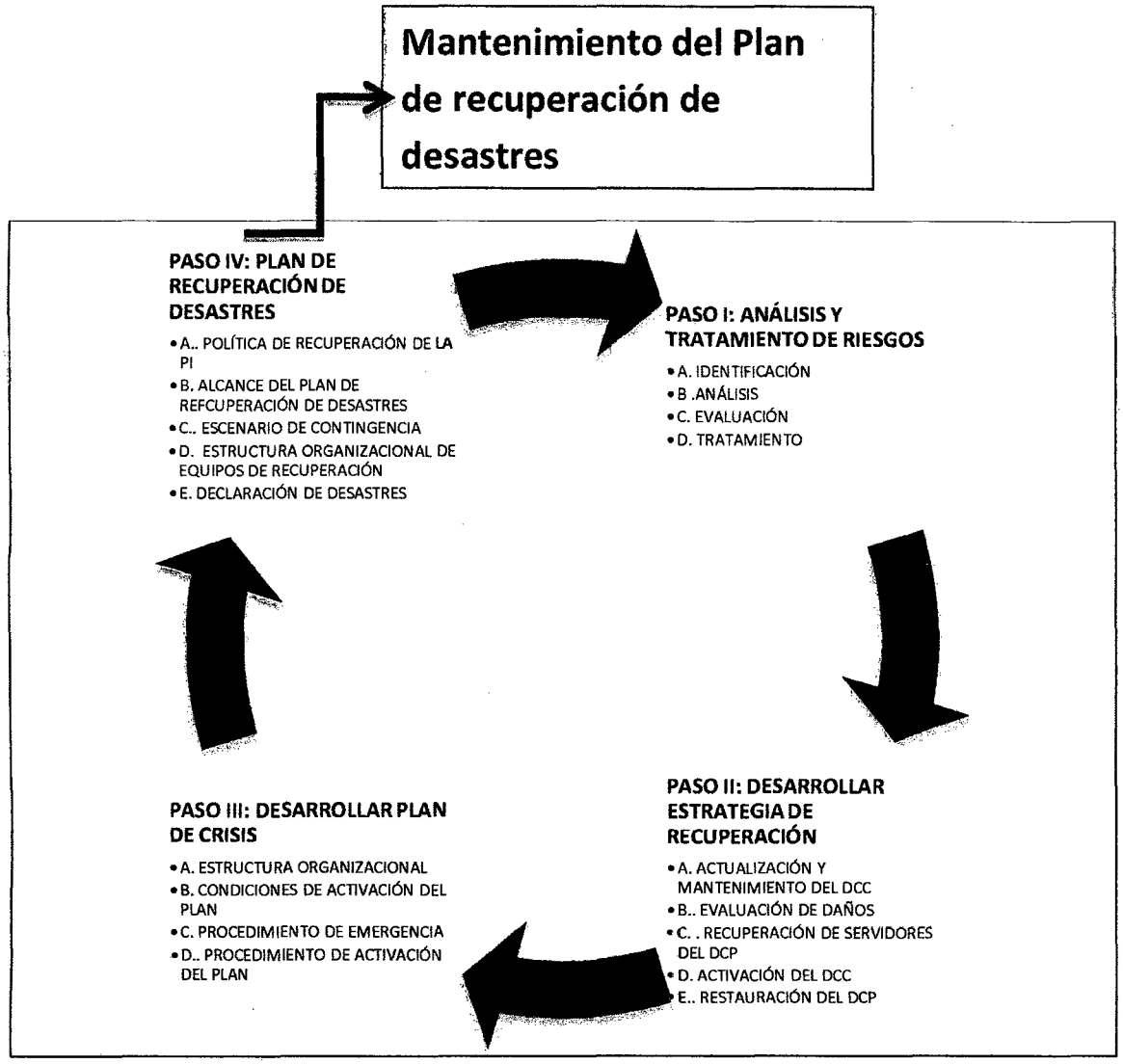


Fuente: Elaboración propia

CAPÍTULO IV

PROPUESTA O APORTE: MODELO TEÓRICO O CONCEPTUAL

Como fruto de la investigación se ha diseñado la siguiente METODOLOGÍA BASADA EN UN ENFOQUE SOA, DE UN PLAN DE RECUPERACIÓN DE DESASTRES PARA UNA PLATAFORMA DE INTEROPERABILIDAD, la cual consta de 4 pasos y cuyos aspectos resaltantes se diagraman y serán desarrollados a continuación:



Fuente: Elaboración propia

4.1. PASO I: ANÁLISIS Y TRATAMIENTO DE RIESGOS

FUNDAMENTO: El primer paso en esta metodología para poder desarrollar el PRD, bajo en enfoque SOA, es identificar los riesgos del Sistema que se pretende proteger, que en este escenario es la información transportada y generada por esta infraestructura tecnológica, con este fin se identifican los riesgos mediante entrevistas a los involucrados y consultas a los responsables de la implementación.

Posteriormente se efectúa el análisis de cada riesgo con la evaluación tanto de la probabilidad de ocurrencia como el impacto que genera la amenaza a los activos críticos.

Y por último se elabora el tratamiento de los riesgos con la finalidad de saber que alternativa de solución se va a plantear de acuerdo si se mitiga el riesgo, se evita el riesgo, se transfiere el riesgo o se acepta el riesgo determinándose en cada caso un riesgo residual el cual asume el sistema. Planteándose las acciones que deben tomarse en cada circunstancia.

Este primer paso nos sirve para inventariar los procedimientos adecuados según el ambiente en que se desenvuelve la PI.

A.- IDENTIFICACIÓN DE RIESGOS

En esta etapa se identifican los riesgos a administrar. El análisis y la evaluación de los riesgos se debe realizar en coordinación con los responsables de la Plataforma de Interoperabilidad respectiva quienes identificarán y evaluarán los riesgos principalmente de los activos críticos que soportan la Plataforma.

a) Recolección de la Información para la Identificación de Riesgos

- Entrevista.- Con la entrevista buscamos que se informen los puntos considerados como críticos o más riesgosos en la actividad diaria, así como también conocer cuáles son y han sido los eventos más riesgosos y que efectos produjeron o podrían producir, esta información la brinda el equipo de implementación de la Plataforma de Interoperabilidad respectiva.

- Consulta de Riesgos a los Responsables de la implementación.- Con el fin de reafirmar los riesgos ya determinados anteriormente se debe realizar una consulta a los responsables de la implementación para la validación de los resultados de las matrices previamente evaluadas.

B.- ANÁLISIS DE RIESGOS

Proceso que permite analizar los niveles de probabilidad de ocurrencia de evento no deseado y adverso a la PI impactando negativamente.

Los riesgos se analizarán evaluando y combinando los siguientes criterios:

- Análisis:

Probabilidad (P)

La probabilidad nos indica la posibilidad de que un riesgo se materialice. Ésta se obtiene generalmente con base en el análisis de la frecuencia de ocurrencia del riesgo en un intervalo de tiempo.

La probabilidad así estimada se puede revisar en base a los controles existentes, métodos alternativos o redundancias, y el conocimiento experto de las personas que participan en la evaluación del riesgo, todo ello actúa como amortiguadores de la probabilidad de ocurrencia.

Así mismo, la escala de probabilidades a considerar se basará en un estimado muy referencial y soportado principalmente por la experiencia de los especialistas de la PI.

La calificación de la probabilidad es la siguiente:

Como se trata de un caso nuevo, se emplearan los criterios que se listan a continuación para la asignación de probabilidades. En caso se trate de un activo o grupo de activos que no cumple con algunos de los criterios se empleará la premisa del 50 – 50 de probabilidad.

a. Componente muy utilizado

b. Controles inexistentes

c. Falta de conocimiento y experiencia usuaria.

Probabilidad (P)	Criterio	Puntuación
Muy probable	Varias veces al mes Presenta los tres criterios	5
Probable	Una vez al mes Presenta el criterio (a) y alguno de los otros 2.	4
Posible	Presenta sólo el criterio (a) o sólo los criterios (b) y (c)	3
Improbable	De uno a dos años Presenta uno de los criterios entre (b) y (c)	2
Raro	Uno cada Mas de dos años Presenta ninguno de los criterios señalados	1

Consideraciones al evaluar

Impacto (I)

El Impacto producto de la materialización de la amenaza refiere a esa pérdida tangible y/o intangible que sufre la organización y que afecta directamente a los objetivos estratégicos, misión y visión de la misma.

Impacto (I)	Criterio	Puntuación
Grave	Afecta e impacta la disponibilidad irreversiblemente	5
Severo	Afecta e impacta la disponibilidad severamente	4
Moderado	Afecta e impacta la disponibilidad parcialmente	3
Bajo	Afecta e impacta la disponibilidad mínimamente	2
Muy Bajo	No Afecta	1

Nivel de Riesgo (NR)

El Nivel de Riesgo (NR) se define como el resultado del producto de la Probabilidad y el Impacto, y considera el grado de exposición del activo y para lo cual se tendrá que tomar acciones si es que ésta cae en un nivel no aceptable por la Organización.

Nivel de Riesgo = Probabilidad x Impacto

			Impacto (I)				
			Grave	Severo	Moderado	Bajo	Muy Bajo
			5	4	3	2	1
Probabilidad (P)	Muy probable	5	25	20	15	10	5
	Probable	4	20	16	12	8	4
	Posible	3	15	12	9	6	3
	Improbable	2	10	8	6	4	2
	Raro	1	5	4	3	2	1

Nivel de Riesgo (NR)	Clase de Riesgo (CR)
15-25	**EXTREMO**
8-14	**ALTO**
4-6	**MODERADO**
1-3	**BAJO**

C.- EVALUACIÓN DEL RIESGO

La puntuación obtenida en los resultados del Nivel de Riesgo determinará el nivel de exposición al que se encuentra el proceso o activo analizado.

Este nivel de exposición se conoce como Clase de Riesgo y se clasifica, conforme se aprecia en el diagrama anterior, de la siguiente manera:

Clase de Riesgo (CR)	Criterio	Nivel de Riesgo (NR)
Extremo	Puede afectar seriamente al servicio que ofrece la Plataforma de Interoperabilidad, en términos de Indisponibilidad del Servicio ofrecido, paralización de las operaciones más allá del tiempo tolerable, estimado con juicio experto. Pérdidas económicas considerables, y daño considerable a la imagen de la institución.	15-25
Alto	Puede afectar a los niveles de operación y servicio de la PI, incumplimiento de metas, pérdidas económicas importantes.	8-14
Moderado	Afecta al cumplimiento de un objetivo secundario o de soporte. Puede afectar la operación de la PI.	4-6
Bajo	No causa un efecto considerable en la organización.	1-3

Se comparará el nivel de riesgo detectado durante el proceso de análisis de acuerdo a los criterios de riesgo establecidos previamente. El producto de la evaluación será una lista de riesgos con prioridades (de acuerdo a la clasificación del riesgo) para una acción posterior.

La acción posterior (tratamiento) a la evaluación se realizará considerando los siguientes criterios:

Clasificación	¿Se acepta?	Tratamiento	Observación
Bajo	Sí	Aceptar	Monitoreo
Moderado	Sí	Aceptar	Monitoreo
Alto	No	A definir	Ver punto 4.1.4
Extremo	No	A definir	Ver punto 4.1.4

Si un riesgo, luego de la evaluación, presenta una clasificación de Bajo o Moderado será considerado para la organización como **Riesgo Aceptado**, permaneciendo monitoreado y revisado periódicamente para verificar si permanece en su condición de aceptable.

Si un riesgo resulta clasificado como Alto o Extremo, se considerará como **No Aceptado**, debiendo ser tratado de acuerdo a lo señalado en el punto 4.1.4 (Identificar Opciones para el tratamiento de los riesgos).

D.- TRATAMIENTO DE RIESGOS

El tratamiento de los riesgos involucra identificar el rango de opciones para tratar los riesgos, evaluar esas opciones, preparar planes para tratamiento de los riesgos e implementarlos.

- **Identificar Opciones para el Tratamiento de los Riesgos**

  Luego del Análisis y de la Evaluación de Riesgos se deberán identificar las mejores opciones para tratar los riesgos.

  Para la búsqueda de controles según la estrategia que se adopte se utilizará la Norma Internacional ISO/IEC 27001 (SGSI) (Anexo A de la Norma). Dentro de las estrategias de tratamiento de Riesgos se considera lo siguiente:

  a) **Evitar el riesgo** decidiendo no proceder con la actividad que probablemente generaría el riesgo (cuando esto es práctico); o eliminando la amenaza que ocasionaría el riesgo, hecho generalmente muy costoso.

Se tendrá especial cuidado en evitar riesgos por una actitud de aversión al riesgo ya que esta actitud puede aumentar la significación de otros riesgos.

Consideraciones:

La aversión a riesgos tiene como resultado:

i) Decisiones de evitar o ignorar riesgos independientemente de la información disponible y de los costos incurridos en el tratamiento de esos riesgos.
ii) Dejar las opciones críticas y/o decisiones en otras partes;
iii) Seleccionar una opción porque representa un riesgo potencial más bajo independientemente de los beneficios.

b) Mitigar: Reducir la probabilidad de la ocurrencia

i) Condiciones contractuales;
ii) Programas de Auditoria y Cumplimiento
iii) Revisiones formales de requerimientos, especificaciones, diseño, ingeniería operaciones;
iv) Inspecciones y controles de procesos;
v) Mantenimiento preventivo;
vi) Aseguramiento de calidad, administración y estándares;
vii) Investigación y desarrollo, desarrollo tecnológico;
viii) Capacitación y Entrenamiento.
ix) Supervisión;
x) Comprobaciones;
xi) Controles técnicos.

c) **Transferir los riesgos**

Esto involucra que otra parte soporte o comparta parte del riesgo. Los mecanismos incluyen el uso de contratos, arreglos de seguros y estructuras organizacionales (si fuera el caso).

La transferencia de un riesgo a otras partes, o la transferencia física a otros lugares (centros de respaldo), reducirán el riesgo para la Compañía, pero puede no disminuir el nivel general del riesgo en su totalidad.

Como consecuencia del tratamiento de riesgos, generalmente aparecen riesgos que merecen ser tratados diferenciadamente.

a) **Tratamiento del Riesgo Residual**

Como es natural, las acciones de tratamiento del riesgo no lo eliminan completamente, siempre habrá una probabilidad marginal que generaría un riesgo residual. Es posible también que aparezcan nuevos riesgos, que se denominan riesgos secundarios. Ambos requieren de un análisis de riesgos.

Deberán ponerse en práctica planes para administrar las consecuencias de esos riesgos si los mismos ocurriesen, incluyendo identificar medios de financiar dichos riesgos.

- **Evaluar Opciones de Tratamiento de los Riesgos**

Las opciones deberán ser evaluadas sobre la base del alcance de la reducción o la eliminación del riesgo, y el alcance de cualquier beneficio u oportunidad adicional creada, tomando en cuenta los criterios de riesgo establecidos con anterioridad y valorizados en el proceso de Análisis de Riesgos. Pueden considerarse y aplicarse una cantidad de opciones ya sea individualmente o combinadas.

La selección de la opción más apropiada involucra balancear el costo de implementar cada opción contra los beneficios derivados de la

misma (costo/beneficio). En general, el costo de administrar los riesgos necesitará ser conmensurada con los beneficios obtenidos.

En alguna oportunidad será recomendable aceptar un riesgo porque el costo de su tratamiento supera los perjuicios que ocasionaría su presencia.

En función a los resultados del análisis de riesgo para la PI es preciso evaluar las opciones y/o controles para el tratamiento con base en el estándar internacional ISO/IEC 27001 (Anexo A de la Norma) o también en el ISO/IEC 27002

4.2. PASO II: DESARROLLAR ESTRATEGIA DE RECUPERACIÓN

FUNDAMENTO: En el presente paso se describe la estrategia de recuperación ante una situación de desastre de la Plataforma de Interoperabilidad que opera en el Data Center Principal (DCP).

La estrategia define las acciones ante escenarios que podrían ameritar activar el Data Center de Contingencia o en su defecto restablecer los servicios y/o componentes tecnológicos individuales de la PI.

Aquí se presentan las actividades a ejecutar en base a una secuencia lógica de decisiones dependiendo del impacto, la severidad y el tiempo que podría durar el incidente, así mismo se presenta el modelo de procedimientos técnicos a desarrollar y la lista de aplicaciones críticas que necesitan contar con su respectivo **procedimiento de recuperación**, dichos documentos deberán ser desarrollados por los especialistas de las plataformas.

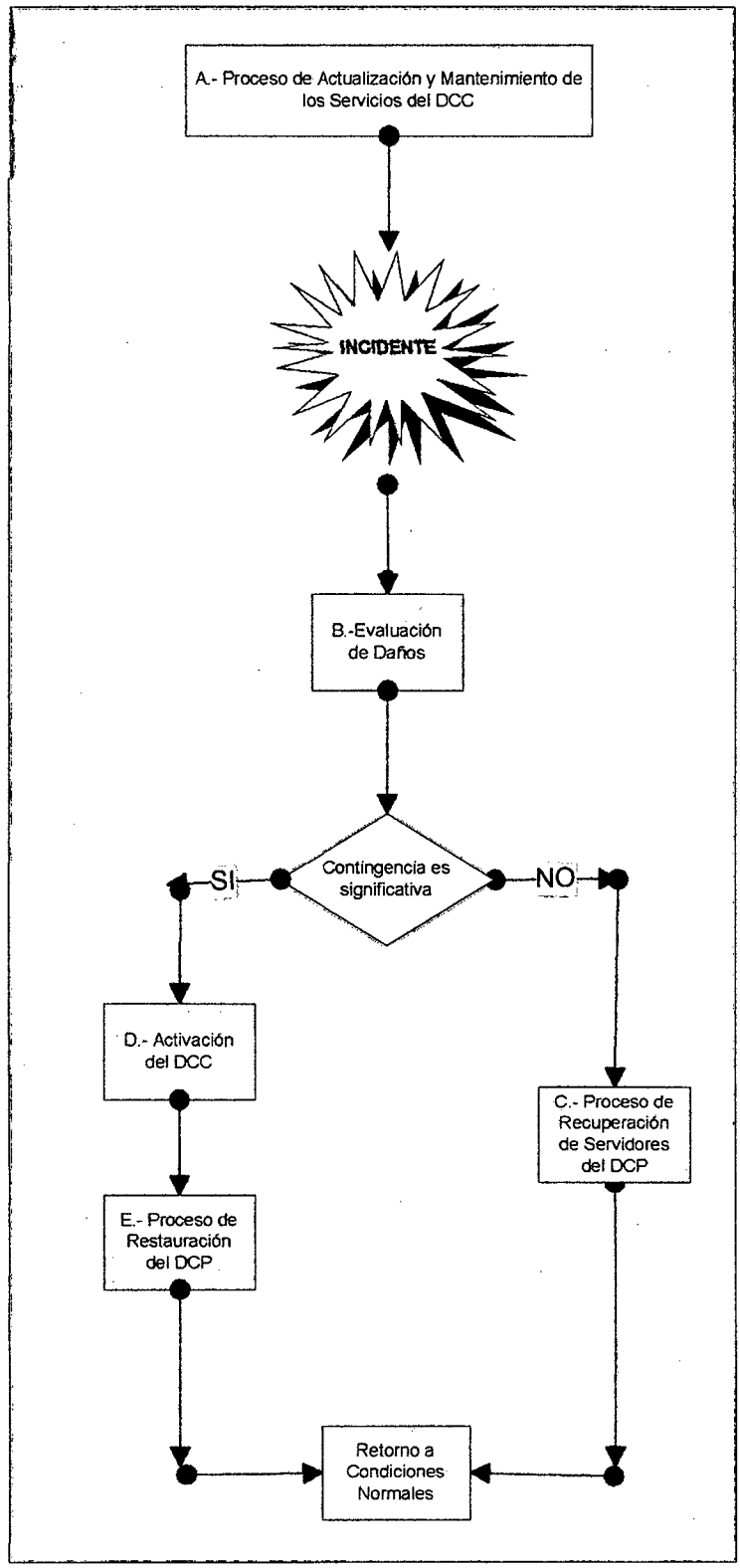
El paso II se justifica ya que se debe tener claramente en el DRP las actividades más importantes que deben tomarse en cuenta durante la ocurrencia del desastre de forma tal que no se pierda tiempo en analizarlas al momento de su ocurrencia.

NOTA: El escenario de Desastres que activará el Plan de Recuperación y el Data Center de Contingencia se cumplirá con base en lo definido en la Política del Plan: *"El Plan de Recuperación de Desastres se ejecutará únicamente cuando una*

indisponibilidad severa y por tiempo prolongado afecte negativamente el servicio en el Data Center Principal"

ESTRATEGIA DE RECUPERACIÓN

A continuación se presenta la estrategia de recuperación definida según el escenario que define la Política y el camino a adoptar, este esquema se presenta como actividades de antes, durante y después de un desastre, las mismas que van acompañadas de acciones a ejecutar.



Fuente: Elaboración propia

Desarrollo de Estrategia de Recuperación

La estrategia de recuperación ante una contingencia, y con mayor razón ante un desastre, empieza con un conjunto de acciones previas a cualquier tipo de contingencia; continúa con la planificación de un conjunto de acciones durante la contingencia y finaliza con la planificación de las acciones que nos permitirán retornar a la condición de normalidad cuando se ha superado la contingencia. Veamos cada una de estas etapas.

A.- PROCESO DE ACTUALIZACIÓN Y MANTENIMIENTO DE LOS SERVICIOS DEL DATA CENTER DE CONTINGENCIA (DCC)

a) Objetivos

Este proceso tiene por objeto asegurar el correcto funcionamiento del DCC antes de cualquier desastre, siendo prioridad ***mantener sincronizados los servicios definidos en el DCC con el DCP.***

- Mantener actualizados los sistemas de información con las últimas versiones en producción.
- Mantener actualizada la información (data) de los aplicativos de producción en los equipos de contingencia de la PI.
- Las Plataformas que soportan las Aplicaciones críticas según el análisis de Impacto deberán ser actualizadas con las versiones de los sistemas operativos de acuerdo a los servicios que se están corriendo de tal manera que las aplicaciones funcionen correctamente.
- Asegurar los esquemas de producción y de contingencia de las Telecomunicaciones con mantenimientos preventivos, respaldos de las configuraciones y pruebas periódicas que aseguren la disponibilidad del servicio en el tiempo definido para el Punto de Recuperación Objetivo. Las pruebas periódicas deben estar definidas en la política del Plan de Recuperación de Desastres.

b) Responsabilidades

Función	Descripción / Responsabilidad
Administrador del Plan de Recuperación de TI de la PI	Es el "líder" del equipo y principal responsable del Plan de Recuperación de Desastres de la PI, encargado de asegurar que el DCC siempre se encuentre operativo y sincronizado. Así como de realizar los controles necesarios para verificar que el plan se cumpla. Deberá realizar las coordinaciones con personal del área, proveedores y usuarios.
Administradores de Plataformas y Recuperación de Aplicaciones de la PI.	- Realizar copias de respaldo en el DCP - Realizar el proceso de 'restore' de información en el DCC con el objetivo de asegurar que los respaldos funcionen correctamente, con base a un cronograma de pruebas - Mantener nivelados los servidores del DCC con los servidores del DCP, actualizando las aplicaciones en el DCC al momento de realizar los pases a producción.

c) Descripción

Mantener actualizados los sistemas de información con las últimas versiones de Producción. Esto incluye actualizaciones de los sistemas o nuevas versiones.

d) Controles

Luego de ejecutado los respaldos, se deberá verificar que la restauración se realice en forma correcta. Si hubiera algún problema, anomalía u observación al proceso, ésta debe registrarse a fin de identificar posibles errores que podrían afectar severamente.

e) Resultado de la ejecución de este procedimiento

La actualización de los servidores de Contingencia permite que el DCC tenga disponible sistemas de información de la PI

B.- PROCESO DE EVALUACIÓN DE DAÑOS

Ante algún evento de Desastres que afecte la disponibilidad de los sistemas de la PI, se deberán efectuar los esfuerzos para proveer la operatividad de los Servicios de Tecnología de Información en el menor tiempo e impacto posible.

Este procedimiento comprende las siguientes actividades:

a) Notificación del Evento

La responsabilidad de esta actividad está asignada al Administrador del Plan de Recuperación de la PI, en caso de ausencia, otro Administrador de la Plataforma que se encuentre en operación o de turno se encargará de esta actividad.

Las acciones a ejecutar son:

- Evaluar inmediatamente el impacto del evento y adoptar las medidas de emergencia necesarias.
- Notificar al **Administrador de la Plataforma de Interoperabilidad (PI)** sobre el evento que ha afectado la operatividad del Data Center Principal (DCP)
- Averiguar sobre las fuentes que ocasionaron el evento. Si fuese un evento interno se deberá contactar con la persona de soporte apropiado (Administración) para obtener un primer diagnóstico.
- Notificar a la Administración de la PI, los detalles del evento, la fuente, el primer diagnóstico y las acciones preliminares.
- Registrar las acciones efectuadas en el formato **"Hoja de Control de Acciones ante Contingencias"** (Anexo 1).

- Adicionalmente, se utilizará el formato **"Notificación del Evento"** (Anexo 2), que va a servir para el proceso de recuperación del DCP.

b) Evaluación de Daños

La responsabilidad de esta actividad está asignada al Administrador de la PI, en caso de ausencia de éste, otro funcionario que se encuentre en operación o de turno se encargará de esta actividad.

Las acciones a ejecutar son:

- Dependiendo del evento se coordinará con los responsables (personal interno o externo) para evaluar los daños en la infraestructura de cómputo. Esta actividad deberá realizarse al más breve plazo de ocurrido el evento.
- Para esta actividad, si la situación lo permite, se tendrá un reporte con los detalles del evento sobre las Aplicaciones críticas de la PI
- El Informe de Evaluación de Daños servirá para definir los procedimientos de recuperación del procesamiento computarizado. Se deberá estimar el tiempo necesario para recuperar o reemplazar los recursos afectados.
- Dependiendo del tiempo de recuperación o reemplazo del recurso afectado se deberán evaluar las posibilidades de recuperar la operatividad del recurso afectado.
- El responsable de la PI deberá identificar en qué escenario de contingencias se encuentra para activar la contingencia en el Data Center de Contingencia, según Política del plan de recuperación de la plataforma de interoperabilidad: *"El Plan de Recuperación de Desastres se ejecutará únicamente cuando una indisponibilidad severa y por tiempo prolongado afecte negativamente el servicio en el Data Center Principal"*

De acuerdo a lo recabado en el análisis de impacto tenemos los siguientes escenarios:

Escenario 1:	No amerita el uso y activación del DCC, debido a que los servidores, equipos y/o servicios sufren una indisponibilidad parcial y que no afecta a todo el servicio de la PI, por lo tanto las acciones y/o procedimientos se tendrán que orientar específicamente a recuperar el equipo, servicio y/o aplicación de la PI afectado.
Escenario 2:	Amerita uso y activación del DCC debido a que el incidente es catalogado como indica la Política y se activa el procedimiento de Activación de DCC, operando y entregando el servicio de la PI desde el Data Center de Contingencia hasta recuperar la operatividad del Data Center Principal.

C.- PROCEDIMIENTO DE RECUPERACIÓN DE SERVIDORES DEL DATA CENTER PRINCIPAL

Procedimiento de Recuperación de los Servidores de la PI
Objetivo Recuperar la operatividad de los servidores de aplicaciones, base de datos y servicios que brinden soporte a la Plataforma de Interoperabilidad (PI)); los mismos que se encuentran distribuidos en los distintos servidores y aplicaciones.
Premisa: Este procedimiento se iniciará sólo si durante la evaluación del daño se identificó que la recuperación podría realizarse con los especialistas técnicos del Data Center Principal, es decir no se activa el Plan de Recuperación de Desastres.
Responsabilidad Los responsables de este procedimiento son los administradores de las plataformas y

comunicaciones que soportan el servicio de la PI.

Procedimiento

1. El responsable de Administración del Plan de Recuperación, con base al informe de diagnóstico, definirá las acciones de recuperación.

2. El responsable de Administración del Plan de Recuperación convocará a los especialistas necesarios para solucionar el problema.

3. Los sistemas antes mencionados se encuentran instalados en el Data Center Principal contando con una réplica para el caso de contingencia, ubicada en el Data Center de Contingencia.

Documentación de Incidentes:

4. Se deberá documentar cada incidente ocurrido, registrando características, soluciones, percances, etc. para tener una base de datos de incidentes y que pueda ser utilizada en futuros incidentes.

El responsable del Área de TI deberá completar y firmar la **"Hoja de Control de Acciones de Contingencias"** (Anexo 1) con el detalle de los acontecimientos tales como: fecha, horas, descripción del evento, tiempos de inactividad, uso de procedimientos, respuesta de los clientes, coordinaciones internas, otros.

La "Hoja de Control de Acciones de Contingencias" deberá ser remitida al responsable de la PI en un plazo no mayor de 48 horas luego de cerrada las acciones de contingencias, indicando las causas, impacto y acciones de solución adoptadas en el evento.

Procedimientos de Recuperación de los Servidores Críticos de la PI

<table>
<tr><td colspan="2">Procedimiento de Recuperación de Servidor XXXX</td></tr>
<tr><td>Código: PROC_SRV001</td><td>Responsable: Administrador de Servidores</td></tr>
<tr><td>Nombre Servidor:</td><td>Ubicación: DCP</td></tr>
<tr><td>Plataforma:</td><td>Aplicaciones: Listar las aplicaciones que se encuentra en el servidor</td></tr>
<tr><td colspan="2">Características Técnicas:

Aquí se colocará las características técnicas de los equipos tecnológicos</td></tr>
<tr><td colspan="2">Detalle de Recuperación:

Falla de Hardware:

- Hacer un diagnóstico rápido de la posible falla. Si de acuerdo a este se estima que el servidor no podrá estar activo durante un tiempo determinado (estimado por juicio experto), se procederá con los pasos detallados a continuación.
- Se colocará el detalle de los pasos a seguir cuando ocurre un incidente en el hardware del Servidor en mención

Falla de Software Base y/o Aplicaciones:

- Hacer un diagnóstico rápido de la posible falla. Si de acuerdo a este se estima que el servidor no podrá estar activo durante un tiempo determinado (estimado por juicio experto), se procederá con los pasos detallados a continuación.

- Se colocará el detalle de los pasos a seguir cuando ocurre un incidente en el software base y/o aplicación en mención.</td></tr>
</table>

D.- ACTIVACIÓN DEL DATA CENTER DE CONTINGENCIA (DCC)

a) Objetivo:

Asegurar la continuidad operativa técnica de la PI luego de ocurrido un desastre, mediante la apertura y activación del Data Center de Contingencia previo resultado de evaluación de los daños.

Procedimiento de Activación del Data Center de Contingencia (DCC)
Premisa El uso de del Data Center de Contingencia se activará y atenderá la producción en totalidad en caso se cumpla el escenario de DESASTRE del DCP, el DCC se ivará cumpliendo el tiempo establecido de recuperación.
Objetivo El objetivo de este procedimiento es activar el(los) servidor(es) de red de ntingencia ubicado en una sede alterna.
Responsables: Responsables de las Plataformas tecnológica de la PI
Detalle de Actividades **Acciones de Coordinación** 1. El Líder del Comité será responsable de coordinar con los diferentes equipos-rsonal la activación de los equipos tecnológicos del DCC. 2. El Líder del Comité coordinará los accesos y facilidades para el traslado de los ministradores de las plataformas de contingencia. 3. El Líder del Comité será responsable de coordinar con la empresa de ecomunicaciones la ejecución del procedimiento de activación del enlace de municaciones para brindar el servicio por este medio alterno. **Acciones de Activación/Validación**

4. Los administradores de las plataformas deberán revisar, verificar y ejecutar las ividades de validación de operatividad de las plataformas que operaron en ntingencia y en alta disponibilidad.

5. Los administradores de las plataformas deberán validar los servicios de las icaciones que brinda la PI

6.- El administrador de las telecomunicaciones deberá validar el servicio de ntingencia que entrega el enlace alterno del DCC..

7. Verificar que todos los servicios se encuentran activos coordinando y validando n los usuarios de la PI la operatividad normal del servicio.

E.- PROCESO DE RESTAURACIÓN DEL DC PRINCIPAL

a) Objetivo:

Asegurar la restauración del DCP luego de haber superado el desastre y dadas las condiciones necesarias para el retorno de las operaciones en las instalaciones del DCP.

b) Responsabilidades

Función	Descripción
Administrador del Plan de Recuperación de TI	Coordinará todas las acciones necesarias con el equipo de TI, proveedores y personal involucrado para poner operativo el Data Center Principal.

b) Definición

Este procedimiento comprende la inspección al Data Center Principal, el encendido del DC Principal y prueba de servicios, la recuperación de Hardware, Software de Base y Aplicaciones, la sincronización del DC principal y la reapertura del DC principal. En el 'Procedimiento de Restauración del DC Principal' se encuentra el detalle del proceso.

c) Controles

Se ha establecido en el proceso tareas de verificación de responsabilidad del Administrador del Plan de Recuperación de TI.

d) Resultado

El Data Center Principal operativo para su utilización por los usuarios de la PI.

Procedimiento de Restauración del DC Principal:

Procedimiento de Restauración del Data Center Principal			
N°	RESPONSABLE	ACTIVIDAD	
	Inspección del DC Principal		
1	Administrador del Plan de Recuperación de TI	INSPECCIONA	El DC principal para verificar que la infraestructura física presenta las condiciones técnicas necesarias para el retorno de las operaciones. Se deberá coordinar con los diferentes proveedores la revisión de instalaciones eléctricas, cableado, aire acondicionado e infraestructura adicional necesaria.
2	Administrador del Plan de Recuperación de TI	PREPARA	Los informes técnicos que garanticen que el DC principal puede estar operativo nuevamente. Se comunicará a los responsables de la PI que reiniciará sus operaciones normalmente, indicando el día y la hora, así como el tiempo estimado de sincronización y puesta en producción.
	Reinicio de operaciones del DC Principal y prueba de servicios		

3	Administradores de las Plataformas Tecnológicas.	PRUEBA	Los equipos, que consiste en: Encendido de los servidores, equipos de Comunicaciones, servidores y Aplicaciones que necesita la PI. Se deberá verificar el estado de todos los equipos encendidos diagnosticando su estado. Se deberá verificar la operatividad de las telecomunicaciones.
4	Administrador del Plan de Recuperación de TI	ELABORA	Inventario de equipos que presentaron problemas y evaluar las alternativas de solución a los mismos. Se comunicará a los responsables de la PI el estatus de las operaciones y las posibles *consecuencias* de tal situación.
	Recuperación de Hardware y Software de Base		
5	Administrador del Plan de Recuperación de TI	COORDINA	Con los responsables de la PI y las áreas involucradas la reparación, levantamiento y/o adquisición de hardware y software dañado. El Administrador del Plan de Recuperación de TI deberá de contar con la relación de

			proveedores, así como con los contratos vigentes tanto de mantenimiento como adquisiciones.
6	Administrador del Plan de Recuperación de TI	COMUNICA	A la Dirección sobre el impacto de los daños encontrados y los tiempos estimados de solución de problemas.
	- ***Sincronización del DC principal*** - ***Se realiza después de haber superado los problemas de hardware y software identificados.***		
7	Administrador del Plan de Recuperación de TI	SINCRONIZA	La data de los sistemas de información y de los servicios que estuvieron operativos en el DCA durante su funcionamiento, se debe tener en cuenta lo siguiente: Determinar: Fase 1: Definido este como la fecha y hora en cual se tiene data confiable en el servidor de datos en su defecto el último respaldo disponible. Fase 2: Definido este como la fecha y hora desde que se comenzó a operar el DCC ingresando data en el servidor de datos. Determinar el "bloque de información" que no se encuentra en ningún almacenamiento

			producto del desastre presentado. El Administrador del Plan de Recuperación de TI, después de evaluar las Fases 1 y 2, la información faltante, deberá, ordenar la data de los respaldos necesarios y disponer de los medios necesarios para la carga de la información faltante en el equipo de producción del DC Principal.
8	Administrador del Plan de Recuperación de TI	DEFINE	Para cualquier otro servicio no establecido explícitamente en este documento y que se haya implementado en el DCC durante su operación, el método adecuado de sincronización de tal manera que se garantice la continuidad de las operaciones en el momento de la reapertura del DC Principal.
	Reapertura del DC Principal		
9	Administrador del Plan de Recuperación de TI	VERIFICA	Que existan las condiciones requeridas para el reinicio de operaciones, para lo cual deberá tomar en cuenta lo siguiente: • Todos los servicios han sido probados • La información se encuentra en los equipos de producción del DC Principal

			• Las Telecomunicaciones han sido restablecidas en el DCP.
10	Administrador del Plan de Recuperación de TI	COMUNICA	A los responsables de la PI sobre la situación del DC Principal y la restauración de los servicios.
11	Administrador del Plan de Recuperación de TI	COORDINA	Con los responsables de la PI la reapertura del DC Principal y la puesta en servicio post recuperación y retorno a operaciones normales.
12	Administrador del Plan de Recuperación de TI	COMUNICA	La reapertura del DC Principal a los usuarios de la PI dando por superada la situación presentada por el desastre.
13	Administrador del Plan de Recuperación de TI	EVALUA	Conjuntamente con el equipo que administra la plataforma de la PI todas las acciones realizadas durante la situación vivida como consecuencia del desastre y levantar el acta de "*lecciones aprendidas*" que servirá como "*feedback*" y mantenimiento del presente plan.

4.3. PASO III: DESARROLLAR EL PLAN DE CRISIS

FUNDAMENTO: El objetivo de cada paso es proporcionar los mecanismos para establecer las comunicaciones efectivas y eficientes entre los diferentes equipos y proveedores que participan en la recuperación de las operaciones de la Plataforma de Interoperabilidad (PI) en una situación de caos, contingencia y stress.

Aquí se proporcionará el esquema organizacional que va a dirigir las acciones y brindar las pautas en una situación de contingencia. Así mismo se presenta las actividades de los procedimientos de activación y emergencia.

En este paso en forma similar al paso II, la explicación de su elaboración es evitar justamente el caos y el stress que significa cuando sucede un evento (desastre) de esta naturaleza y no saber cómo actuar, teniendo el gran riesgo de ejecutar procedimientos o acciones inseguras que puedan dañar de alguna manera el sistema que deseamos proteger siendo el remedio peor que la enfermedad.

A.- ESTRUCTURA ORGANIZACIONAL

COMITÉ DE CONTINGENCIA Y RECUPERACIÓN

El Comité de Contingencia y Recuperación está conformado por parte del personal que administra la PI, el cual tiene por finalidad participar en el Plan de Recuperación de Desastres y poder llevar adelante los procedimientos establecidos en éste.

Las actividades del Comité de Contingencia y Recuperación no se limitan al momento de la ocurrencia de un desastre sino que su labor debe desarrollarse antes, durante y después de un incidente severo (Desastre).

a) Tareas:

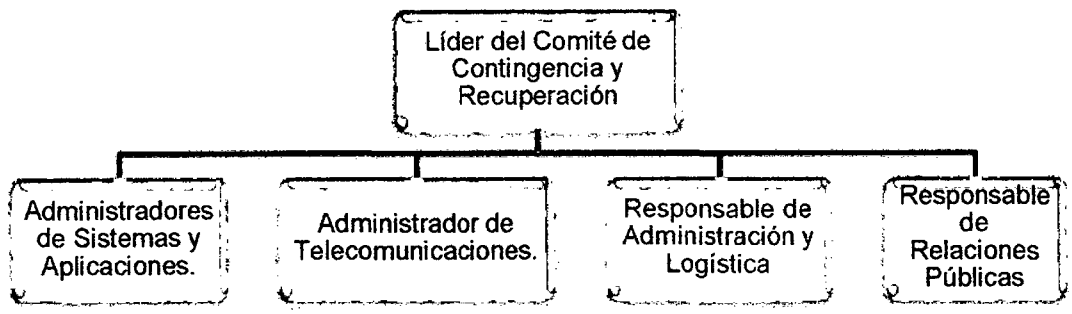
Las tareas generales que tiene el Comité de Contingencia y Recuperación son:

- Coordinar las acciones a tomar con todas las instancias correspondientes.

- Conseguir los recursos necesarios para reiniciar los sistemas y las comunicaciones críticas.
- Coordinar los traslados de equipos y recursos necesarios para la operación en contingencia.
- Notificar a proveedores e instituciones el esquema de atención a brindar mientras dure la contingencia.
- Coordinar y restablecer los sistemas y las telecomunicaciones.
- Mantener actualizado el Plan de Recuperación de Desastres.
- Realizar las pruebas de recuperación de los sistemas (plataformas tecnológicas) y las comunicaciones en forma periódica.

b) Organización.

En el diagrama se muestra la organización del Comité de Contingencia y Recuperación de la Institución. Este comité se encargará de trabajar de manera preventiva el esquema y estrategia de recuperación, tomará acciones y decisiones dependiendo de la situación de desastre y se encargará de recuperar y restablecer las operaciones y atención de los servicios brindados por la Plataforma de Interoperabilidad.



Organización del Comité de Contingencia y Recuperación

c) Roles y Responsabilidades

1. Líder del Comité

Antes del evento:

a) Designar a las personas responsables que se encargarán de actualizar periódicamente el Plan de Recuperación de Desastres y la distribución controlada de sus copias.
b) Supervisar el entrenamiento y pruebas establecidas para contingencias.
c) Velar por el cumplimiento de las medidas de seguridad de control de accesos, respaldo de información y medidas de seguridad de los Centros de Cómputo Primario y de Contingencia.
d) Establecer convenios de reposición de equipo crítico de sistemas y comunicaciones en coordinación con el responsable de Administración y Logística.

Durante y Después del evento:

a) Coordinar la activación e implementación del Plan de Recuperación de Desastres.
b) Comunicar la ocurrencia del siniestro e informar el impacto sobre la organización.
c) Mantener informados a la Gerencia General y al Comité Corporativo de las actividades de contingencia y recuperación.
d) Supervisar a los Administradores de sistemas y al responsable de redes y comunicaciones en el momento de la restauración de los sistemas y las comunicaciones.
e) Priorizar el orden de comunicación con cada uno de los equipos de recuperación.
f) Comunicar al responsable de Administración y Logística los contratos o convenios a ejecutarse y la adquisición de equipos necesarios.

g) Asignar nuevas funciones a cada miembro del equipo en caso sea necesario.
h) Elaborar el informe de la evaluación de daños.

2. Responsable de Administración y Logística

Antes del evento:

a) Coordinar el abastecimiento de los recursos de prevención con el Líder del Comité y el responsable de redes y comunicaciones.
b) Mantener vigente los contratos de reposición del equipo de sistemas y comunicaciones, coordinando con el Líder del Comité.
c) Verificar que se mantiene actualizada la Lista de Proveedores, en coordinación con el Responsable de Redes y Comunicaciones y los Administradores de Sistemas y Aplicaciones.

Después del evento:

a) Coordinar con la Oficina de Sistemas la reposición de los equipos de sistemas y comunicaciones de acuerdo a los contratos pactados.
b) Notificar a los proveedores, los equipos requeridos si no fuera hecho directamente por Sistemas.
c) Efectuar las compras de los equipos y repuestos necesarios para el restablecimiento de los sistemas y comunicaciones.
d) Coordinar el pago a proveedores en el caso de servicios o compra de equipos.
e) Administrar los gastos de contingencia.

3. Responsable de Relaciones Públicas

Antes del evento:

a) Definir un esquema de comunicación de forma que la Institución pueda afrontar la ocurrencia de una contingencia.

b) Enmarcar este esquema de comunicación dentro de la normatividad institucional y las posibles contingencias.

Durante y después del evento:

a) Emitir información y respuesta a los medios de comunicación, clientes, usuarios, proveedores e instituciones públicas la situación de la Institución y los planes para su normal operatividad.
b) Informar los locales y teléfonos alternos a donde los clientes, proveedores y público puedan encontrar información mientras dure la contingencia.
c) Coordinar el personal y recursos necesarios para el servicio de atención a clientes, proveedores y público.
d) Mantener la imagen de seriedad y cumplimiento de la Institución.

4. Administrador de Redes y Comunicaciones

Antes del evento:

a) Verificar que se mantienen actualizados los diagramas de los Data Centers, los Diagramas de Red, las especificaciones de hardware, la configuración de los equipos y los procedimientos de recuperación.
b) Monitorear la red y definir medidas preventivas para minimizar o evitar las contingencias de comunicaciones.
c) Verificar que se ejecutan los procedimientos de respaldo de información, en cumplimiento a las políticas.
d) Participar en las pruebas del Plan de Recuperación de Desastres.

Después del evento:

a) Apoyar en la tarea de evaluación preliminar de daños.
b) Examinar físicamente los equipos de sistemas y comunicaciones de los Data Centers.
c) Preparar un inventario del equipo afectado.

d) Instalar o supervisar el cableado para las comunicaciones, en caso sea necesario.
e) Restaurar los equipos y sistemas de comunicaciones.
f) Realizar pruebas integrales de los equipos y aplicaciones hasta descartar la presencia de fallas y/o errores.
g) Coordinar con el Líder del Comité para el reinicio de operaciones.
h) Coordinar con los Administradores de Sistemas y Aplicaciones el soporte a los usuarios y clientes de la PI.
i) Coordinar con las empresas que dan soporte a las funciones críticas de la Oficina de Sistemas para la activación del servicio.
j) Colaborar en la elaboración del Informe de Evaluación de Daños.

5. Administradores de Sistemas y Aplicaciones.

Antes del evento:

a) Verificar que se mantiene actualizado el Inventario de Sistemas y Aplicaciones.
b) Participar en el mantenimiento del Plan de Recuperación de Desastres.
c) Coordinar periódicamente que se cumplan en forma apropiada y completa los procedimientos de respaldo de los sistemas a su cargo.
d) Participar en las pruebas del Plan de Recuperación de Desastres.

Después del evento:

a) Apoyar en la tarea de evaluación preliminar de daños.
b) Verificar si es posible recuperar datos de los equipos. En caso contrario, localizar las copias del software y datos que fueron resguardadas externamente.
c) Coordinar el retiro de los medios de respaldo del local de resguardo exterior.

d) Apoyar en la restauración de las bases de datos y los programas ejecutables de los servidores.
e) Apoyar en las pruebas integrales de los equipos y aplicaciones hasta descartar la presencia de fallas y/o errores.
f) Documentar y reportar los errores y/o fallas encontrados.
g) Coordinar el soporte a los usuarios de la PI.
h) Colaborar en la elaboración del Informe de Evaluación de Daño

B.- CONDICIONES DE ACTIVACIÓN DEL PLAN

El Plan de Recuperación de Desastres puede ser activado por el Líder del Comité de Contingencia y Recuperación en caso de cumplirse algunas de las siguientes condiciones:

Condiciones de Contingencia	Escenario a Recuperar
a) Presencia de un siniestro severo que interrumpa la normal operación de los sistemas y servicios informáticos. **b) Daños causados por un siniestro que no permitan la ejecución normal de los sistemas críticos.** **c) Que las instalaciones físicas del Data Center Primario haya sufrido un deterioro tal que no sea posible ejecutar ningún proceso.**	Destrucción de Data Center
d) Caída inesperada de un servidor crítico de la PI **e) Inadecuada restauración de copias de respaldo.**	Falla de servidores
f) Caída inesperada de un equipo central y crítico de comunicaciones de la PI **g) Imposibilidad de contar con comunicaciones entre el Data Center Primario y el de Contingencia**	Falla de telecomunicaciones

h) Corte de energía eléctrica en el Data Center Principal. **i) UPS no funciona cuando se pierde energía eléctrica y el Grupo Electrógeno no enciende.**	Falla de energía eléctrica

C.- PROCEDIMIENTO DE EMERGENCIA

Considerando que el principal objetivo es salvaguardar la integridad física de los trabajadores y personas que se encuentren en las instalaciones de la Institución, en caso de siniestros que pongan en riesgo la vida del personal (Ejemplo: incendios, terremotos, atentados destructivos), antes de activar el proceso de contingencia de los sistemas y servicios informáticos se debe ejecutar el Procedimiento de Emergencia.

Procedimiento de Emergencia

N°	Actividad	Responsable
1	Identificar positivamente el siniestro, dando aviso al personal que se encuentra de labor en la Oficina – Data Center.	Personal presente en la oficina / Data Center al momento del siniestro
2	Si observa fuego o humo dentro de la sala de cómputo, haga lo siguiente: ▪ Active la alarma contra incendios. ▪ Si es seguro, utilice los extintores. No trate de apagar el fuego solo.	Personal presente en la oficina / Data Center al momento del siniestro.
3	Ante la presencia de un terremoto y si el tiempo lo permite, haga lo siguiente: ▪ Apague los servidores y equipos. ▪ Corte el fluido eléctrico.	Personal presente en la oficina / Data Center al momento del siniestro.
4	Prestar ayuda a otras personas presentes en el área siniestrada.	Personal presente en la oficina / Data Center al momento del siniestro.

N°	Actividad	Responsable
5	Determinar si es necesario evacuar el lugar del siniestro.	Personal presente en la oficina / Data Center al momento del siniestro.
6	Dar aviso del siniestro a los bomberos, seguridad del edificio, personal médico, o quien corresponda.	Personal presente en la oficina / Data Center al momento del siniestro.

D.- PROCEDIMIENTO DE ACTIVACIÓN DEL PLAN

La activación del Plan de Recuperación de Desastres de la PI significa que se ejecutan las actividades de evaluación de daño, reunión del comité de Contingencia y Recuperación de la PI y, sobre la información producto del incidente, se toma una decisión, esta podría ser recuperarse en el mismo Data Center Primario o activar el Data Center de Contingencia y recuperar los servicios de la PI cumpliendo los tiempos de recuperación establecidos.

Procedimiento de Activación

N°	Actividad	Responsable
1	Contactar al Líder del Comité de Contingencia y recuperación.	Personal presente en las oficinas al momento de la contingencia
2	Identificar, si es posible, la causa de la discontinuidad de los sistemas y servicios informáticas.	Personal presente en las oficinas al momento de la contingencia o Líder del Comité de Contingencia y Recuperación
3	Evaluar las condiciones presentadas y decidir si se activa el Plan de Recuperación de Desastres	Líder del Comité de Contingencia y Recuperación
4	En caso de activación: Informar al Comité de Contingencias y Recuperación la ejecución del Plan de Recuperación e indicar a los integrantes de los equipos la ejecución de sus Procedimientos Técnicos a fin de recuperar la operatividad en el menor tiempo posible (RTO)..	Líder del Comité de Contingencia y Recuperación

4.4. PASO IV: PLAN DE RECUPERACIÓN DE DESASTRES

FUNDAMENTO: El Plan de Recuperación de Desastres describe el proceso de planeación, desarrollo, prueba e implantación de procesos y procedimientos de recuperación que servirá en caso de una posible contingencia que pueda presentarse en el Data Center donde opera la Plataforma de Interoperabilidad.

Tomando en consideración el diseño de procedimientos para las pruebas de Contexto, de Organización y de Operación las que deben ser ejecutadas y verificadas para comprobar la validez del PRD. Este paso busca asegurar la reanudación eficiente y efectiva de los Servicios de TI en el menor tiempo e impacto posible.

Los documentos que conforman el Plan de Recuperación de desastres son los siguientes:

- Plan de Recuperación.
- Plan de Gestión de Crisis
- Procedimientos de Recuperación.

Los objetivos que busca cumplir el Plan de Recuperación de Desastres, es lograr contar con un esquema organizado, viable y ágil en el momento que este documento sea requerido para enfrentar una situación de desastre.

Los principales objetivos del Plan son los siguientes:

- Documentar las actividades de recuperación de la operatividad y el servicio ante un incidente o evento severo.
- Descripción de la estructura organizacional necesarios para restaurar las operaciones en el Data Center de contingencia.
- Documentar los Procedimientos de recuperación necesaria e indispensable para recuperar las operaciones y el servicio en el tiempo definido.
- Cumplir con el tiempo objetivo de recuperación definido.
- Familiarizar a los equipos de recuperación con pruebas de contingencia periódicas y de escenarios cercanos a la realidad.

Su justificación se da obviamente por ser el documento que consolida las buenas prácticas anteriores y que está preparada para ser ejecutada y verificada en cualquier momento, siendo pues el compendio de todos los pasos anteriores los cuales deben documentarse y establecerse posiblemente en su primera versión, ya que éste puede ir variando en el tiempo según las revisiones periódicas recomendadas para mantener su actualización.

A.- POLÍTICA DE LA RECUPERACIÓN DE LA PLATAFORMA DE INTEROPERABILIDAD

Las Políticas que rigen el presente plan y bajo el marco en el cual se desarrollará y ejecutará el Plan de Recuperación de Desastres se han definido las siguientes Políticas:

a. El Plan de Recuperación de Desastres se ejecutará únicamente cuando una indisponibilidad severa y por tiempo prolongado afecte negativamente el servicio en el Data Center principal.
b. La recuperación del servicio de Tecnología de Información se realizará únicamente en el Data Center de Contingencia.
c. La ejecución del Plan de Recuperación de Desastres no contempla contingencias parciales, es decir sólo se ejecuta ante una situación total de desastre.
d. El Plan contempla respuesta a fallas de origen físico en el Data Center principal y en el Data Center de contingencia, no brinda respuesta a fallas de origen lógico o de software aplicativo.
e. La ejecución del plan es realizada íntegramente por los especialistas de cada plataforma, junto con proveedores previamente identificados para soporte.
f. El Plan de Recuperación de Desastres no contempla la recuperación de los clientes o proveedores que utilizan la plataforma de interoperabilidad
g. La estrategia de recuperación de la plataforma de interoperabilidad permitirá habilitar el servicio dentro de la ventana de tiempo de recuperación definida.
h. En caso de presentarse eventos severos que pongan fuera de servicio completamente tanto el Data Center Principal como el de Contingencia, se optará por declarar a la PI fuera de servicio por un tiempo determinado en la evaluación del impacto del desastre (evaluación de daños).

La estrategia de recuperación de la Plataforma de Interoperabilidad permitirá recuperar dentro de la ventana de tiempo de recuperación definida, tiempo que permitirá recuperar las operaciones, minimizando el impacto del evento.

B.- ALCANCE DEL PLAN DE RECUPERACIÓN DE DESASTRES

El Plan se orienta a recuperar en el Data Center de Contingencia las plataformas tecnológicas de interoperabilidad (PI) que se encuentran instaladas en el Data Center Principal producto de un evento que interrumpa la operatividad normal de funcionamiento.

C.- ESCENARIO DE CONTINGENCIA

De acuerdo al ítem (a) de la Política de Recuperación, el Plan de Contingencia y Recuperación ante Desastres se activará en escenarios de desastres catastróficos y que imposibilite la operación normal de entrega de servicios de TI desde el Data Center Principal, siendo este *Indisponible* para continuar operando desde este Data Center.

Así mismo se ha identificado otros tipos de escenarios cuyo impacto no es generalizado y sólo afectaría a servicios puntuales que ofrece la Plataforma de Interoperabilidad por lo que se podría tomar acciones y respuesta de contingencia puntuales.

D.- ESTRUCTURA ORGANIZACIONAL – EQUIPOS DE RECUPERACIÓN TECNOLÓGICA.

El Comité de Contingencia y Recuperación está conformado por parte del personal que administra la PI, el cual tiene por finalidad participar en el Plan de Recuperación de Desastres y poder llevar adelante los procedimientos establecidos en éste.

Las actividades del Comité de Contingencia y Recuperación no se limitan al momento de la ocurrencia de un desastre sino que su labor debe desarrollarse antes, durante y después de un incidente severo (Desastre).

Las tareas generales que tiene el Comité de Contingencia y Recuperación son:

- Coordinar las acciones a tomar con todas las instancias correspondientes.
- Conseguir los recursos necesarios para reiniciar los sistemas y las comunicaciones críticas.
- Coordinar los traslados de equipos y recursos necesarios para la operación en contingencia.
- Notificar a proveedores e instituciones el esquema de atención a brindar mientras dure la contingencia.
- Coordinar y restablecer los sistemas y las telecomunicaciones.
- Mantener actualizado el Plan de Recuperación de Desastres.
- Realizar las pruebas de recuperación de los sistemas (plataformas tecnológicas) y las comunicaciones en forma periódica.

E.- DECLARACIÓN DE DESASTRE

Dentro de la estrategia de la estrategia de recuperación ante desastres el objetivo es asegurar la continuidad operativa técnica de la PI luego de ocurrido un desastre

Luego del resultado de la evaluación de daños se DECLARARA EL DESASTRE activando el Data Center de Contingencia.

Procedimiento de Activación del Data Center de Contingencia (DCC)
Premisa El uso de del Data Center de Contingencia se activará y atenderá la producción en su totalidad en caso se cumpla el escenario de DESASTRE del DCP, el DCC se activará cumpliendo el tiempo establecido de recuperación.
Objetivo El objetivo de este procedimiento es activar el(los) servidor(es) de red de contingencia ubicado en una sede alterna.
Responsables: Responsables de las Plataformas tecnológica de la PI
Detalle de Actividades **Acciones de Coordinación** 1. El Líder del Comité será responsable de coordinar con los diferentes equipos-personal la activación de los equipos tecnológicos del DCC. 2. El Líder del Comité coordinará los accesos y facilidades para el traslado de los administradores de las plataformas de contingencia. 3. El Líder del Comité de Recuperación será responsable de coordinar con la empresa de Telecomunicaciones la ejecución del procedimiento de activación del enlace de comunicaciones para brindar el servicio por este medio alterno. **Acciones de Activación/Validación** 4. Los administradores de las plataformas deberán revisar, verificar y ejecutar las

actividades de validación de operatividad de las plataformas que operaron en contingencia y en alta disponibilidad.

5. Los administradores de las plataformas deberán validar los servicios de las aplicaciones que brinda la PI

6.- El administrador de las telecomunicaciones deberá validar el servicio de contingencia que entrega el enlace alterno del DCC..

7. Verificar que todos los servicios se encuentran activos coordinando y validando con los usuarios de la PI la operatividad normal del servicio.

4.5. MANTENIMIENTO DEL PLAN DE RECUPERACIÓN DE DESASTRES Y SU CONTROL DE CAMBIOS

La metodología formulada no puede estar culminada sin considerar un mantenimiento al Plan de Recuperación de Desastres para mantener la vigencia permanente y pueda ser utilizado con toda eficacia.

Las verificaciones regulares del Plan de Contingencia y Recuperación validan la eficacia de los procesos y procedimientos que son mantenidos en el Plan. Dado que se espera que surjan diversos cambios en el ambiente, esta política apunta a ejercicios regulares y programados del Plan para asegurar que las aplicaciones críticas estén disponibles para soportar la Institución en caso de un desastre.

Además, los ejercicios proveen una oportunidad para educar y entrenar al personal que administra la Plataforma de Interoperabilidad. Esta política promueve la rotación del personal que constituye los Equipos de Recuperación, para aumentar la base del personal entrenado para la ejecución del Plan y sus procedimientos durante un evento.

Las causas de efectuar mantenimiento al Plan de Contingencia son de origen interno o externo.

- Los cambios deben reflejarse en adiciones, retiros o reemplazo de hojas o capítulos del Plan, esto dependerá del alcance o profundidad de los cambios.

- Todo el material retirado del Plan deberá ser fechado y archivado para llevar un control de cambios a través de la existencia del mismo.
- Todas las acciones de cambio deberán actualizar, de ser necesario, el soporte en papel y los archivos magnéticos existentes, considerando principalmente el ejemplar existente en el almacén externo de registros vitales.

Los motivos de resultados de la ocurrencia de una Contingencia real se puede dar por evento o producto de:

- Cambios en la organización de la Administración de la PI
- Resultados de prueba de Plan de Contingencia.
- Resultados de la ocurrencia de una Contingencia real
- Desarrollo de sistemas
- Mantenimiento de programas informáticos
- Mejoras en la plataforma tecnológica de hardware y software
- Cambios en la infraestructura de los locales
- Introducción de nuevas tecnologías
- Cambios en los esquemas de comunicaciones LAN/WAN
- Nuevos controles de seguridad implementados

La revisión integral del Plan en caso no se de ninguno de los eventos antes mencionados deber ser dos veces al año.

Bitácora de Cambio de Versiones

Las modificaciones efectuadas sobre el Plan deberán estar resumidas en una Bitácora para facilitar una revisión rápida de la historia de los cambios.

La siguiente es una plantilla inicial para facilitar dichas anotaciones, las cuales deberán tener el grado de detalle necesario para ubicar en el documento original cualquier cambio de manera inequívoca y rápida.

Contiene los siguientes campos:

- **Versión del Plan**: Numeración que permite identificar los cambios del documento, esto se representará de acuerdo a si constituye un cambio parcial que no afecte la totalidad del documento o un cambio mayor que afecte el documento. En el primer caso se usará numeración con

decimales por ejemplo versión 1.2; versión 2.3; etc. En el segundo caso serán números enteros por ejemplo versión 1, versión 2, etc.

- **Fecha:** En formato año/mes/día, contiene la fecha en que se inicia la vigencia del cambio en el Plan
- **Responsable**: Apellidos y nombres del Líder de Contingencia al momento de efectivizarse el cambio en el Plan.
- **Tipo de cambio:** Breve referencia del motivo por el que se produce el cambio (cambios organizativos, mejoras tecnológicas, legislación oficial, cambios en normas internas, etc.)
- **Descripción**: Amplio detalle de la *modificación:*

  Título(s), subtítulo(s), capítulo(s) o párrafo(s) titulado(s) en que se hace(n) la corrección,

  Naturaleza del cambio que puede ser retiro, reemplazo o adición

Versión	*Fecha*	*Responsable*	*Tipo de cambio*	*Descripción del cambio*

CAPÍTULO V

ANÁLISIS COMPARATIVO ENTRE LA SOLUCIÓN EXISTENTE Y LA SOLUCIÓN PROPUESTA

5.1. VENTAJAS Y DESVENTAJAS DE LA SOLUCIÓN PROPUESTA

Como información adicional, la Solución existente es la que prescinde del Plan de Recuperación de Desastres (PRD), en otras palabras dicha solución comprende solo la implementación de la PI orientada a SOA sin tener ninguna documentación respecto a procedimientos que deberían seguirse ante un siniestro de esta magnitud, considerándose esta solución la línea base de comparación con la mejora lograda y la Solución propuesta es la que está contemplando el desarrollo del PRD bajo un enfoque SOA para esta clase de infraestructura, reduciendo de esta forma la interrupción del servicio que conlleva a mejorar su disponibilidad y asegurar la información comprometida.

VENTAJAS

- Existe un Manual de procedimientos que está previamente elaborado respecto a las acciones que deben ejecutarse en caso de un desastre bajo el enfoque de:

  Pruebas de Contexto

Pruebas de Organización
Pruebas operacionales

Mientras que en la solución existente solo existe la construcción de la plataforma que está regida por algunas acciones no escritas y que son más o menos conocidas por el equipo que está a cargo con el riesgo que no sean las mejores y la omisión de algunos pasos importantes.

- El personal técnico ya sabe que tiene que hacer en caso de un desastre o de lo contrario se basa en el plan desarrollado en este estudio, situación muy distinta de la solución existente la que no contempla dicha capacitación.

- De acuerdo al Plan de Crisis los stakehoders especialmente los externos ya están al tanto de sus acciones en caso de un siniestro que pueda afectar la plataforma de interoperabilidad. Mientras que en la solución existente no se tiene esta información y el riesgo de sus acciones inseguras es muy alto.

DESVENTAJA

- Si dichos procedimientos que se han desarrollado en el Plan de Recuperación de Desastres no se han probado mediante simulacros previamente organizados y planificados, existe el gran riesgo que la aplicación de este plan sea ineficiente y puede suceder que en vez de mitigar la discontinuidad de las operaciones se acentúe aun más el desastre que se está afrontando pudiendo ser peor en función de los procedimientos equivocados que se piensen aplicar.

5.2. RESULTADOS OBTENIDOS

La estrategia de recuperación ante una contingencia, y con mayor razón ante un desastre, empieza con un conjunto de acciones previas a cualquier tipo de contingencia; continúa con la planificación de un conjunto de acciones durante la contingencia y finaliza con la planificación de las acciones que nos permitirán retornar a la condición de normalidad cuando se ha superado la contingencia.

Esto nos da idea como el Plan de Recuperación de Desastres (PRD) debe contemplar las alternativas de recuperación y continuidad del servicio en diferentes escenarios que sean los más probables de acuerdo a las condiciones ambientales de la PI

5.3. RESUMEN COMPARATIVO SIN PRD vs. CON PRD

En el siguiente cuadro se muestra el resumen de los aspectos más resaltantes de ambos escenarios:

ACCIONES (ligadas al evento)	SIN Plan de Recuperación de Desastres	CON Plan de Recuperación de Desastres
ANTES	No existe documentación ni procedimientos para mantener las bases de datos sincronizadas ni los WS sincronizados	Procedimientos (base de datos y WS) actualizados para activar el DCC
DURANTE	Verificar la no existencia de cambios. Replicar y sincronizar BD. Coordinar con quien corresponda el redireccionamiento de WS	Procedimientos actualizados y automáticos para mantener bases de datos sincronizadas y WS configurados para su redireccionamiento al DCP

DESPUÉS	Análisis de impacto y determinación de pasos para recuperar el DCP	Enlace según evento ocurrido con plan de contingencia respectivo.

CAPÍTULO VI

CASO DE ESTUDIO (validación y pruebas)

6.1. DESCRIPCIÓN DEL AMBIENTE DEL CASO DE ESTUDIO

Activos críticos de TI (DCP/DCC)

La principal y primaria actividad para los análisis de impacto y de riesgo es la identificación de activos críticos y sensibles que conforman la PI, la identificación y dependencias que existen entre los componentes permiten evaluar la cadena de impacto en el servicio cuando uno de ellos sufre indisponibilidad.

A continuación se presentan los activos que conforman el servicio que brinda la PI:

1. Data Center Principal

Nombre de Servidor	Servidor Físico	Aplicación y/o Sistemas (Físico)	Servidor Virtual		Cant. de Aplicaciones	Aplicación y/o Sistemas(Virtual)
Servidor base de datos	2	(2) EnterpriseDB (1) RHN Management + Provisioning + Monitoring (2)Red Hat Enterprise Linux	0		--	--
Servidor de virtualización	6	(1) RHN Management + Provisioning + Monitoring (1)RHEL AP	3	MV1	1 CPU	SOA Software Service Manager / Network Director
				MV2		Intalio BPM
				MV3	--	--
		(1) RHN	3	MV1	1 CPU	SOA Software

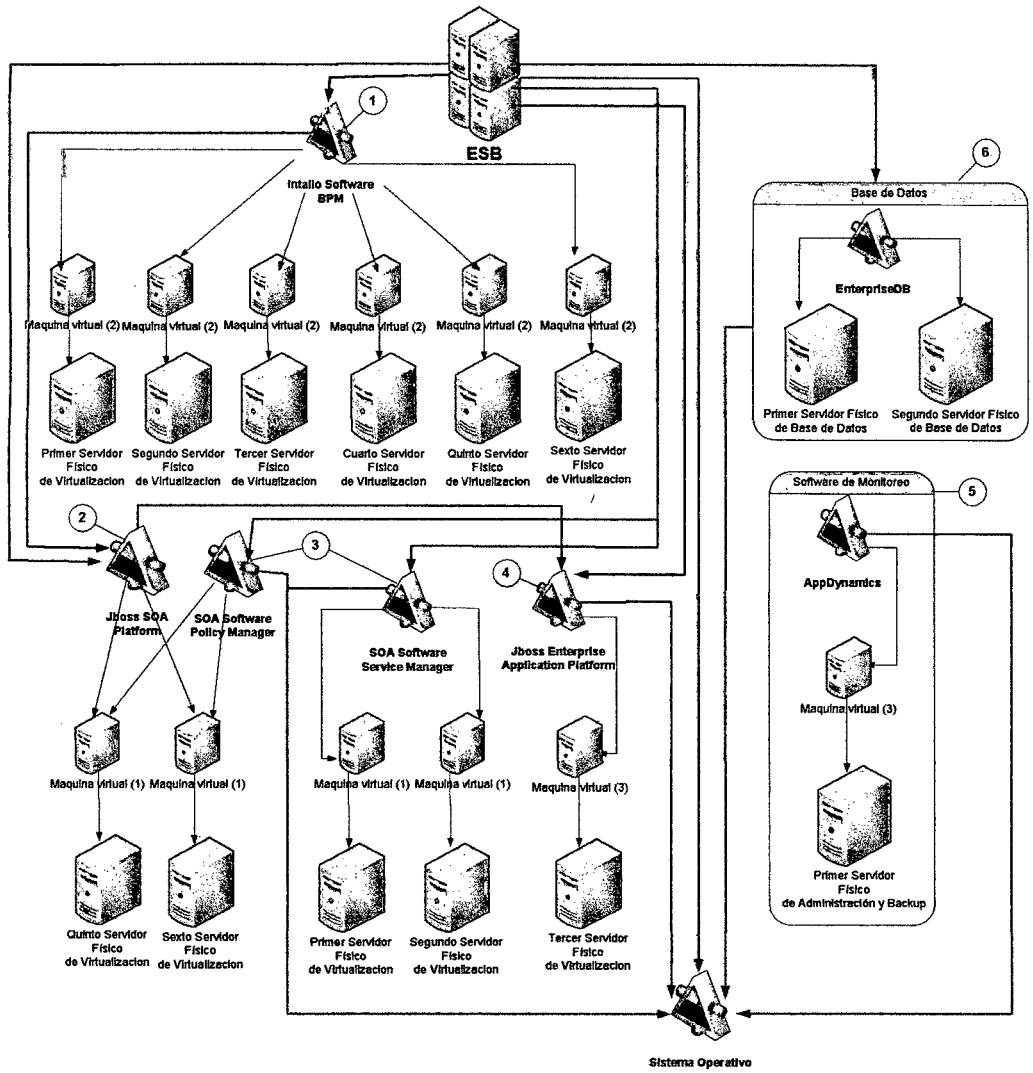
		Management + Provisioning + Monitoring (1)RHEL AP				Service Manager / Network Director
				MV2		Intalio BPM
				MV3	–	–
		(1) RHN Management + Provisioning + Monitoring (1)RHEL AP	3	MV1	1	RH Directory Server Master
				MV2	1	My SQL
				MV3	2 Sockets	**Liferay** Jboss Enterprise Application Platform
		(1) RHN Management + Provisioning + Monitoring (1)RHEL AP	3	MV1	1	RH Directory Server Replica
				MV2	1	My SQL
				MV3	2 Sockets	**Liferay** Jboss Enterprise Application Platform
		(1) RHN Management + Provisioning + Monitoring (1)RHEL AP	3	MV1	2 Sockets	SOA PM
				MV2	1	Intalio BPM
				MV3	1	Moodle+OTRS
		(1) RHN Management + Provisioning + Monitoring (1)RHEL AP	3	MV1	2 Sockets	SOA PM
				MV2		Intalio BPM
				MV3	1	BI Suite STD **(O3)**
Servidor de Administración y Backup	**2 (1 Servidor Físico sin MV, y el otro con MV)**	(1) RHN Management + Provisioning + Monitoring (2)RHEL AP	3	MV1	1	Red Hat Satelite
				MV2	1	Jboss ON Manager for SOA / Jboss ON Monitoring for SOA Platform
				MV3	1	AppDynamics
		Backup(2) Zmanda Network for Amanda Enterprise Edition Backup Server (RHEL 5)	0	–	–	–

2. Data Center de Contingencia.

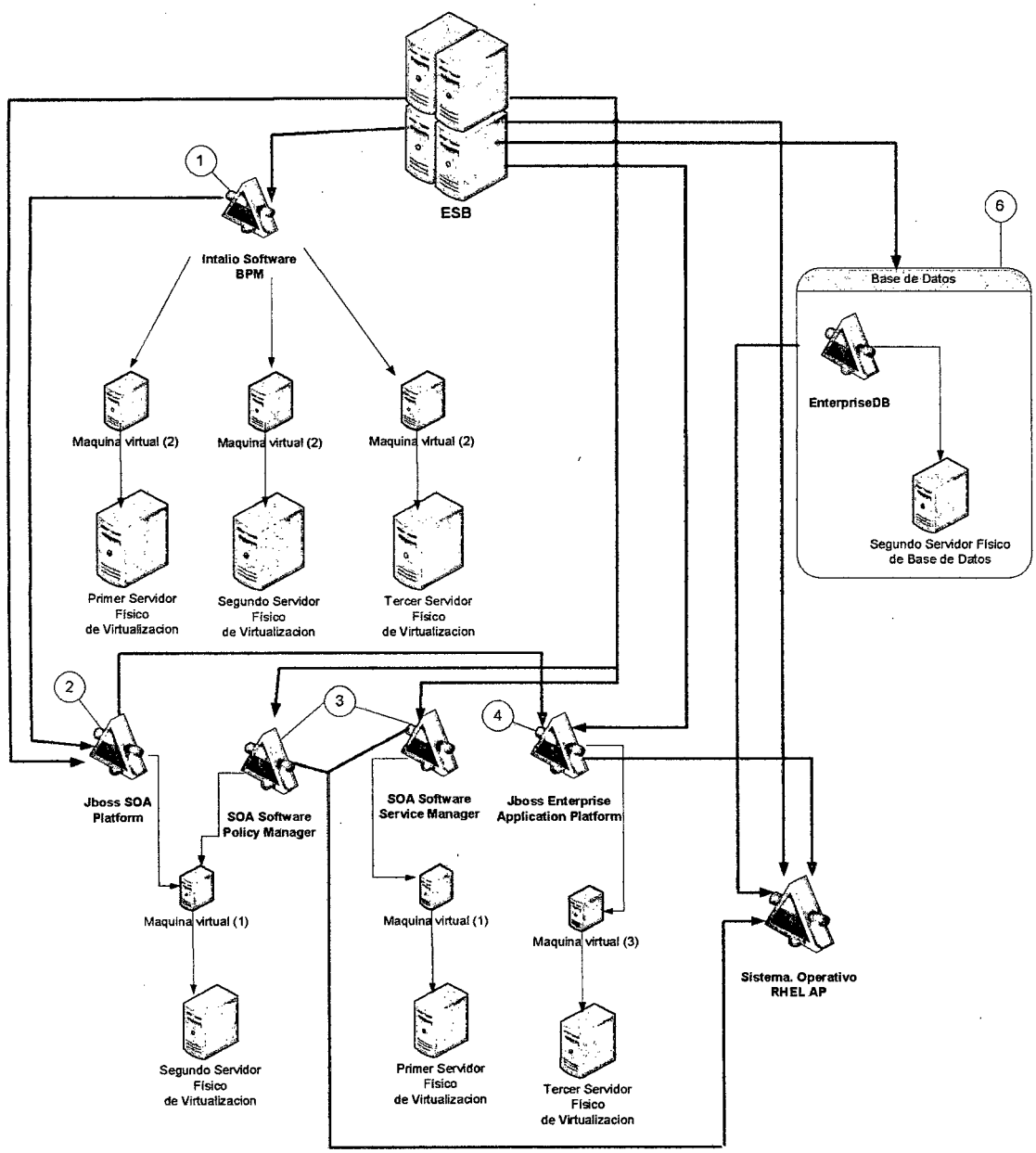
Nombre de Servidor	Servidor Físico	Aplicación y/o Sistemas (Físico)	Servidor Virtual		Cant. de Aplicaciones	Aplicación y/o Sistemas(Virtual)
Servidor base de datos	2	(2) EnterpriseDB (1) RHN Management + Provisioning + Monitoring (2)Red Hat Enterprise Linux	0		--	--
Servidor de virtualización	6	(1) RHN Management + Provisioning + Monitoring (1)RHEL AP	3	MV1	1 CPU	SOA Software Service Manager / Network Director
				MV2		Intalio BPM
				MV3	--	--
		(1) RHN Management + Provisioning + Monitoring (1)RHEL AP	3	MV1	1 CPU	SOA Software Service Manager / Network Director
				MV2		Intalio BPM
				MV3	--	--
		(1) RHN Management + Provisioning + Monitoring (1)RHEL AP	3	MV1	1	RH Directory Server Master
				MV2	1	My SQL
				MV3	2 Sockets	**Liferay** Jboss Enterprise Application Platform
		(1) RHN Management + Provisioning + Monitoring (1)RHEL AP	3	MV1	1	RH Directory Server Replica
				MV2	1	My SQL
				MV3	2 Sockets	**Liferay** Jboss Enterprise Application Platform
		(1) RHN Management + Provisioning + Monitoring (1)RHEL AP	3	MV1	2 Sockets	SOA PM
				MV2	1	Intalio BPM
				MV3	1	Moodle+OTRS
		(1) RHN Management + Provisioning + Monitoring	3	MV1	2 Sockets	SOA PM
				MV2		Intalio BPM
				MV3	1	BI Suite STD (O3)

		(1)RHEL AP				
Servidor de Administración y Backup	**2 (1 Servidor Físico sin MV, y el otro con MV)**	**(1)** RHN Management + Provisioning + Monitoring **(2)**RHEL AP	3	MV1	1	Red Hat Satelite
				MV2	1	Jboss ON Manager for SOA / Jboss ON Monitoring for SOA Platform
				MV3	1	AppDynamics
		Backup(2) Zmanda Network for Amanda Enterprise Edition Backup Server (RHEL 5)	0	–	–	–

Análisis de Impacto de la PI – Mapa de Configuración y Dependencias Data Center Principal



Data Center Contingencia



6.2. DISEÑO DE LAS PRUEBAS, EXPERIMENTOS Y/O VALIDACIÓN

En esta sección se busca establecer los métodos y pautas para ejecutar las pruebas de contingencia regularmente, siendo esta la única manera de asegurar que el Plan realmente sirve para su propósito.

PLAN DE PRUEBAS DE RECUPERACIÓN DE DESASTRES

El propósito de este punto es identificar y documentar los procedimientos que deberán ejecutarse en un ambiente de prueba. Incluye los objetivos de la prueba, el escenario de la prueba y sus premisas, así mismo esto debe contener un programa de pruebas que asegure la frecuencia de ejecución por los participantes y/o equipos de recuperación, las etapas de la prueba y los criterios para evaluar la prueba que eventualmente modificarán el Plan de Continuidad producto de los resultados obtenidos.

Objetivos:

- Demostrar la viabilidad del Plan de contingencia y de la estrategia de recuperación implementada.
- Llevar a cabo un entrenamiento repetitivo de los integrantes de los Equipos de Recuperación.
- Validar las ventanas y los tiempos de recuperación.
- Identificar las revisiones y actualizaciones que requiera el Plan.
- Proveer a los participantes el beneficio psicológico de estar preparados para llevar a cabo las tareas de recuperación durante una crisis.
- Promover el trabajo en Equipo.

Origen de las Pruebas

La programación de las pruebas obedece a varios factores entre los cuales se pueden mencionar:

- Programación periódica establecida con los equipos de recuperación como mecanismo de control de calidad de la función de recuperación.
- Cuando haya modificaciones de hardware, software operativo, de infraestructura y/o aplicativos; o cuando existan cambios significativos en el ambiente de los procesos de negocio cubiertos por el Plan.
- También pueden realizarse cuando se prevea el riesgo de que suceda un evento que afecte la operación de TI, como problemas laborales o de orden público.
- Por requerimientos de cumplimiento legal y normativos.

Categoría de las Pruebas

Hay 3 categorías básicas de pruebas de acuerdo a su naturaleza que pueden llevarse a cabo:

I. **Pruebas de Contexto.**
II. **Pruebas de Organización.**
III. **Pruebas Operacionales.**

Es posible también aplicar una combinación de estas categorías para lograr un ejercicio más completo del Plan.

I.- Pruebas de Contexto

Las Pruebas de contexto consisten básicamente en la realización de actividades con los empleados que les permitan estar en contacto permanente con el tema de recuperación, conocerlo y poner en práctica las partes del plan no asociadas a actividades o tareas de la recuperación.

Forma parte de esta categoría las pruebas de Notificación de Emergencia, las cuales brindan un método seguro y de bajo costo, para detectar omisiones generales, causadas por cambios en el personal designado en los Equipos de Recuperación. Consiste en verificar que la información de las Listas de Llamada esté vigente.

II.- Pruebas de Organización

Esta modalidad de prueba se focaliza en verificar la integridad y veracidad de las actividades y tareas asignadas a los Equipos de Recuperación, a la vez que brinda una

oportunidad para entrenar a sus integrantes, sin tener que interrumpir la producción o incurrir en gastos de traslado al Data Center de Contingencia.

El objetivo principal de esta modalidad de prueba es asegurar que el Plan ha definido todas las funciones y sus responsabilidades, y que se ha incluido toda la documentación de soporte. También puede ser utilizado para identificar el hardware, el software de base o las aplicaciones que pudieren haber sufrido cambios en los últimos meses.

La Prueba de Organización es denominada como "prueba de escritorio", este ejercicio es liderado por un Coordinador y generalmente podrá tomar entre 2 y 3 horas.

III.- Pruebas Operacionales

Una Prueba Operacional es un ejercicio planificado que incluye la habilitación de los sistemas, subsistemas y aplicaciones de la PI, mediante el traslado de recursos humanos y tecnológicos de Contingencia, en el cual se ejecutarán los procedimientos de recuperación contenidos en este Plan.

El objetivo principal de este tipo de pruebas es asegurar que la plataforma de recuperación y los enlaces de comunicaciones requeridos para restablecer las aplicaciones críticas estén disponibles, y que el personal está entrenado en la ejecución de los procedimientos documentados en este Plan.

Esta categoría de pruebas podrá tener un alcance parcial (por ejemplo, validación de los procedimientos técnicos de recuperación) o total, al incluir a la totalidad de los componentes del Plan.

Parámetros Generales de las Pruebas

- Alcance de la Prueba
    - Participantes
    - Notificación
    - Infraestructura
    - Aplicaciones
- Definir Objetivos de la Prueba

- Objetivos y resultados esperados
- Límite de tiempo

- Medición de la Prueba
  - Registro de tiempo durante la prueba
  - Documentar problema/desviación de la prueba
- Evaluación de la Prueba
  - Cumplimiento de Objetivos

Con el fin de realizar una prueba en forma efectiva, es necesario tener en cuenta que se deben identificar los objetivos principales, específicos y los resultados esperados para la prueba, teniendo en cuenta que estos se convertirán en los lineamientos sobre los que se realizará la planificación, por tanto la definición de los objetivos debe contemplar un trabajo detallado que conjugue requerimientos funcionales de operatividad con las expectativas de servicio asociadas.

Se debe establecer el límite de tiempo para la prueba, para que no afecte la operación normal de la Plataforma de Interoperabilidad (PI).

Fases de las Pruebas

Toda prueba requiere completar las 3 Fases de su desarrollo:

A. Planificación y Preparación (Pre-Prueba)
B. Ejecución (Prueba)
C. Revisión (Post-Prueba)

A.- Planificación y Preparación

Dentro de los 15 días previos a cada prueba, el Líder del Comité de Contingencia y Recuperación mantendrá una o varias reuniones de planificación con los integrantes del Comité. En éstas se revisarán los objetivos y alcances de cada ejercicio, el equipamiento requerido y todo otro componente que sea necesario para la oportunidad. Se deberá tener en cuenta para ello.

- Objetivos y alcance de la Prueba

- Parámetros de la Prueba
- Escenario de Prueba
- Desarrollo del Ejercicio
- Participantes de la Prueba

B.- Ejecución

La Ejecución debe realizarse en la fecha y hora programada y estará a cargo de los equipos de recuperación previamente coordinados y con los recursos necesarios para llevar a cabo la Prueba.

El Líder de Comité se encargará de supervisar y administrar la prueba, coordinando en todo momento las actividades de recuperación según lo planificado, se encargará también de tomar el tiempo de ejecución con la finalidad de cumplir con los tiempos objetivos de recuperación (RTO) que la Institución requiere para recuperarse.

C.- Revisión

La revisión de la Prueba debe realizarse luego de la ejecución de la misma, el Líder del Comité se encargará de realizar y emitir un Informe de la Prueba realizada la misma que contiene como mínimo el siguiente índice:

A. Descripción de la Prueba
B. Alcance de la Prueba
C. Equipos de ejecución
D. Resultados de la Prueba
E. Incidentes de las pruebas
F. Evaluación de Resultados
G. Anexos y evidencias.

El Informe de la Prueba será difundido a quien el Líder del Comité de Contingencia y Recuperación considere pertinente.

6.3. RESULTADOS

- Con la identificación de los componentes de Tecnologías de Información que conforman la PI y las aplicaciones que brindan el servicio a sus clientes externos se logró elaborar el mapa de configuración de los Data Centers, el

cual permite de manera rápida identificar las dependencias y por consiguiente determinar el impacto del servicio cuando estos fallan o sufren una indisponibilidad.

En ese sentido se tuvo los siguientes resultados:

Indicador X_1: Nivel de cumplimiento

Bajo el concepto, por juicio experto, que las pruebas son realmente exitosas si están en un rango del 70 % y 100 %

Índices:

$X_{1.1}$: Nro. de pruebas exitosas de Contexto / Nro. de pruebas totales de Contexto.

Métricas → Contactos verificados

En este caso se hicieron 12 pruebas totales de Contexto (una prueba mensual por la facilidad en su realización) de las cuales 11 fueron exitosas.

$X_{1.1}$: 11/12 = 0.92 → 92% Esta dentro del rango propuesto

$X_{1.2}$: Nro. de pruebas exitosas de Organización /Nro. de pruebas totales de Organización.

Métricas → Actividades verificadas

En este tipo de pruebas se hicieron 12 pruebas totales de Organización (una prueba mensual por la facilidad en su realización) de las cuales 9 fueron exitosas.

$X_{1.2}$: 9/12 = 0.75 → 75% Esta dentro del rango propuesto

$X_{1.3}$: Nro. de pruebas exitosas de Operación /Nro. de pruebas totales de Operación.

Métricas → Componentes verificados.

En este tipo de pruebas se hicieron 6 pruebas totales de Operación (una prueba bimestral por la complejidad en su realización) de las cuales 5 fueron exitosas.

$X_{1.3}$: 5/6 = 0.83 → 83% Esta dentro del rango propuesto

- La PI está conformada por aplicaciones que en conjunto brindan el servicio y estos a su vez son soportados por distintas plataformas (servidores físicos y virtuales), base de datos y sistemas operativos. Así mismo es posible determinar la dependencia y el flujo de información que existe entre las distintas aplicaciones que soportan la PI.

Indicador Y_1:

Continuidad del servicio

Índice:

$Y_{1.1}$: Tiempo objetivo de recuperación (TOR) o (Recovery Time Objective)
Contiene el Failover (Conmutación por falla) y el Failback (Restauración por falla)
TOR = Tiempo de Failover + Tiempo de Failback
Métrica → Minutos

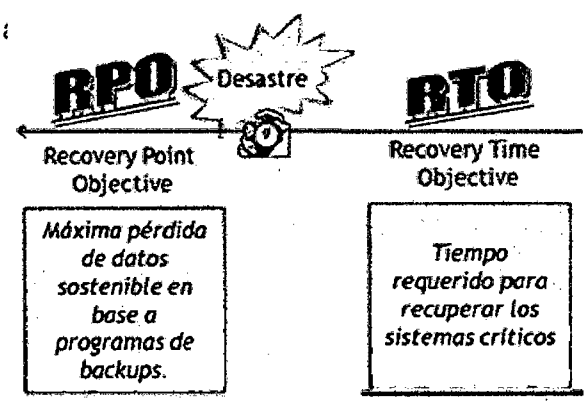
Indicador Y_2:

Disponibilidad del servicio

Índice:

$Y_{2.1}$: Punto objetivo de recuperación (POR) o RPO (Recovery Point Objective)
Métrica → Datos perdidos

- Al revisar las estrategias de recuperación ante un incidente severo y de duración prolongada, los especialistas de la implementación de la PI indicaron lo siguiente respecto a



- El Tiempo Objetivo de Recuperación (RTO) de las plataformas tecnológicas en el Data Center de Contingencia - Failover es igual a Seis (6) minutos, tiempo resultante del esquema de Alta Disponibilidad, trasladando de manera automática los servicios críticos de la PI del Data Center Principal al Data Center de Contingencia.
- La restauración del Servicio de la PI trasladando los servicios del Data Center de Contingencia al Data Center Principal – Failback es igual a Ocho (8) minutos, producto de restauración y cambios de los servicios de manera semi-automática.
- El TOR = Tiempo de Failover + Tiempo de Failback = 6' + 8' = 14'
- Punto Objetivo de Recuperación (RPO), respecto a la tolerancia de pérdida de información y/o data huérfana, los especialistas de la implementación aseguran que el RPO es igual a Cero, es decir no es tolerable la pérdida de información y

esto se debe en esencia a la réplica de información a través de fibra oscura y al doble commit cuando se efectúa o realiza una transacción en la PI. Por la replicación de la Base de Datos el RPO es 0%

- La matriz que se encuentra en el Anexo 3 indica el "Impacto de la No Disponibilidad del Servicio en base a la importancia y criticidad de la Aplicaciones que conforman la PI". Así mismo se indica las plataformas que las conforman, la cual permite identificar la criticidad de la misma y en la cual se debe enfocar los esfuerzos de asegurar la alta disponibilidad y el funcionamiento de esta estrategia cuando una contingencia severa indisponga el servicio.
- El impacto que se muestra en este análisis nos indica el orden de importancia y la priorización en el orden de recuperación en caso de una contingencia e indisponibilidad del Servicio de la PI.
- El Análisis de Riesgos es el proceso mediante el cual se identifican las amenazas y vulnerabilidades de los principales activos y mediante la estimación del impacto y probabilidad de ocurrencia de las principales amenazas es posible determinar, cualitativamente, la magnitud del riesgo.
- Este proceso comprendió las actividades de Identificación de Activos, Análisis de Riesgos y el tratamiento de los riesgos encontrados bajo el marco de referencia ISO/IEC 27001 – (Anexo A de la Norma).

Análisis de Riesgo

- Para el análisis de riesgos nos basamos en los conceptos que se definen a continuación:

- *AMENAZA:* Es un evento o situación que existe, y es independiente del control de la organización o sujeto de análisis, y que potencialmente puede causar daño o perjuicio de algún tipo y desencadenar otras amenazas. Para el análisis tenemos que las amenazas más críticas son las siguientes: Inundaciones, terremoto, fuego, incendio, sabotaje, ataques terroristas, vandalismo, falla

general en el sistema de energía, falla en la seguridad física, falta de personal para las operaciones y soporte de los servicios que brinda la PI.

- *VULNERABILIDAD:* Debilidad que puede ser explotada por una amenaza. Para cada amenaza se identificaron las vulnerabilidades a las que están expuestos los principales activos de la PI afectados.

- *IMPACTO Y PROBABILIDAD:* Para evaluar los riesgos, se calculó el impacto y la probabilidad de ocurrencia de la amenaza tomando en consideración los mecanismos de protección existentes para el control de los Activos en relación a los Riesgos a los que se encuentra expuesto.

Indicador Y_3:

Riesgo de TI

Índices:

$Y_{3.1}$: Nivel de Impacto de las amenazas

Niveles: Grave, Severo, Moderado, Bajo y Muy Bajo
Métrica → Puntuación

$Y_{3.2}$: Probabilidad de ocurrencia de las amenazas

Niveles: Muy frecuente, Probable, Posible, Improbable y Raro
Métrica → Puntuación

$Y_{3.3}$: Nivel de riesgo de la PI

Niveles: Extremo, Alto, Moderado, Bajo
Métrica → Puntuación

- La Probabilidad de ocurrencia de las amenazas se estimo considerando los siguientes niveles

Probabilidad (P)	Criterio	Puntuación
Muy frecuente	Varias veces al mes	5
Probable	Una vez al mes	4
Posible	Cada seis meses	3
Improbable	De uno a dos años	2
Raro	Uno cada Mas de dos años	1

- El *impacto de las amenazas* se clasificó por el tipo de consecuencias que las amenazas pueden producir en los activos de información, considerando los siguientes niveles:

Impacto (I)	Criterio	Puntuación
Grave	Afecta e impacta la disponibilidad irreversiblemente	5
Severo	Afecta e impacta la disponibilidad severamente	4
Moderado	Afecta e impacta la disponibilidad parcialmente	3
Bajo	Afecta e impacta la disponibilidad mínimamente	2
Muy Bajo	No Afecta	1

- El Nivel de Riesgo al que el activo está expuesto, está dado por el producto de la Probabilidad de Ocurrencia con el Impacto de la amenaza. En base al impacto y a la probabilidad de ocurrencia de las amenazas identificadas se definió cuatro Niveles de Riesgo:

Clase de Riesgo (CR)	Criterio	Nivel de Riesgo (NR)
Extremo	Puede afectar seriamente al servicio que ofrece la Plataforma de Interoperabilidad del Estado Peruano, en términos de Indisponibilidad del Servicio ofrecido, paralización de las operaciones más allá del tiempo tolerable. Pérdidas económicas considerables, y daño considerable a la imagen de la institución.	15-25
Alto	Puede afectar a los niveles de operación y servicio de la PI, incumplimiento de metas, pérdidas económicas importantes.	8-14
Moderado	Afecta al cumplimiento de un objetivo secundario o de soporte. Puede afectar la operación de la PI.	4-6
Bajo	No causa un efecto considerable en la organización.	1-3

Este es el resultado del Indicador Y_3:

			Impacto (I)				
			Grave	Severo	Moderado	Bajo	Muy Bajo
			5	4	3	2	1
Probabilidad (P)	Muy probable	5	25	20	15	10	5
	Probable	4	20	16	12	8	4
	Posible	3	15	12	9	6	3
	Improbable	2	10	8	6	4	2
	Raro	1	5	4	3	2	1

- Así mismo se definió las siguientes acciones en función a los resultados del análisis:

Clasificación	¿Se acepta?	Tratamiento	Observación
Bajo	Sí	Monitoreo	Aceptar
Moderado	Sí	Monitoreo	Aceptar
Alto	No	A definir	Mitigar, Transferir
Extremo	No	A definir	Mitigar, Transferir

6.4. ANÁLISIS Y TRATAMIENTO DE RIESGOS

Del análisis de riesgos realizado se ha detectado los activos que son utilizados por la PI, haciendo hincapié en aquellas amenazas con nivel de riesgo extremo y alto, las cuales requerirán un tratamiento de riesgo especial para reducir su nivel de riesgo hallada a un valor de riesgo aceptable de nivel moderado o bajo.

A continuación se presentan aquellos activos identificados con nivel de tolerancia Extrema y Alto:

Activo	Tipo de Riesgo	Amenaza
Aplicaciones	Recursos Humanos	Falta de personal para las operaciones y soporte de los servicios que brinda este equipo.
		Incumplimiento de los controles que garanticen la confidencialidad de la información que se maneja en la PI
		1. Inadecuado programa de capacitación y entrenamiento del personal responsable de la administración de la plataforma. 2. La selección o

		asignación de personal
Data Center	Desastres Naturales/Humanos/Ambientales	Fuego, Incendio
		Terremoto, Inundación
		Ataque destructivo, Terrorismo, vandalismo
		Falla general del sistema de energía.
		Falla o errores de seguridad física.
		No existe redundancia local.
Servidores Físicos	Software, Recursos Humanos	Problemas con la disponibilidad y performance de los servicios por errores de administración y control de cambios
		Problemas con el funcionamiento del equipo por errores humanos ante la ausencia de procedimientos operativos.

Es importante destacar que se debe poner énfasis en proponer acciones para el tratamiento de los riesgos que permitan reducir los Niveles de Riesgo Extremo y Alto para los activos aquí presentados, a un nivel de riesgo aceptable por los responsables de la PI o riesgo residual.

Los controles y mecanismos de protección que se proponen deben estar acordes con las necesidades de reducir los riesgos de manera inmediata.

Tratamiento del Riesgo

Se ejecutó en función a las necesidades de reducir los riesgos, los controles preventivos y correctivos que permitan minimizar los riesgos encontrados en el análisis de ejecutado son extraídos de la norma internacional ISO/IEC 27001 – (Anexo A de la Norma), sin embargo estos controles son generales, la personalización de estos según la necesidad de la PI deriva en acciones a tomar de manera inmediata debido a los resultados obtenidos.

A continuación se presentan los principales controles seleccionados de la norma internacional ISO/IEC 27001 (Anexo A de la Norma) que mitigarán los riesgos encontrados:

- A.8.1.2 Selección
- A.9.1.2 Controles físicos de entrada
- A.9.1.4 Protección contra amenazas externas y ambientales
- A.9.2.1 Ubicación y protección de equipos
- A.9.2.2 Instalaciones de Suministros
- A.10.1.3 Segregación de Tareas
- A.10.3.1 Gestión de Capacidades
- A.6.1.5 Acuerdos de Confidencialidad
- A.11.1.1 Políticas de control de acceso
- A.12.5.1 Procedimientos de control de cambios
- A.13.2.1 Responsabilidades y Procedimientos
- A.14.1.3 Desarrollar e implementar PCN que incluyan Seguridad de la Información.

Estos controles se derivan de la BS ISO/IEC 17799:2005, equivalente a la ISO 27002, Cláusulas del 5 al 15 que proporcionan los lineamientos de los controles especificados en A.5 al A.15

6.5. RESULTADOS COMPARATIVOS DE LA INVESTIGACIÓN

A continuación se muestra el cuadro comparativo entre el escenario original – SIN PRD (línea base) y el escenario CON PRD:

ESCENARIO \ ESTADO	FAILOVER	RESTAURACIÓN	FAILBACK
SIN Plan de Recuperación de desastres	**72 horas y alto riesgo:** • Replicación y sincronización de bases de datos • Coordinación y redireccionamiento de 14 instituciones que interoperan con el grupo empresarial para activar el DCC	**Mayor tiempo y mayor riesgo:** • Determinar causa del evento. • Evaluar impacto. • Elaborar procedimientos para restaurar DCP. • Riesgos al ejecutar procedimientos erróneamente	**6 horas y alto riesgo:** • Coordinación y Sincronización manual de base de datos y WS para retornar al DCP en estado original
CON Plan de Recuperación de desastres	**6 minutos y bajo riesgo:** • Sincronización automática de bases de datos y WS para activar DCC	**Menor tiempo y bajo riesgo:** • Invocar plan de contingencia correspondiente al evento desastre y ejecutarlo	**8 minutos y bajo riesgo:** • Sincronización semi-automática siguiendo procedimiento para retornar al estado original

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

- Conforme al resultado comparativo (6.5) del escenario base (SIN PRD) versus el escenario con PRD podemos concluir que en los tres estados (FAILOVER; Restauración y FAILBACK), existe un mayor de tiempo de disponibilidad así como un menor riesgo utilizando la Metodología basada en un enfoque SOA y que desarrolla el PRD.
- Considerando que el estado mas significativo para mostrar la gran mejora en la continuidad de servicio es el denominado tiempo de conmutación por falla (FAILOVER) con el que se logra solo 6 minutos para recuperar el servicio redireccionándolo automáticamente al DCC, podemos verificar que nuestra Metodología objeto de esta investigación agrega valor al negocio tomando en cuenta que sin PRD fue de fue de 4,320 minutos.
- Contar con un PRD también involucra un menor riesgo en la ejecución de los procedimientos durante el FAILOVER, RESTAURACION y FAILBACK, debido a que provienen de un estudio previo y han sido probados y actualizados, por cualquier cambio en la arquitectura SOA de las empresas que conforman la Plataforma de Interoperabilidad del grupo empresarial.
- La implementación de la Metodología objeto de este estudio, es rentable para una organización del tamaño de este grupo empresarial como se observa en el cuadro adjunto, en el que se ha considerado un solo evento de desastre al año:

ESCENARIO \ RUBROS	INVERSION (elaboración PRD)	COSTO OPERATIVO (1 persona para mantenimiento y actualización)	COSTO POR EVENTO DESASTRE (FAILOVER)
SIN PRD	0	0	72 * US 10,000/hora =US $ 720,000
CON PRD	US $ 30,000	US $ 18,000	US $ 1,000

ROI = (720,000 – (30,000 + 18,000 + 1,000)) / (30,000 + 18,000 + 1,000)= 13.7

RECOMENDACIONES

- Aquellas organizaciones que pretendan implementar una Plataforma de Interoperabilidad con enfoque SOA, deberían de estimar el costo de interrupción de sus transacciones por hora con el fin de considerar la implementación de esta Metodología basada en un enfoque SOA, de un Plan de Recuperación de Desastres para una Plataforma de Interoperabilidad.
- El análisis de riesgo y su tratamiento se deben realizar de manera periódica y/o cuando exista un cambio trascendental en las plataformas o servicio que presta la PI.
- Los Data Centers necesitan implementar controles de seguridad física, acceso y electromecánica a fin de reducir los riesgos ambientales, humanos y de naturaleza.
- Respecto a la Evaluación de Resultados del tratamiento de riesgos, es importante señalar que el tipo de Riesgo "Recursos Humanos", debe tratarse de manera especial, tomando en cuenta una capacitación efectiva de conocimientos con actualización permanente.

RESUMEN DE LOS APORTES REALIZADOS EN LA TESIS

- Desarrollar una metodología que sirva de base para construir un Plan de Recuperación de Desastres, bajo el enfoque SOA, para Plataformas sumamente complejas como la PI.
- Determinación de índices muy importantes como el ROI (return of investment) de la Implementación de esta Metodología basada en un enfoque SOA; de una Plan de Recuperación de desastres para una Plataforma de Interoperabilidad.
- Las pruebas de contexto, organización y operación sirven como medida efectiva de la eficiencia que debe tener la organización que aplica el PRD, con el fin de mantenerlo operativo
- La elaboración del análisis de riesgos con una metodología que permita determinar el tratamiento de esos riesgos calificados como críticos para optar por la acción de solución más conveniente.

RECOMENDACIONES PARA FUTURAS INVESTIGACIONES

- Hay un crecimiento sostenido en la implementación de Plataformas de interoperabilidad, bajo enfoque SOA, cada vez más grandes, ambiciosas y complejas lo cual requiere de mayor profundidad en las consideraciones y consideración de pruebas diversas y de mayor exigencia.
- Que los trabajos de investigación se fundamenten en escenarios con la última tecnología y así poder generar beneficios a las entidades que la requieren.
- No perder de vista la innovación de las soluciones, las cuales deben ser desarrolladas con mucha creatividad para agregar valor a la investigación.
- Que la estructura de la investigación sea flexible para que pueda adecuarse a cualquier tipo de investigación.
- Que el investigador conozca el área de conocimiento de la investigación para que su aporte a la ciencia sea mayor y bien fundamentado.

REFERENCIAS BIBLIOGRÁFICAS

- Neaga, Gregor; Winters, Bruce; Laufman Pat, (1998). S-O-S- en su Sistema de Computación- Prentice Hall Hispanoamérica, S.A.

- Erl, Thomas, (2005). Service-Oriented Architecture. Concepts, Technology and Design. Pearson Education

- Concepción Muñoz Delgado, (1998), *Geografía*, Anaya.

- Diccionario de la lengua española 2005 (2010). wordreference.com (ed.): «software» (diccionario). Espasa-Calpe.

- IEEE Std, IEEE Software Engineering Standard, (1993). Glossary of Software Engineering Terminology. IEEE Computer Society Press.

- WIKIPEDIA, (2012). La enciclopedia libre. [en línea].

- Haeberer, A. M.; P. A. S. Veloso, G. Baum, (1988). Formalización del proceso de desarrollo de software (Ed. preliminar edición). Buenos Aires: Kapelusz

- Huidobro Moya, José Manuel. (2006). Redes y servicios de telecomunicaciones. Madrid: Thomson.

- Treatise on Electricity and Magnetism, (1873).

- Stallings, William (2004). *Comunicaciones y Redes de Computadores*. Prentice Hall

- Comer, Douglas, (2000). *Redes Globales de Información con Internet y TCP/ IP.* Prentice Hall

- Jim Hoffer, (Jan 2001). "Backing Up Business - Industry Trend or Event", Health Management Technology.

- Feenberg, Daniel, (14 de mayo de 2004). «Can Intelligence Agencies Read Overwritten Data? A response to Gutmann.». National Bureau of Economic Research.

- M. Bishop, (December 2002). Computer Security: Art and Science, chapter 25. Addison-Wesley.

- C. Eckert. IT-Sicherheit. Oldenbourg, (2004). Manunchen [u.a.].

- M. Whitman and Herbert Mattord, (2003). Principles of Information Security, Course Technology.

- A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, (1996). Handbook of Applied, Cryptography. CRC.

- Sommerville, Ian, (2005). Ingeniería del software (7ma. edición). Madrid: Pearson Educación S.A.

- Norma Técnica Peruana NTP ISO/IEC 27001-2005, Sistema de Gestión de Seguridad de la Información ISMS.

GLOSARIO

Término	Definición
DRP (Plan de Recuperación ante Desastres)	Un plan claramente definido y documentado a ser utilizado en una situación de emergencia, evento, incidente o crisis. Usualmente un DRP considera la recuperación de recursos, servicios y acciones necesarias a realizar con personal clave, que son requeridas para recuperar las Tecnologías de Información.
Incidente	Una ocurrencia o percepción que amenaza las operaciones, personal, valor accionario, accionistas, marca, reputación, confianza, y/o cualquier riesgo estratégico que afecte los objetivos del negocio.
Desastre	Un evento catastrófico repentino no planeado que causa daños o pérdidas irreparables. Un evento que compromete la disponibilidad de funciones críticas, procesos o servicios por un periodo de tiempo de manera no aceptable. Un evento donde la alta dirección de una organización activa su plan de continuidad.
"Posible Desastre"	Ha ocurrido una falla en el área que ha paralizado el proceso, pero todavía está en evolución – es una alerta", solo se pide que se informe de la situación actual, no se moviliza personal.
"Alerta de Desastre"	El tiempo de recuperación está por vencerse, de manera preventiva se solicita a los integrantes del Comité de Contingencia y Recuperación iniciar las coordinaciones con sus equipos de recuperación para el transporte del personal y habilitación de sitio alterno, recursos, registros vitales, y proveedores.

Término	Definición
"Declaración de Desastre"	Es un hecho que el tiempo de recuperación se vence, antes de ello, se decide activar los planes, para lo cual se da inicio a la movilización del personal y a las pruebas preliminares de los recursos a utilizar.
Disponibilidad (Availability)	Concepto que define cualquier mecanismo diseñado para minimizar el "tiempo fuera" del servicio ofrecido. Cuando falla la disponibilidad aparece la continuidad.
Registro Vital	Cualquier documento o recurso de almacenamiento sin el cual no es posible la recuperación de un proceso o función.
RTO (Recovery Time Objective, Tiempo Objetivo de Recuperación)	Identifica el tiempo en el cual las actividades de misión crítica y/o sus dependencias deben ser recuperadas.
RPO (Recovery Point Objective – Punto objetivo de recuperación)	Es el tiempo transcurrido desde la última copia de respaldo antes de ocurrido el evento serio o desastre.
Data Center de Contingencia	Es un sitio mantenido en espera para ser utilizado cuando ocurra en evento serio o desastre y mantener la continuidad del negocio de las actividades de misión crítica.
Data Huérfana	Información creada, modificada, eliminada entre la última copia de seguridad (Backup) y el momento del desastre.
Respaldos (Backups)	El resguardo de información correspondiente a un sistema o aplicación en un medio que pueda ser almacenado en el Data Center y/o en un lugar externo. Los backups de datos pueden ser usados para restaurar datos corruptos, perdidos o para

Término	Definición
	recuperar sistemas completos y bases de datos en caso de desastre. Deben ser considerados confidenciales y ser protegidos de daños físicos y robo.

ANEXOS

Anexo 1: Hoja de Control de acciones de contingencia

HOJA DE CONTROL DE ACCIONES DE CONTINGENCIA

Descripción del Evento

Fecha: _____ Hora: _____

Evaluación del Impacto: _____

Quien reporto el evento:_____

Acciones preliminares adopatadas

_____
_____
_____
_____

Informes Preliminares

Sistemas: _____
Administración: _____
Otros: _____

Evaluación de Daños

_____
_____
_____
_____
_____
_____

Autorización del Activación del Plan

Fecha/ Hora: _____

Autorizado por: _____ Firma: _____

Restricciones a la autorización

_____
_____
_____

Anexo 2: Check List – Notificación del Evento.

Check List - NOTIFICACION DEL EVENTO			
Actividad	**Responsable**	**Fecha / Hora**	**Descripción de la ocurrencia**
Dimensión del Evento Tipo de Evento Fuente del Evento Componente afectado Hora del evento			
Identificación de la fuente del evento A: En el mismo DCP B: En el edificio C: Terceros (Telefonía, Luz)			
Identificación de Componentes de Software afectado: (Indicar según el inventario)			
Primer Diagnostico: De los Proveedores de Hardware De los Proveedores de Hardware Del Area de TI (PIDE)			
Notificación del Evento Detalle / Descripcion del evento			

ANEXO 3

Impacto de la No Disponibilidad del Servicio en base a la importancia y criticidad de la Aplicaciones que conforman la PI

Ítem	Sistema o Aplicación	Descripción	Impacto en el Servicio MA/A/M/B	Plataforma TI -DCP	Plataforma TI - DCC
1	Jhoss Enterprise Application Platform	JBoss Enterprise Application Platform es un servidor de aplicaciones JAVA que cumple con las especificaciones J2EE Versión 1.5.	**MUY ALTO**	Servidor de Virtualizacion-MV3	Servidor de Virtualizacion-MV3
2	RHEL AP	Red Hat Enterprise Linux Advance Platform es un Sistema operativo Linux de tipo empresarial que incluye soporte para maquinas virtuales ilimitadas, clúster de alta disponibilidad y soporte a sistema avanzados de almacenamiento de clúster.	**MUY ALTO**	Servidor de Virtualizacion	Servidor de Virtualizacion
3	Red Hat Enterprise Linux	Red Hat Enterprise Linux es un sistema operativo Linux de tipo empresarial que incluye soporte	**MUY ALTO**	Servidor de Base de Datos	Servidor de Base de Datos

		hasta 4 maquinas virtuales.			
4	Jboss SOA Platform	Jboss SOA Platform es una suite de aplicaciones unificada para encontrar, integrar y orquestar los servicios de negocios de aplicaciones empresariales SOA, y otros activos de TI en la automatización de los procesos de negocios.	**MUY ALTO**	Servidor de Virtualizacion	Servidor de Virtualizacion
		Es un servidor basado en LDAP que centraliza configuración de aplicaciones, perfiles de usuario, datos del grupo, las políticas y la información de control de acceso en un sistema operativo independiente, registro basado en la red. La formación de la central depositaria de una infraestructura de gestión de identidades, simplifica la administración de usuarios, eliminando la redundancia de datos y automatización de			

		datos de mantenimiento.			
5	SOA Software Policy Manager	SOA Software Policy Manager Es una solución para la administración de la seguridad de la arquitectura SOA basado en políticas.	**MUY ALTO**	Servidor de Virtualizacion - MV1	Servidor de Virtualizacion - MV1
6	SOA Software Service Manager / Network Director	SOA Software Service Manager es un sistema que intermedia y provee las bases para la administración, seguridad y cumplimiento de políticas de acceso a las aplicaciones y web service dentro de una arquitectura SOA. SOA Software Network Director es una aplicación que realiza el enrutamiento inteligente de servicios e intermediación flexible ofreciendo virtualización de servicios, alta disponibilidad, balanceo de carga y otros. Provee objetos de tipo stateless	**MUY ALTO**	Servidor de Virtualizacion - MV1	Servidor de Virtualizacion - MV1

		ofreciendo una performance y escalabilidad excepcional combinadas con una capacidad para mediación, enrutamiento y cumplimiento de políticas.			
7	EnterpriseDB	EnterpriseDB es el gestor de base de datos que comparte funcionalmente muchas características de tipo empresarial del gestor de base de datos Oracle y que además es compatible con el lenguaje PL/SQL de Oracle.	**ALTO**	Servidor de Base de Datos	Servidor de Base de Datos
8	Intalio Server / Intalio BAM / Intalio Portal (3 years)	Intalio Server es el BPMS, que cuenta además de una herramienta grafica de diseño de procesos BPM, cuenta con un motor de ejecución del código BPM expresado en el lenguaje BPEL. Intalio BAM es un sistema de monitoreo de procesos de negocios (business activity Monitoring) que permite sacar	**ALTO**	Servidor de Virtualizacion-MV2	Servidor de Virtualizacion-MV2

		estadísticas e indicadores de gestión. Intalio Portal es un portal web (Liferay portal) que provee muchas funcionalidades que facilitan la administración de contenidos web.			
9	RHN Satélite	Red Hat Network Satelite es una solución de gestión de sistemas web fácil de manejar, la cual permite administrar la plataforma operativa Red Hat Enterprise Linux, realiza actualizaciones de software, tales como gestión de la configuración, aprovisionamiento y control en servidores Red Hat Enterprise Linux, tanto físicos como virtuales.	**MEDIO**	Servidor de Adm. Y Backup - MV1	--
10	RHN Management + Provisioning + Monitoring	RHN Management, Provisioning, Monitoring (Administración, Aprovisionamiento y Monitoreo, respectivamente) son módulos de Red Hat Network que adicionan la capacidad de monitoreo, administración y aprovisionamiento de la plataforma a	**MEDIO**	Servidor de Base de Datos, Servidor de Virtualizacion y Servidor Adm. y Backup	Servidor de Base de Datos, Servidor de Virtualizacion y Servidor Adm. y Backup

		administrar basándose en estándares abiertos.			
11	AppDynamics	AppDynamics es un gestor de monitoreo y rendimiento de aplicaciones con soporte para Java/.NET, ofrece una resolución rápida de problemas a través del monitoreo de flujo de transacciones.	**MEDIO**	Servidor de Adm. Backup - MV3	--
12	AppDynamics - Agentes	Los agentes de AppDynamics son conectores o nexos entre el cliente y el servidor AppDynamics que mediante llamadas SOAP y XML monitorean las aplicaciones del entorno.	**MEDIO**	--	Servidor de Virtualizacion
13	BI Suite STD	Es un completo sistema de Inteligencia de Negocios (BI). Incluye todos los estándares de BI y Data Warehousing. Además de proporcionar herramientas para la consolidación de datos de múltiples fuentes en un almacén de datos.	**MEDIO**	Servidor de Virtualizacion - MV3	--

14	Jboss ON Manager for SOA	Jboss ON Manager para SOA es el servidor para el monitoreo y administración de la plataforma SOA de Jboss.	**MEDIO**	Servidor Adm. Y Backup - MV2	Servidor Adm. Y Backup - MV2
15	Jboss ON Monitoring for SOA Platform	Jboss ON Monitoring para SOA Platform es el componente agente que permite realizar el monitoreo y administración de los servidores que contienen la plataforma SOA de Jboss.	**MEDIO**	Servidor Adm. Y Backup - MV2	Servidor Adm. Y Backup - MV2
16	Zmanda Network for Amanda Enterprise Edition Backup Server (RHEL 5) and 5 backups clients	Zmanda Network para Amanda Enterprise es el software para realizar respaldo de la información (Backup) que soporta Red Hat Enterprise Linux y permite a los administradores programar, configurar y ejecutar copias de seguridad con un entorno seguro y fácil de usar.	**BAJO**	Servidor de Adm. Y Backup	Servidor de Adm. Y Backup

ANEXO 4: MATRIZ DE CONSISTENCIA

PROBLEMAS	OBJETIVOS	HIPÓTESIS	VARIABLES	INDICADORES	INDICES
PROBLEMA PRINCIPAL ¿En qué medida una metodología basada en un enfoque SOA que desarrolle el Plan de Recuperación de Desastres (PRD), mejora el servicio de la Plataforma de Interoperabilidad (PI) en un Grupo Empresarial?	OBJETIVO GENERAL Mejorar el servicio de la PI en un Grupo Empresarial mediante el PRD.	HIPOTESIS GENERAL Si se desarrolla el Plan de Recuperación de Desastres para la Plataforma de Interoperabilidad, entonces mejorará el servicio de intercambio de información en el Grupo Empresarial.	VARIABLE INDEPENDIENTE X:Metodología basada en un enfoque SOA, del Plan de Recuperación de Desastres (PRD)	X_1: Nivel de cumplimiento de pruebas del PRD	$X_{1.1}$: Nro. de pruebas exitosas de Contexto / Nro. de pruebas totales de Contexto. Métricas → Contactos verificados por prueba $X_{1.2}$: Nro. de pruebas exitosas de Organización/Nro. de pruebas totales de Organización. Métricas → Actividades

PROBLEMAS SECUNDARIOS 1. ¿De qué manera el Análisis de Riesgo e Impacto de TI determina las vulnerabilidades, niveles de ocurrencia e impacto en la PI? 2. ¿De qué forma el Plan de Crisis minimiza el proceso de recuperación de desastres en la Plataforma de	OBJETIVOS ESPECIFICOS 1. Determinar las vulnerabilidades, niveles de ocurrencia e impacto mediante el Análisis de Riesgo y de Impacto de TI en la PI. 2. Minimizar el proceso de recuperación de desastres por medio del Plan	HIPÓTESIS ESPECIFICAS 1. Si se aplica el Análisis de Riesgo y de Impacto de TI entonces se determinarán las vulnerabilidades, niveles de ocurrencia e impacto a la PI 2. Si se implementa el Plan de Crisis entonces se minimizará el proceso de	VARIABLE DEPENDIENTE Y: Servicio de la PI.	Y_1: Continuidad de Servicio	verificadas por prueba $X_{1.3}$: Nro. de pruebas exitosas de Operación/Nro. de pruebas totales de Operación. Métricas → Parámetros verificados por prueba $Y_{1.1}$: Tiempo objetivo de recuperación (TOR)

Interoperabilidad? 3. ¿En qué medida el Plan de Contingencia y Recuperación asegura la continuidad del servicio de la PI.?	de Crisis en la PI. 3. Asegurar la continuidad del servicio de intercambio de información en la PI mediante el Plan de Contingencia y Recuperación.	recuperación de desastres en la PI. 3. Si se desarrolla el Plan de Contingencia y Recuperación se asegurará la continuidad del servicio de información en la PI.		Y_2: Disponibilidad de Servicio Y_3:Riesgo de TI	$Y_{2.1}$: Punto objetivo de recuperación (POR). $Y_{3.1}$: Nivel de Impacto de las amenazas $Y_{3.2}$: Nivel de ocurrencia de las amenazas $Y_{3.3}$: Nivel de vulnerabilidad de la PI

ISO/IEC 27001 (SGSI) ANEXO A[23]

(NORMATIVO)

OBJETIVOS DE CONTROL Y CONTROLES

Los objetivos de control y los controles que figuran en la tabla A.1 se derivan y alinean directamente con los que figuran en NTP ISO/IEC 17799:2006, capítulos 5 a 15. Las listas en estas tablas no son exhaustivas y la organización puede considerar que son necesarios objetivos de control y controles adicionales. Los objetivos de control y los controles de estas tablas deben seleccionarse como parte del proceso ISMS especificado en 4.2.1.

La NTP ISO/IEC 17799:2006, capítulos 5 a 15 ofrecen asesoría de implementación y pautas sobre las mejores prácticas en apoyo de los controles especificados de A.5 a A.15.

Tabla A.1 – Objetivos de control y controles

A.5 Política de seguridad

A.5.1 Política de seguridad de la información *Objetivo de control:* Ofrecer directivas de gestión y soporte en concordancia con los requerimientos del negocio y las regulaciones y leyes pertinentes.		
A.5.1.1	*Documentos de política de seguridad de la información*	Control El documento de políticas debe ser aprobado por la gerencia, publicado y comunicado, según sea apropiado, a todos los empleados y terceras partes que lo requieran.
A.5.1.2	*Revisión de la*	Control

[23] Norma Técnica Peruana NTP ISO/IEC 27001-2005, Sistema de Gestión de Seguridad de la Información ISMS

	política de seguridad de información	La política será revisada en intervalos planificados, y en caso de cambios que la afecten, asegurar que siga siendo apropiada, conveniente y efectiva.

A.6 Seguridad organizacional

A.6.1 Organización interna *Objetivo de control:* Gerenciar seguridad de la información dentro de la organización.		
A.6.1.1	*Comité de Gestión de seguridad de la información*	Control La gerencia debe respaldar activamente la seguridad dentro de la organización a través de una dirección clara, un compromiso apropiado, recursos adecuados y conocimiento de las responsabilidades en la seguridad de información.
A.6.1.2	*Coordinación de la seguridad de la información*	Control Las actividades en la seguridad de información deben ser coordinados por representantes de diferentes partes de la organización que tengan roles relevantes y funciones de trabajo.
A.6.1.3	*Asignación de responsabilidades sobre seguridad de la información*	Control Todas las responsabilidades sobre la seguridad de información deben ser claramente definidas.
A.6.1.4	*Proceso de autorización para las nuevas instalaciones de procesamiento de información*	Control Debe establecerse y definirse un proceso de autorización gerencial para las nuevas instalaciones de procesamiento de información.
A.6.1.5	*Acuerdos de*	Control

	confidencialidad	Se debería implementar e identificar regularmente los requerimientos de confidencialidad o los acuerdos de no acceso reflejando las necesidades de la organización para la protección de información.
A.6.1.6	*Contacto con autoridades*	Control Se debe mantener contactos apropiados con las autoridades pertinentes.
A.6.1.7	*Contacto con grupos de interés especial*	Control Se debe mantener contactos con grupos de interés especial u otros foros de especialistas en seguridad así como de asociaciones profesionales.
A.6.1.8	*Revisión independiente de seguridad de la información*	Control El alcance de la organización para manejar la seguridad de información, así como su implementación (como por ejemplo: los objetivos de control, los controles, las políticas, procesos y procedimientos) deben ser revisados independientemente durante intervalos planificados o cuando ocurran cambios significativos en la implementación.
A.6.2 Seguridad del acceso de terceros *Objetivo de control:* Mantener la seguridad de las instalaciones de procesamiento de la información organizacional que acceden, procesan, comunican o gestionan terceros.		
A.6.2.1	*Identificación de riesgos del acceso de terceros*	Control Se evaluará los riesgos asociados con el acceso a las instalaciones de procesamiento de la información organizacional por parte de terceros, y se implementarán controles de seguridad adecuados.
A.6.2.2	*Requerimientos de seguridad cuando se trata con*	Control Se deben identificar todos los requerimientos de seguridad

	clientes	antes de dar acceso a clientes a los activos o a la información de la organización.
A.6.2.3	*Requerimientos de seguridad en contratos con terceros*	Control Las negociaciones que involucran el acceso, procesamiento, comunicación o manejo de terceros de las instalaciones de procesamiento de información organizacional o la adición de productos o servicios a dichas instalaciones deben cubrir todos los requisitos de seguridad necesarios.

A.7 Gestión de activos

A.7.1 Responsabilidad por los activos *Objetivo de control:* Mantener la protección apropiada de los activos organizacionales.		
A.7.1.1	*Inventario de activos*	Control Se realizará y mantendrá un inventario de todos los activos importantes asociados con cada sistema de información.
A.7.1.2	*Propiedad de los activos*	Control Toda la información y los activos asociados con las instalaciones de procesamiento de información deben ser propiedad[24] de una parte designada de la organización.
A.7.1.3	*Uso aceptable de los activos*	Control Se deben de identificar, documentar e implementar las reglas para el uso aceptable de los activos de información asociados con las instalaciones de

[24] El término "propietario" identifica a un individuo o entidad que aprueba la responsabilidad por la gestión por controlar la producción, desarrollo, mantenimiento, uso y seguridad de los activos. El término "propietario" no significa que la persona tiene algún derecho de propiedad realmente sobre el activo.

		procesamiento de información.
A.7.2 Clasificación de la información *Objetivo de control:* Asegurar que los activos de información reciban un nivel de protección adecuado.		
A.7.2.1	*Guías de clasificación*	Control La información debe ser clasificada en términos de su valor, requisitos legales, sensibilidad y criticidad para la organización.
A.7.2.2	*Marcado y tratamiento de la información*	Control Se definirá e implementará un conjunto de procedimientos apropiados para etiquetar y manejar información de conformidad con el esquema de clasificación adoptado por la organización.

A.8 Seguridad personal

A.8.1 Seguridad antes del empleo[25] *Objetivo de control:* Asegurar que los empleados, contratistas y usuarios externos entiendan sus responsabilidades y que estos sean adecuados a los roles para los cuales han sido considerados y reducir así el riesgo de estafa, fraude o mal uso de las instalaciones.		
A.8.1.1	*Roles y responsabilidades*	Control Se documentarán y definirán los roles de seguridad y las responsabilidades de los empleados, contratistas y usuarios externos en concordancia con la política de seguridad de la información de la organización.
A.8.1.2	*Investigación*	Control

[25] Explicación: la palabra "empleo" se utiliza aquí para cubrir las siguientes situaciones diferentes: empleo de las personas (temporalmente o durante largo tiempo), designando roles de trabajo, cambiando roles de trabajo, asignando contratos, y la terminación de cualquiera de estos arreglos.

		Se llevarán a cabo verificaciones del personal de planta, contratistas y personal temporal al momento de solicitar el trabajo, en concordancia con las leyes, regulaciones y ética; y proporcional a los requisitos del negocio, la clasificación de la información a ser accedida y a los riesgos percibidos.
A.8.1.3	*Términos y condiciones de la relación laboral*	Control Los empleados, contratistas y terceros suscribirán un acuerdo de confidencialidad como parte de los términos y condiciones iniciales de su empleo en donde se señalará la responsabilidad del empleado en cuanto a la seguridad de la información.
A.8.2 Durante el empleo *Objetivo de control:* Asegurar que todos los empleados, contratistas y usuarios externos sean conscientes de las amenazas y riesgos en el ámbito de la seguridad de la información, y que estén preparados para sostener la política de seguridad de la organización en el curso de trabajo normal y reducir el riesgo de error humano.		
A.8.2.1	*Gestión de responsabilidades*	Control La gerencia debe requerir a los empleados, contratistas y a los usuarios externos aplicar la seguridad en concordancia con las políticas y procedimientos de la organización.
A.8.2.2	*Puesta al tanto, educación y entrenamiento en la seguridad de información*	Control Todos los empleados de la organización y, donde sea relevante, contratistas y terceras partes deben estar al tanto y recibir un entrenamiento apropiado y actualizaciones.
A.8.2.3	*Proceso disciplinario*	Control Debe existir un proceso disciplinario para los empleados que hayan cometido una violación de seguridad.

A.8.3 Finalización o cambio de empleo *Objetivo de control:* Asegurar que los empleados, contratistas y usuarios externos dejen o cambien de organización de una forma ordenada.		
A.8.3.1	*Responsabilidades de finalización*	Control Debe informarse sobre los incidentes de seguridad a través de canales administrativos adecuados tan pronto como sea posible.
A.8.3.2	*Devolución de activos*	Control Todos los empleados, contratistas y usuarios externos deben realizar la devolución de los activos de la organización que están en su posesión cuando termine su empleo, contrato o acuerdo.
A.8.3.3	*Retiro de los derechos de acceso*	Control El derecho de acceso a la información y a las instalaciones de procesamiento de información, que se le otorga a los empleados, contratistas y usuarios externos, debe ser removido cuando termine su empleo, contrato o acuerdo; o modificado ante cambios.

A.9 Seguridad física y del entorno

A.9.1 Áreas seguras *Objetivo de control:* Evitar accesos no autorizados, daños e interferencias contra los locales y la información del negocio.		
A.9.1.1	*Perímetro de seguridad física*	Control Las organizaciones usarán perímetros de seguridad (barreras como paredes, puertas con control de entrada

		por tarjeta o recepciones) para proteger áreas que contienen información e instalaciones de procesamiento de información.
A.9.1.2	*Controles físicos de entradas*	Control Las áreas seguras estarán protegidas mediante controles de acceso adecuados para garantizar que únicamente personal autorizado pueda ingresar.
A.9.1.3	*Seguridad de oficinas, despachos y recursos*	Control Se deben designar y mantener áreas seguras con el fin de proteger las oficinas, despachos e instalaciones.
A.9.1.4	*Protección contra amenazas externas y ambientales*	Control Se deben designar y mantener protección física contra daños por fuego, inundación, terremoto, explosión, manifestación civil y otras formas de desastre natural o realizado por el hombre.
A.9.1.5	*El trabajo en las áreas seguras*	Control Se debe designar y mantener protección física y pautas para trabajar en áreas seguras.
A.9.1.6	*Áreas aisladas de carga y descarga*	Control Las áreas de carga y descarga deben controlarse y, cuando sea posible, aislarse de las instalaciones de procesamiento de información para evitar un acceso no autorizado.
A.9.2 Seguridad de los equipos *Objetivo de control:* Prevenir pérdidas, daños o comprometer los activos así como la interrupción de las actividades del negocio.		
A.9.2.1	*Instalación y*	Control

	protección de equipos	El equipamiento será ubicado o protegido para reducir los riesgos de amenazas, peligros ambientales y oportunidades de acceso no autorizado.
A.9.2.2	*Suministro eléctrico*	Control El equipamiento se protegerá de fallas de energía y otras anomalías eléctricas causadas por fallo en el suministro eléctrico.
A.9.2.3	*Seguridad del cableado*	Control Se protegerá el cableado de energía y telecomunicaciones que transportan datos o respaldan servicios de información frente a interceptaciones o daños.
A.9.2.4	*Mantenimiento de equipos*	Control El equipamiento recibirá un adecuado mantenimiento para garantizar su continua disponibilidad e integridad.
A.9.2.5	*Seguridad de equipos fuera de los locales de la organización*	Control Se debe aplicar seguridad al utilizar equipamiento para procesar información fuera de los locales de la organización tomando en cuenta los diferentes riesgos en los que se incurre.
A.9.2.6	*Seguridad en el re-uso o eliminación de equipos*	Control Todos los equipos que contienen almacenamiento de datos deben ser revisados con el fin de asegurar que los datos sensibles y el software con licencia han sido removidos o sobrescritos antes de desecharlos o reutilizarlos.
A.9.2.7	*Retiro de propiedad*	Control

		Los equipos, información y software no deben ser retirados fuera de la organización sin una autorización previa.

A.10 Gestión de comunicaciones y operaciones

A.10.1 Procedimientos y responsabilidades de operación *Objetivo de control:* Asegurar la operación correcta y segura de los recursos de procesamiento de información.		
A.10.1.1	*Documentación de procedimientos operativos*	Control Los procedimientos operativos identificados en la política de seguridad serán documentados y mantenidos y estarán disponibles a todos los usuarios que lo requieran.
A.10.1.2	*Gestión de cambios*	Control Se controlarán los cambios en las instalaciones y sistemas de procesamiento de la información.
A.10.1.3	*Segregación de tareas*	Control Se segregarán las obligaciones y las áreas de responsabilidad con el fin de reducir las oportunidades de modificaciones no autorizadas o mal uso de los activos de la organización.
A.10.1.4	*Separación de los recursos para desarrollo y para producción*	Control Se separarán las instalaciones de prueba y desarrollo de las instalaciones de producción con el fin de reducir el riesgo de acceso no autorizado o de modificación no intencionada o cambios en el sistema operacional.

A.10.2 Gestión de entrega de servicios externos *Objetivo de control:* Implementar y mantener un nivel apropiado de seguridad de información		
A.10.2.1	*Entrega de servicios*	Control Debemos asegurarnos que los controles de seguridad, las definiciones de servicio y los niveles de entrega incluidos en el acuerdo de servicios externos sean implementados, estén operativos y sean mantenidos por el personal externo.
A.10.2.2	*Monitoreo y revisión de los servicios externos*	Control Los servicios, reportes, y registros provistos por terceras partes deben ser monitoreados y revisados regularmente. Igualmente, se deben de llevar a cabo auditorias con regularidad.
A.10.2.3	*Gestión de cambios de los servicios externos*	Control Se debe manejar los cambios en la provisión de servicios, incluyendo el mantenimiento y mejora de la política de seguridad de información, procedimientos y controles, tomando en cuenta la criticidad de los sistemas de negocio y procesos envueltos en la reevaluación de riesgos.
A.10.3 Planificación y aceptación del sistema *Objetivo de control:* Minimizar el riesgo de fallas de los sistemas.		
A.10.3.1	*Gestión de la capacidad*	Control Se monitorearán las demandas de capacidad y se harán las proyecciones de futuros requerimientos de capacidad para asegurar el desarrollo requerido por el sistema.
A.10.3.2	*Aceptación del sistema*	Control

		Establecerán los criterios de aceptación para sistemas de información nuevos, actualizaciones y nuevas versiones y se llevarán a cabo pruebas adecuadas del sistema antes de la aceptación.
A.10.4 Protección contra software malicioso *Objetivo de control:* Proteger la integridad del software y de la información.		
A.10.4.1	*Controles contra software malicioso*	Control Para ofrecer protección frente a software malicioso, se implementarán controles de detección, prevención y procedimientos adecuados de toma de conciencia con los usuarios.
A.10.4.2	*Controles contra software móvil*	Control Donde sea autorizado el uso de software móvil, la configuración debe asegurar que este opere de acuerdo a una política de seguridad clara y definida. Igualmente, se debe prevenir la ejecución de código móvil no autorizado.
A.10.5 Gestión interna de respaldo y recuperación *Objetivo de control:* Mantener la integridad y disponibilidad del procesamiento de información y servicios de comunicación.		
A.10.5.1	*Recuperación de la información*	Control Se obtendrán y probarán las copias de recuperación y respaldo de información y software regularmente en concordancia con la política acordada.
A.10.6 Gestión de seguridad de redes *Objetivo de control:* Asegurar la salvaguarda de información en las redes y la protección de la infraestructura de soporte.		

A.10.6.1	*Controles de red*	Control Se implementará un conjunto de controles para lograr y mantener la seguridad en las redes, y mantener la seguridad de los sistemas y aplicaciones usuarios de la red, incluyendo la información en tránsito.
A.10.6.2	*Seguridad de los servicios de red*	Control Se deben identificar e incluir en cualquier acuerdo de servicio de red los aspectos de seguridad, niveles de servicio y requisitos de gestión, así estos servicios sean provistos interna o externamente.
A.10.7 Utilización y seguridad de los medios de información *Objetivo de control:* Prevenir daños, modificaciones o destrucciones a los activos e interrupciones de las actividades del negocio.		
A.10.7.1	*Gestión de medios removibles*	Control Deben de existir procedimientos para la gestión de medios removibles.
A.10.7.2	*Eliminación de medios*	Control Se eliminarán los medios con seguridad y garantía cuando ya no se necesiten, utilizando procedimientos formales.
A.10.7.3	*Procedimientos de manipulación de la información*	Control Se establecerán procedimientos para el manejo y almacenamiento de la información con el fin de proteger dicha información de divulgaciones no autorizadas o su mal uso.
A.10.7.4	*Seguridad de la documentación de sistemas*	Control La documentación del sistema se protegerá de accesos

		no autorizados.
A.10.8 Intercambio de información y software *Objetivo de control:* Mantener la seguridad de información y el intercambio de software dentro de la organización y con entidades externas.		
A.10.8.1	*Políticas y procedimientos para el intercambio de información*	Control Se deben establecer políticas, procedimientos y controles para proteger el intercambio de información durante el uso de todo tipo de recursos de comunicación.
A.10.8.2	*Acuerdos de intercambio*	Control Se deben de establecer acuerdos para el intercambio de información y software entre la organización y entidades externas.
A.10.8.3	*Seguridad de medios físicos en tránsito*	Control Los medios a ser transportados deberán ser protegidos de acceso no autorizado, mal uso o corrupción durante su transporte fuera de las barreras físicas de la organización.
A.10.8.4	*Seguridad del correo electrónico*	Control La información envuelta en correos electrónicos debe ser protegida apropiadamente.
A.10.8.5	*Seguridad en los sistemas de información de negocio*	Control Se deben desarrollar e implementar políticas y procedimientos para proteger la información asociada con la interconexión de los sistemas de información de negocios.

A.10.9 Servicios de comercio electrónico *Objetivo de control:* Mantener la seguridad en los servicios de comercio electrónico y la seguridad en su uso.		
A.10.9.1	*Seguridad en comercio electrónico*	Control El comercio electrónico será protegido frente a actividades fraudulentas, controversias contractuales y divulgación o modificación de información.
A.10.9.2	*Seguridad en las transacciones en línea*	Control La información envuelta en las transacciones en línea debe ser protegida para prevenir transmisiones incompletas, rutas incorrectas, alteración no autorizada de mensajes, o duplicación no autorizada de mensajes.
A.10.9.3	*Sistemas públicamente disponibles*	Control Se protegerá la integridad de la información públicamente disponible para prevenir modificaciones no autorizadas.
A.10.10 Monitoreo *Objetivo de control:* Mantener la seguridad en los servicios de comercio electrónico y en su uso.		
A.10.10.1	*Registro de auditoria*	Control Se deben producir y guardar, por un periodo acordado, los registros de auditoría que registran las actividades de los usuarios, excepciones y eventos de seguridad, con el fin de asistir a investigaciones futuras y al monitoreo del control de acceso.
A.10.10.2	*Uso del sistema de*	Control

	monitoreo	Se deben establecer procedimientos para monitorear las instalaciones de procesamiento de información y los resultados del monitoreo de actividades deben ser revisados regularmente.
A.10.10.3	*Protección de la información de registro*	Control Las instalaciones e información de registro deben ser protegidas contra acceso forzado y no autorizado.
A.10.10.4	*Registros de administrador y operador*	Control Las actividades del administrador y operadores deben ser registradas.
A.10.10.5	*Registros con faltas*	Control Las faltas deben ser registradas, analizadas y se deben tomar acciones apropiadas.
A.10.10.6	*Sincronización de reloj*	Control Los relojes de todos los sistemas relevantes de procesamiento de información dentro de la organización deben estar sincronizados con una fuente de tiempo actual acordado.

A.11 Control de accesos

A.11.1 Requisitos de negocio para el control de accesos *Objetivo de control:* Controlar los accesos a la información.		
A.11.1.1	*Política de control de accesos*	Control Se debe establecer, documentar y revisar una política de control de accesos, basado en requisitos de acceso de seguridad y del negocio.

A.11.2 Gestión de acceso de usuarios *Objetivo de control:* Asegurar que el acceso de usuarios es autorizado y prevenir el acceso no autorizado a los sistemas de información.		
A.11.2.1	*Registro de usuarios*	Control Habrá un procedimiento de registro y anulación formal de usuarios para otorgar acceso a todos los sistemas de información multiusuario y servicios.
A.11.2.2	*Gestión de privilegios*	Control Se restringirá y controlará la asignación y uso de privilegios.
A.11.2.3	*Gestión de contraseñas de usuario*	Control Se controlará la asignación de contraseñas a través de un proceso formal de gestión.
A.11.2.4	*Revisión de los derechos de acceso de los usuarios*	Control La gerencia conducirá un proceso formal y de manera periódica para revisar los derechos de acceso del usuario.
A.11.3 Responsabilidades de los usuarios *Objetivo de control:* Evitar el acceso no autorizado de usuarios y el compromiso o robo de la información o de las instalaciones de procesamiento.		
A.11.3.1	*Uso de contraseñas*	Control Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas.
A.11.3.2	*Equipo informático de usuario desatendido*	Control Se exige al usuario que asegure protección adecuada a un equipo desatendido.

A.11.3.3	*Política de pantalla y escritorio limpio*	Control Se debe adoptar una política de escritorio limpio para papeles y dispositivos de almacenamiento removibles. Igualmente, se debe adoptar una política para las instalaciones de procesamiento de información.
A.11.4 Control de acceso a la red *Objetivo de control: Prevenir el acceso no autorizado a los servicios de red.*		
A.11.4.1	*Política de uso de los servicios de la red*	Control Los usuarios deben tener acceso directo únicamente a los servicios cuyo uso está específicamente autorizado.
A.11.4.2	*Autenticación de usuarios para conexiones externas*	Control El acceso de usuarios remotos debe estar sujeto a autenticación.
A.11.4.3	*Autenticación de equipos en la red*	Control Se debería considerar equipos de identificación automática para autentificar conexiones desde ubicaciones y equipos específicos.
A.11.4.4	*Protección a puertos de diagnóstico y configuración remota*	Control Debe controlarse la seguridad en el acceso a los puertos de diagnóstico físico y lógico.
A.11.4.5	*Segregación en las redes*	Control Los grupos de servicios, usuarios y sistemas de información deben ser segregados en las redes.
A.11.4.6	*Control de conexión*	Control

	a las redes	La capacidad de conexión de los usuarios de redes compartidas, especialmente aquellas que se extienden fuera de las fronteras de la organización, debe restringirse de conformidad con la política de control de acceso y los requisitos de las aplicaciones de negocio (véase 11.1).
A.11.4.7	*Control de enrutamiento en la red*	Control Se deben implementar controles de ruteo para asegurar que las conexiones de computadora y los flujos de información no violen la política de control de acceso de las aplicaciones de negocios.
A.11.5 Control de acceso al sistema operativo *Objetivo de control:* Prevenir accesos no autorizados a los sistemas operativos.		
A.11.5.1	*Procedimientos seguros de conexión*	Control Se usará un proceso de registro de conexión (login) seguro para acceder a los servicios de información.
A.11.5.2	*Identificación y autenticación del usuario*	Control Todos los usuarios tienen un identificador único para su uso propio y exclusivo para sus actividades y debe elegirse una técnica de autenticación adecuada para sustentar la identidad del usuario.
A.11.5.3	*Sistema de gestión de contraseñas*	Control Sistemas de gestión de contraseñas proveerán medios efectivos e interactivos, cuyo objetivo es asegurar contraseñas de calidad.
A.11.5.4	*Uso de los programas utilitarios del sistema*	Control Se debe registrar y controlar firmemente el uso de programas utilitarios que puedan ser capaces de forzar el sistema y los controles de aplicación.

A.11.5.5	*Desconexión automática de terminales*	Control Las sesiones inactivas deben cerrarse luego de un periodo definido de inactividad.
A.11.5.6	*Limitación del tiempo de conexión*	Control Se usará restricciones de tiempos de conexión para ofrecer seguridad adicional para las aplicaciones de alto riesgo.
A.11.6 Control de acceso a las aplicaciones e información *Objetivo de control:* Evitar el acceso no autorizado a la información contenida en los sistemas.		
A.11.6.1	*Restricción de acceso a la información*	Control El acceso a las funciones de información y de aplicación por usuarios y personal de soporte serán restringidos con la política de control de acceso.
A.11.6.2	*Aislamiento de sistemas sensibles*	Control Los sistemas sensibles tendrán un ambiente de cómputo dedicado (aislado).
A.11.7 Informática móvil y teletrabajo *Objetivo de control:* Garantizar la seguridad de la información cuando se usan dispositivos de informática móvil y facilidades de teletrabajo.		
A.11.7.1	*Informática y comunicaciones móviles*	Control Se pondrá en práctica una política formal y se adoptarán los controles adecuados para protegerse frente a los riesgos de trabajar con puntos de computadores móviles y medios de comunicación.
A.11.7.2	*Teletrabajo*	Control

		Se desarrollarán e implementaran políticas, procedimientos y estándares para las actividades de teletrabajo.

A.12 Adquisición de sistemas de información, desarrollo y mantenimiento

***A.12.1 Requisitos de seguridad de los sistemas* de información** *Objetivo de seguridad:* Garantizar que la seguridad esté incluida dentro de los sistemas de información.		
A.12.1.1	*Análisis y especificación de los requisitos de seguridad*	Control Los requisitos de negocios para nuevos sistemas, o ampliaciones de los sistemas existentes, especificarán los requisitos de control.
A.12.2 Proceso correcto en aplicaciones *Objetivo de control:* Prevenir errores, pérdidas, modificaciones no autorizadas o mal uso de los datos del usuario en las aplicaciones.		
A.12.2.1	*Validación de los datos de entrada*	Control Se validará el ingreso de datos a los sistemas de aplicación para asegurar que sean correctos y adecuados.
A.12.2.2	*Control del proceso interno*	Control Se incorporarán verificaciones y validaciones para detectar cualquier corrupción de los datos procesados.
A.12.2.3	*Integridad de mensajes*	Control Se deben identificar requisitos para la autenticación y

		protección de la integridad de mensajes. Igualmente, se deben implementar e identificar controles apropiados.
A.12.2.4	*Validación de los datos de salida*	Control Los datos de salida de una aplicación se validarán para garantizar que el procesamiento de la información almacenada sea correcto y adecuado a las circunstancias.
A.12.3 Controles criptográficos *Objetivo de control:* Proteger la confidencialidad, autenticidad o integridad de los medios criptográficos.		
A.12.3.1	*Política de uso de los controles criptográficos*	Control Debe desarrollarse e implementarse una política sobre el uso de controles criptográficos para proteger la información.
A.12.3.2	*Gestión de claves*	Control Se usará un sistema de gestión de claves con el fin de apoyar el uso de técnica criptográfica dentro de la organización.

A.12.4 Seguridad de los archivos del sistema *Objetivo de control:* Asegurar la seguridad de los archivos del sistema.		
A.12.4.1	*Control del software en producción*	Control Se pondrá en práctica procedimientos para controlar la implementación del software en sistemas operacionales.
A.12.4.2	*Protección de los datos de prueba del*	Control

	sistema	Se protegerán y controlarán los datos de prueba los cuales deben ser seleccionados cuidadosamente.
A.12.4.3	*Control de acceso a la librería de programas fuente*	Control El acceso a las librerías de programas fuente debe ser restringido.
A.12.5 Seguridad en los procesos de desarrollo y soporte *Objetivo de control:* Mantener la seguridad del software de aplicación y la información.		
A.12.5.1	*Procedimientos de control de cambios*	Control La implementación de cambios se controlará estrictamente mediante el uso de procedimientos formales de control de cambios.
A.12.5.2	*Revisión técnica de los cambios en el sistema operativo*	Control Cuando los sistemas operativos son cambiados, se deben de revisar y probar las aplicaciones críticas de negocio con el fin de asegurar que no existan impactos adversos en las operaciones o seguridad de la organización.
A.12.5.3	*Restricciones en los cambios a los paquetes de software*	Control No se debe fomentar las modificaciones en los paquetes. Se debe limitar a cambios necesarios y todos estos cambios deben ser estrictamente controlados.
A.12.5.4	*Fuga de información*	Control Se deben de prevenir las oportunidades de fuga de información.

A.12.5.5	*Desarrollo externo del software*	Control La organización debe supervisar y monitorear el desarrollo externo de software.
A.12.6 ***Gestión de vulnerabilidades técnicas*** *Objetivo de control:* Reducir los riesgos que son el resultado de la explotación de vulnerabilidades técnicas publicadas.		
A.12.6.1	*Control de vulnerabilidades técnicas*	Control Se debe obtener información a tiempo sobre las vulnerabilidades técnicas de los sistemas de información que se utilizan. La exposición de la organización a tales vulnerabilidades debe ser evaluada y se debe tomar medidas apropiadas asociadas al riesgo.

A.13 Gestión de incidentes en la seguridad de información

A.13.1 Reportando eventos y debilidades en la seguridad de información *Objetivo de control:* Asegurar que los eventos y debilidades en la seguridad de información asociados con los sistemas de información sean comunicados de manera tal que permitan tomar una acción correctiva a tiempo.		
A.13.1.1	*Reportando eventos de la seguridad de información*	Control Los eventos en la seguridad de información deben ser reportados lo más rápido posible a través de canales apropiados.
A.13.1.2	*Reportando debilidades de seguridad*	Control Todos los empleados, contratistas o personal externo usuario de los sistemas y servicios de información, deben estar obligados de notar y reportar cualquier debilidad en la seguridad de los sistemas y servicios.

A.13.2 Gestión de los incidentes y mejoras en la seguridad de información *Objetivo de control:* Asegurar que un alcance consistente y efectivo sea aplicado en la gestión de incidentes de la seguridad de información.		
A.13.2.1	*Responsabilidades y procedimientos*	Control. Se deben de establecer procedimientos y responsabilidades de gestión con el fin de asegurar una respuesta rápida, efectiva y ordenada ante incidentes en la seguridad de información.
A.13.2.2	*Aprendiendo de los incidentes en la seguridad de información*	Control Deben existir mecanismos que habiliten que los tipos, volúmenes y costos de los incidentes en la seguridad de información sean cuantificados y monitoreados.
A.13.2.3	*Recolección de evidencia*	Control Cuando exista una acción de seguimiento contra una persona u organización, luego de que un incidente en el sistema de información envuelva acción legal (civil o criminal), se debe de recolectar, retener y presentar evidencia conforme con las reglas dentro de la jurisdicción.

A.14 Gestión de la continuidad del negocio

A.14.1 Aspectos de la gestión de continuidad del negocio en la seguridad de información *Objetivo de control:* Neutralizar las interrupciones a las actividades del negocio y proteger los procesos críticos del negocio de los efectos de fallas mayores o desastres en los sistemas de información y asegurar su reanudación oportuna.		
A.14.1.1	*Incluyendo la seguridad de la información en la gestión de la continuidad del*	Control Se deben de establecer procedimientos y responsabilidades de gestión con el fin de asegurar una respuesta rápida, efectiva y ordenada ante

	negocio	incidentes en la seguridad de la información.
A.14.1.2	*Continuidad del negocio y evaluación de riesgos*	Control Los eventos que pueden causar interrupciones en los procesos del negocio deben ser identificados así como las probabilidades e impacto de dichas interrupciones y sus consecuencias para la seguridad de la información.
A.14.1.3	*Desarrollando e implementando planes de continuidad que incluyen la seguridad de la información*	Control Se deben desarrollar e implementar planes para mantener o reparar operaciones y asegurar la disponibilidad de información al nivel y tiempo requerido, siguiendo las interrupciones o fallas a los procesos críticos del negocio.
A.14.1.4	*Marco de planificación de la continuidad del negocio*	Control Un simple marco de los planes de continuidad del negocio debe ser mantenido para asegurar que todos los planes sean consistentes, que anexen consistentemente los requisitos de seguridad de la información, para identificar prioridades de prueba y mantenimiento.
A.14.1.5	*Probando, manteniendo y reevaluando los planes de continuidad del negocio*	Control Los planes de continuidad del negocio deben ser probados y actualizados regularmente con el fin de asegurar que se encuentren actuales y que sean efectivos.

A.15 Cumplimiento

A.15.1 Cumplimiento de los requisitos legales *Objetivo de control:* Evitar los incumplimientos de cualquier ley civil o penal, requerimiento reglamentario, regulación u obligación contractual, y de cualquier requerimiento de seguridad.		
A.15.1.1	*Identificación de la legislación aplicable*	Control Se definirán y documentaran explícitamente todos los requerimientos legales, regulatorios y contractuales relevantes y se deben mantener actualizados cada sistema de información.
A.15.1.2	*Derechos de propiedad intelectual (DPI)*	Control Se implementarán procedimientos adecuados para garantizar el cumplimiento de las restricciones legales en el uso de material con respecto a derechos de propiedad intelectual y uso de productos de software propietario.
A.15.1.3	*Salvaguarda de los registros de la organización*	Control Se protegerán los registros importantes de la organización frente a pérdidas, destrucción y falsificación en concordancia con los requisitos regulatorios, contractuales y de negocio.
A.15.1.4	*Protección de los datos y privacidad de la información personal*	Control Se aplicarán controles para proteger información personal en conformidad con la legislación correspondiente y si es aplicable, con las cláusulas contractuales.
A.15.1.5	*Prevención en el mal uso de las instalaciones de procesamiento de*	Control Los usuarios deben ser disuadidos de utilizar las instalaciones del procesamiento de información para

	la información	propósitos no autorizados.
A.15.1.6	*Regulación de los controles criptográficos*	Control Se implementarán controles para permitir el cumplimiento de los acuerdos nacionales, leyes y reglamentos.
A.15.2 Cumplimiento con las políticas y estándares de seguridad y del cumplimiento técnico *Objetivo de control:* Asegurar el cumplimiento de los sistemas con las políticas y normas de seguridad organizacionales.		
A.15.2.1	*Cumplimiento con la política de seguridad*	Control Los gerentes deben tomar acciones para garantizar que todos los procedimientos de seguridad dentro de sus áreas de responsabilidad se lleven a cabo correctamente con el fin de garantizar el cumplimiento de las políticas y estándares de seguridad.
A.15.2.2	*Comprobación del cumplimiento técnico*	Control Debe verificarse regularmente el cumplimiento de la implementación de normas de seguridad en los sistemas de información.
A.15.3 Consideraciones sobre la auditoria de sistemas *Objetivo de control:* Maximizar la efectividad y minimizar las interferencias en el proceso de auditoría del sistema		
A.15.3.1	*Controles de auditoría de sistemas*	Control Se planificarán cuidadosamente las auditorias de los sistemas operacionales a fin de minimizar el riesgo de interrupciones a los procesos de negocio.
A.15.3.2	*Protección de las herramientas de auditoría de sistemas*	Control Se protegerá el acceso a las herramientas de auditoría del sistema para prevenir cualquier posible mal uso o daño.