ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

ESCUELA DE DISEÑO Y COMUNICACIÓN VISUAL

PROYECTO DE GRADUACIÓN

PREVIO A LA OBTENCIÓN DEL TÍTULO DE
ANALISTA DE SISTEMAS

TEMA
"IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD PARA UNA EMPRESA INMOBILIARIA USANDO LOS CONTROLES DE LA ISO 27001"

AUTORES
LUIS ALBERTO CEPEDA FERNÁNDEZ
JHONNY AUGUSTO PLÚAS RONQUILLO
BYRON RODRIGO ZAMORA ZAMORA

DIRECTOR

AÑO
2011

AGRADECIMIENTO

Agradecemos a Dios, y a nuestras familias por su apoyo incondicional, el mismo que nos ha otorgado las fuerzas suficientes para culminar con nuestra carrera, agradecemos también a nuestros profesores y compañeros, por los conocimientos y las experiencias que hemos recibido y hemos compartido con ellos a lo largo de estos años.

Luis Cepeda Fernández.
Jhonny Plúas Ronquillo.
Byron Zamora Zamora.

DEDICATORIA

Dedicamos este trabajo a nuestros padres, hermanos y demás familiares quienes nos apoyaron a través de este largo camino lleno de esfuerzo y sacrificio, y que concluye con la entrega satisfactoria de este proyecto.

A todos nuestros profesores a quienes recordaremos con afecto por ayudarnos a convertirnos en profesionales competitivos, con visión emprendedora, finalmente a todos los quienes olvidamos mencionar pero llevamos en nuestros corazones, Gracias.

Luis Cepeda Fernández.
Jhonny Plúas Ronquillo.
Byron Zamora Zamora.

Firma del Director del Proyecto y Miembros de Tribunal De Graduación

_____

Ing. Víctor Muñoz Chachapoya.
Director de la Materia de graduación

_____

Delegado

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de este Proyecto de Graduación, nos corresponde exclusivamente; y el patrimonio intelectual del mismo a la ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL".

RESUMEN EJECUTIVO

Este trabajo detalla los procesos de la Gestión de Seguridad de la Información basándonos en el dominio de Continuidad del negocio aplicando los controles de la norma ISO/IEC 270001 el cual permitirá minimizar el riesgo ocasionado por posibles amenazas internas y externas que nos ayudara a proporcionar soluciones rápidas y efectivas para asegurar el uso estructurado de recursos.

Con el presente trabajo, no se busca preparar a la empresa inmobiliaria para una eventual certificación en materia de seguridad de la información, sino que proporciona las bases de un SGSI para que una vez implementado, se pueda aprovechar los beneficios que éste ofrece.

Como objetivo primordial es restablecer el servicio lo más rápido posible para evitar que los clientes se vean afectados esto se hace con la finalidad de que se minimicen los efectos de la operación. Mediante el proceso de manejo de incidentes se da como primera etapa la detección del incidente ya que lo tenemos identificado se hace una clasificación del incidente que permitirá realizar la solicitud de cambio el cual implica implementar la solución y finalmente será evaluado, esta solución pasara a la documentación como normas de la empresa.

Este método adopta un enfoque basado en procesos, para establecer, implementar, operar, hacer seguimiento, mantener y mejorar el Modelo de Seguridad de la Información y estar orientado a todos los actores y entidades involucradas que permite mantener un proceso de mejora continua brindando una seguridad razonable.

Es recomendable que todas las fases del plan de continuidad de negocios se cuenten con el apoyo correspondiente por parte de las altas autoridades de la empresa inmobiliaria.

ÍNDICE GENERAL

CAPÍTULO 1

CAPÍTULO 2

CAPÍTULO 3

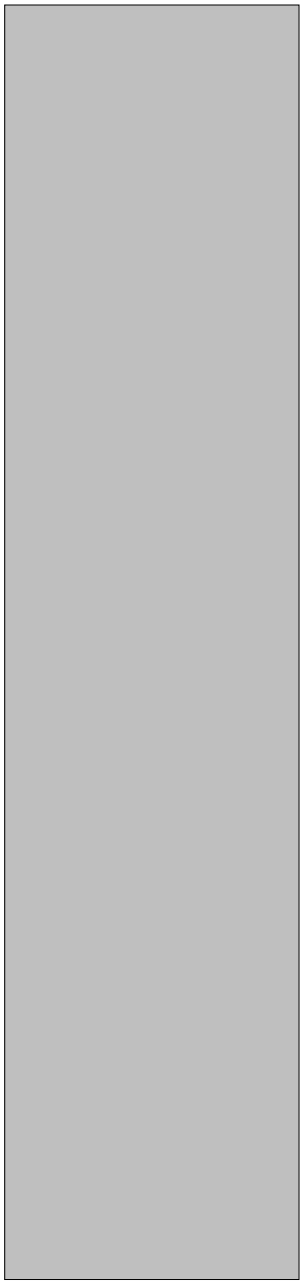
CAPÍTULO 4

CAPÍTULO 5

CAPÍTULO 6

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS



CAPÍTULO 1
INTRODUCCIÓN

1 INTRODUCCIÓN

1.1 VERSIÓN DEL DOCUMENTO

VERSIÓN	FECHA	No. SOLICITUD	RESPONSABLE	DESCRIPCIÓN
1	15/03/2011		Ing. Luis Rodríguez	Borrador del Sistema de Gestión de Seguridad de la Información en el Control de Acceso.
2	27/04/2011		Ing. Luis Muñoz	Presentación de avances del plan de continuidad de negocio.
3	30/04/2011		Ing. Luis Muñoz	Mejoramiento del plan de continuidad del negocio.
4	03/05/2011		Ing. Luis Muñoz	Mejorar Formato e imprimir borrador

Tabla 1-1: Versiones del Documento

1.2 GENERALIDADES

Este trabajo detalla los procesos de la Gestión de Seguridad de la Información del data-center de una empresa inmobiliaria basándonos en el dominio de Continuidad del negocio aplicando los controles de la norma ISO/IEC 270001 necesarios ante las amenazas que pueden interrumpir o afectar la continuidad de los procesos.

Elaborar el diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) para la empresa inmobiliaria, así como también presentar las respectivas recomendaciones para su posterior implementación dentro del alcance del presente trabajo.

Dentro del conjunto de beneficios que se obtendrían al contar con un SGSI se pueden mencionar como:

- Contar con un proceso definido para: Evaluar, Implementar, Mantener y Administrar la Seguridad de la Información en la empresa.
- Diferenciarse en el mercado de otras empresas urbanísticas.
- Tener una metodología para poder administrar los riesgos sobre la información que enfrenta.

Con el presente trabajo, no se busca preparar a la empresa inmobiliaria para una eventual certificación en materia de seguridad de la información, sino que proporciona las bases de un SGSI para que una vez implementado, se pueda aprovechar los beneficios que éste ofrece.

1.3 ANTECEDENTES

Cuando hablamos de seguridad de información, debemos considerar a la información como un activo crítico de las organizaciones y como tal se debe preservar su integridad, confidencialidad y disponibilidad. No es posible eliminar por completo los riesgos, sin embargo es posible reducirlos mediante controles de protección contra amenazas y vulnerabilidades.

En estos tiempos, es importante que las empresas cuenten con un Sistema de Gestión de Seguridad de Información (SGSI), que les facilite el establecer, implementar, operar, monitorear y mantener la seguridad de la información de sus empresas, es por tal razón que la empresa inmobiliaria, no puede dejar de lado este tema.

La empresa inmobiliaria no está libre de sufrir ataques informáticos, pérdida de enlaces, descargas eléctricas, desastres naturales como incendio, terremotos, inundaciones entre otros. Una de las amenazas más comunes que ocurren son las descargas eléctricas donde se reporta la pérdida de información como transacciones realizadas de las ventas, mediante a esas amenazas debemos aplicar procesos que minimice el riesgo para reanudar las actividades en el menor tiempo posible.

1.4 INTRODUCCIÓN DE LA SEGURIDAD DE INFORMACIÓN

Hoy en día la información es un recurso como el resto de los importantes activos comerciales, tiene valor para una organización y por consiguiente debe ser debidamente protegida. La seguridad de la información protege ésta de una amplia gama de amenazas, fraudes asistidos por computadora, espionaje, sabotaje, vandalismo, incendios o inundaciones, daños provocados por virus informáticos, hacking, etc., a fin de garantizar la continuidad comercial, minimizar el daño al mismo y maximizar el retorno sobre las inversiones y las oportunidades.
La información se puede presentar o existir en varias formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, presentada en imágenes, o expuesta en una conversación. Cualquiera sea la forma que adquiere la información, o los medios por los cuales se distribuye o almacena, siempre debe ser protegida en forma adecuada. La seguridad de la información se define como la preservación de las siguientes características:

1.4.1 CONFIDENCIALIDAD DE LA INFORMACIÓN

La información que se intercambian entre individuos y empresas no siempre deberá ser conocida por todo el mundo. Mucha de la información generada por las personas se destina a un grupo específico de individuos, y muchas veces a una única persona. Eso significa que estos datos deberán ser conocidos solo por un grupo controlado de personas.

1.4.2 INTEGRIDAD DE LA INFORMACIÓN

Una información integra es una información que no ha sido alterada de forma indebida o no autorizada. Para que la información se pueda utilizar, deberá estar integrada. Cuando ocurre una alteración no autorizada de la información, quiere decir que la información ha perdido su integridad.

1.4.3 DISPONIBILIDAD

Para que una información se pueda utilizar, deberá estar disponible. Se refiere a la disponibilidad de la información y de toda la estructura física y tecnológica que permita el acceso, tránsito y almacenamiento. La disponibilidad de la información permite que:

- Se utilice cuando sea necesario.
- Que esté al alcance de sus usuarios y destinatarios.
- Se pueda accederla en el momento en que necesiten utilizarla.

1.5 ENTORNO ORGANIZACIONAL EMPRESA IMOBILIARIA

La amplia trayectoria convierte a la inmobiliaria en el mayor promotor de viviendas del Ecuador. Las capacidades organizacionales desarrolladas desde 1973, nos han permitido entregar decenas de miles de viviendas puntualmente, de un extenso catálogo de productos con la máxima flexibilidad en plazos de financiamiento, así como en la elección de ubicación y acabados. Somos los únicos con certificado de calidad ISO 9001:2008, lo que es garantía de cumplimiento, calidad y éxito.

En Ecuador ha desarrollado
- 995 hectáreas totalmente urbanizadas
- 29.000 unidades de vivienda
- 8 centros comerciales
- Parques, edificios de oficinas, hospitales, consultorios, centros educativos, deportivos y de esparcimiento, y toda clase de servicios que hacen que los proyectos sean verdaderas "Ciudades para Vivir".

Con la experiencia que les otorgan más de 35 años de desarrollo de los más ambiciosos y completos proyectos residenciales del Ecuador, que han creado para ti y tu familia, el lugar ideal para iniciar una vida llena de nuevas oportunidades, bienestar y seguridad. Ningún detalle ha sido descuidado para ofrecer una propuesta única que suma calidad y bajo costo. Los acabados y materiales son de primera. La entrega de tu casa será SIEMPRE puntual. Y el financiamiento invita a soñar despierto. Cuando conozcas la inmobiliaria realmente sentirás que encontraste un lugar listo para vivir y crecer.

A medida del crecimiento de la empresa los directivos tomaron la decisión de llevar un proceso automatizado y de total dependencia de la tecnología que mantendría en línea todos sus puntos estratégicos ubicados en diferentes lugares de Guayaquil.

1.6 SITUACIÓN ACTUAL

Actualmente la empresa cuenta con un Data Center que contienen:
Servidores de:

- Dominio, DNS
- Correo
- Base de Datos
- Internet
- Dispositivos Móviles (Black Berry)
- Servidor de Archivos
- Enlaces de Red con Puntos remotos
- Centrales Telefónicas

El data center (Centro de Cómputo) de la empresa está ubicado en Tornero es la conexión principal con los puntos remotos los mismos que se dividen en 4: Punto Remoto 01 que se encuentra en la vía Samborondón, el sitio alterno en Alborada y los Puntos Remotos 02,03 que se encuentran vía Daule, dichos puntos se encarga de dar el servicio para estos puntos que se considerado de ventas.

Estos son medios de dependencia directa del negocio ya que sus actividades son en línea, al momento no cuenta con un plan de continuidad de negocios aplicado al data center sin embargo a través de los años se han presentado problemas como apagones de energía por tiempos prolongados que han durado inclusive 8 horas, adicionalmente ha ocurrido la perdida de enlaces en puntos estratégicos de ventas en centros comerciales, oficinas, obra.

Estas fallas se producen tanto en la matriz como en las sucursales por la falta de entrenamiento de los empleados que los manejan. Desafortunadamente no se le ha dado una verdadera importancia a esta situación. Cada vez vemos sistemas más complejos en la medida en que más dispositivos se conecten a los sistemas y a las redes, entonces será imperativo para la empresa contar con ingenieros y personal entrenado que pueda seguir el ritmo de estos avances e incorporarlos en forma rápida y efectiva en sus negocios.

La mayoría de las organizaciones de todos los sectores en el país, con pocas excepciones; no han tomado consciencia de la imprescindible necesidad de tener en conocimientos los pasos que habría que realizar y las acciones que habría que tomar para que sí, por desgracia hubiera una interrupción en las funciones criticas del negocio, supiera cada miembro de la organización que tendría que hacer para acortar al máximo esa inactividad.

No hay duda ni siquiera para el más escéptico, que el comercio entre organizaciones y el de organizaciones con consumidores, será casi en su totalidad a través del uso de

Internet y demás tecnologías de comunicación en los próximos años. Hoy en día es muy

común que una empresa pueda realizar sus funciones o dar servicios a través de una red de comunicaciones.

Todos estos adelantos tecnológicos han desarrollado una necesidad imperiosa que las empresas tienen que saber solucionar al momento de una interrupción o fallo. Los riesgos a los que una organización está sometida son interminables. Los activos de información que se manejan en la empresa son de importantísimos valor para su desempeño estratégico.

No cabe duda que ya pensando fríamente lo que se debía hacer y quien debía haberlo hecho, en la secuencia correcta se va a conseguir el objetivo principal de asegurar la continuidad del negocio ante cualquier eventualidad.

1.7 OBJETIVOS

1.7.1 OBJETIVO GENERAL

Como objetivo general de este proyecto es minimizar el riesgo ocasionado por posibles amenazas internas y externas que afecten el uso de equipos tecnológicos ubicados en el Data Center e impidan la continuidad del negocio, desarrollar las destrezas para poder manejar un proyecto de implantación del SGSI en una organización en conformidad con el ISO 27001.

El propósito de establecer este Análisis de Seguridad Informática para la empresa inmobiliaria, estableciendo un nivel máximo de seguridad, es proteger la información y los activos de la organización, tratando de conseguir confidencialidad, integridad y disponibilidad de los datos y las responsabilidades que debe asumir cada uno de los empleados mientras permanezca en la organización.

Estas políticas emergen como el instrumento para concienciar a sus miembros acerca de la importancia y sensibilidad de la información y servicios críticos, de tal forma que permitan a la empresa cumplir con su misión.

1.7.2 OBJETIVO ESPECÍFICO

La base del funcionamiento del negocio de la empresa inmobiliaria radica en uso de tecnologías y su principal proceso a no interrumpir es la ventas y comunicaciones (Correo) de la inmobiliaria, nos fijaremos como meta trazada la de mantener en línea y funcionamiento los sistemas que permiten se realice estos proceso con el usos de un plan de continuidad de negocio.

Se han identificado los siguientes objetivos específicos que son:

- Corregir fallas en el funcionamiento de servidores.
- Re direccionamiento de enlaces a sitio alterno.
- Corregir fallas en el funcionamiento de equipo de comunicación.
- Levantar servicio en sito alterno para el funcionamiento de la inmobiliaria.
- Medir proceso de seguimiento a controles establecidos.

1.8 ESTRUCTURA ORGANIZACIONAL

1.8.1 ORGANIGRAMA GENERAL

1.8.2 DESCRIPCIÓN DEL ORGANIGRAMA GENERAL

Las gerencias operativas cuenta con los siguientes departamentos como:

- Directorio.
- Departamento de Recursos Humanos.
- Departamento de Tecnologías.
- Departamento de Proyecto
- Departamento Financiero

1.8.3 DEPARTAMENTO DE COMPRAS

Recibe las requisiciones de compras, es decir, atiende las peticiones en cuanto a carencia de material se refiere, en cada uno de los departamentos involucrados en el proceso productivo como: cemento, arena, granza, granito, herramientas de trabajo.

Analiza detalladamente las fuentes de abastecimiento, tomando en cuenta todos los proveedores activos y potenciales con los cuales la empresa mantiene relaciones comerciales.

Envía las solicitudes de cotización, describiendo detalladamente los materiales que se desean adquirir a los proveedores que han sido preseleccionados por la empresa.

Recibe y analiza las cotizaciones de los proveedores, es decir, realiza un estudio riguroso de cada proveedor por separado en un formato que contendrá los siguientes elementos: Cantidad, precio unitario, precio total, calidad, tiempo de entrega y condiciones de pago.

Selecciona el mejor proveedor que cumpla con mayor cantidad de especificaciones, resultante del análisis anteriormente efectuado.

1.8.4 DEPARTAMENTO DE PROVEEDURIA

Recibe del Departamento de Compras una copia de cada pedido efectuado. Entrega al encargado de control de existencias la documentación. Entrega al auxiliar del Almacén los materiales comprados para que los acomode en los respectivos estantes y patios de almacenamiento.

Registra las entradas y salidas en tarjetas de existencia. Indica al Supervisor del Almacén sobre la carencia de algunos materiales. Coloca los materiales en sus respectivos lugares de almacenamiento. Transporta y entrega el material requerido al departamento solicitante.

1.8.5 DEPARTAMENTO DE VENTAS

Supervisa el trabajo de cada vendedor. Solventa de la mejor manera cualquier problema que se presente con un cliente determinado. Planifica el trabajo de ventas. Coordina reuniones y visitas a los clientes. Estudia el mercado de trabajo. Realiza el pronóstico de ventas por mes. Lleva el acumulado diario de las ventas.

1.8.6 DEPARTAMENTO DE FINANZAS

Envía los cheques a los proveedores, una vez que los materiales solicitados sean entregados.

Se encarga del papeleo interno para dar entrada en el inventario a los nuevos materiales solicitados a los proveedores.

Comprueba los asientos y las sumas en las facturas y registra los detalles financieros de las operaciones.

Retiene el pago de los proveedores, cuando los materiales adquiridos están sujetos, antes de ser aceptados, a inspección y prueba.

Recibe información por parte del Departamento de Compras, en caso de que los materiales aceptados estén defectuosos y el departamento de compras haya negociado con el proveedor alguna rebaja.

1.8.7 DEPARTAMENTO DE RECEPCIÓN DE MATERIALES

Recibe y revisar el pedido, para constatar que cumpla cabalmente con las especificaciones estipuladas en la orden de compra.

Descarga los materiales adquiridos.

Transporta el material comprado hasta el departamento de almacén, para su respectivo almacenamiento.

Revisa las condiciones de los materiales adquiridos. En caso de que, parte de ellos, estén dañados, notifica de inmediato al Departamento de Compras para iniciar las rebajas con el proveedor.

Notifica al Departamento de Compras, en caso de que los materiales comprados estén en buenas condiciones para que pueda pagarse la factura.

1.8.8 PROYECTOS

Diseña proyectos urbanísticos requeridos por la empresa.

Indica cuales son los materiales que se requieren, desde el punto de vista de resistencia, dimensión, dureza, métodos de fabricación al Departamento de Compras.

Satisface las necesidades del cliente.

Investiga todos los aspectos técnicos en cuanto al producto se refiere.

Invoca tecnología para satisfacer nuevas necesidades del producto.

1.8.9 DEPARTAMENTO LEGAL

Revisa las cláusulas de los Contratos, puesto que todas las órdenes de compras son contratos legales. Este procedimiento es realizado por un abogado.

Proporciona asesoría legal al agente de compras, cuando este realice sus actividades contractuales (determinación de precios, mermas en el recibo, manejo de las ofertas, entre otros).

Proporciona asesoría legal, cuando algunas compras que va a efectuar la Empresa requieran de un contrato especial.

1.8.10 DEPARTAMENTO DE ADMINISTRACIÓN DE MATERIALES

Proporciona y mantiene un flujo de materiales que permita la continuidad operativa de la empresa.

Desarrolla proveedores competentes.
Mejora la posición competitiva de la empresa.
Alcanza las mejoras relacionadas con los otros Departamentos de la Empresa.
Racionaliza los costos de la administración.
Estandariza la calidad de los productos requeridos.

CAPÍTULO 2
MARCO TEÓRICO

2 MARCO TEÓRICO

En la actualidad en el país se está adoptando con mayor fuerza el uso de tecnologías para el acceso a diferentes fuentes de información y comunicación, todas las áreas ya sean estas educacionales, empresariales, agrícolas, entre otros, están ligados a un cierto grado de dependencia tecnológica. En muchos de los casos estas dependencias no pueden ser interrumpidas ya que ocasionaría una paralización en sus actividades que puede ser muy significativa a nivel económico o hasta pérdida total de información.

En varias empresas se aplican ciertos procesos de contingencia ante cualquier eventualidad que pueda afectar sus medios de almacenamiento o comunicación. En otros casos se improvisa una solución inmediata.

Con lo anteriormente mencionado se realizará el proyecto utilizando las metodologías de la norma ISO 27001 y buenas prácticas de ITIL.

Las normas ISO2700 nos indican que para la adecuada gestión de seguridad de la información es necesario implementar un sistema que aborde esta tarea de una forma metódica y clara basada en objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización.

La práctica de ITIL establece los conceptos básicos. Las tareas clave a realizar y la documentación resultante. Contiene un catálogo que se trata de una lista de elementos estándar de manera que se cuente con una nomenclatura común a todos los proyectos de análisis y gestión de riesgos donde se aplique ITIL. Así, se enumeran: tipos de activos, dimensiones de valoración de los activos, criterios de valoración de los activos, amenazas típicas sobre los sistemas de información y salvaguardas a considerar a la hora de proteger los sistemas de información.

2.1 ¿QUÉ ES ITIL?

ITIL son las siglas de una metodología desarrollada a finales de los años 80's por iniciativa del gobierno del Reino Unido, específicamente por la OGC u Oficina Gubernativa de Comercio Británica (Office of Goverment Comerce). Las siglas de ITIL significan (Information Technology Infrastructure Library) o Librería de Infraestructura de Tecnologías de Información.
Esta metodología es la aproximación más globalmente aceptada para la gestión de servicios de Tecnologías de Información en todo el mundo, ya que es una recopilación de las mejores prácticas tanto del sector público como del sector privado. Estas mejores prácticas de dan en base a toda la experiencia adquirida con el tiempo en determinada actividad, y son soportadas bajo esquemas organizacionales complejos, pero a su vez bien definidos, y que se apoyan en herramientas de evaluación e implementación.

ITIL como metodología propone el establecimiento de estándares que nos ayuden en el control, operación y administración de los recursos (ya sean propios o de los clientes).

Plantea hacer una revisión y reestructuración de los procesos existentes en caso de que estos lo necesiten (si el nivel de eficiencia es bajo o que haya una forma más eficiente de hacer las cosas), lo que nos lleva a una mejora continua.

Otra de las cosas que propone es que para cada actividad que se realice se debe de hacer la documentación pertinente, ya que esta puede ser de gran utilidad para otros miembros del área, además de que quedan asentados todos los movimientos realizados, permitiendo que toda la gente esté al tanto de los cambios y no se tome a nadie por sorpresa.

En la documentación se pone la fecha en la que se hace el cambio, una breve descripción de los cambios que se hicieron, quien fue la persona que hizo el cambio, así como quien es el que autorizo el cambio, para que así se lleve todo un seguimiento de lo que pasa en el entorno. Esto es más que nada como método con el que se puede establecer cierto control en el sistema de cambios, y así siempre va a haber un responsable y se van a decir los procedimientos y cambios efectuados.

2.2 CONCEPTO DE SOLUCIONES PARA ITIL DESDE EL PUNTO DE VISTA DE NEGOCIO

Según este diagrama vemos como aparentemente tenemos segmentos del negocio aislados, pero en realidad todos tienen algo que ver para la obtención de las soluciones.

Por ejemplo la prestación de servicios muchas veces no sería posible sin la gestión de infraestructura, asimismo las perspectivas del negocio no se darían sin la prestación de servicio y los servicios no serían posibles sin un soporte al servicio.

Y el punto de interacción que se da entre estos segmentos del negocio es la búsqueda de soluciones, donde lo que se busca es que las perspectivas del negocio estén soportadas en base a la prestación de servicios; la prestación de servicios requiere que se le dé un soporte al servicio para que este siempre disponible, la disponibilidad la podemos lograr mediante una gestión de la infraestructura y en lugar de tener al centro las soluciones vamos a tener a los clientes satisfechos.

Figura 2-1: Soluciones ITIL

El proceso de Administración de continuidad de servicios de TI investiga, desarrolla e implementa las opciones de recuperación cuando una interrupción a un servicio alcanza un punto definido.

La elección de la opción a utilizar es por parte del cliente, y forma parte de los acuerdos de niveles de servicio.

La siguiente figura muestra donde se encuentra el proceso de Administración de Continuidad de Servicios de TI y la relación con otros procesos.

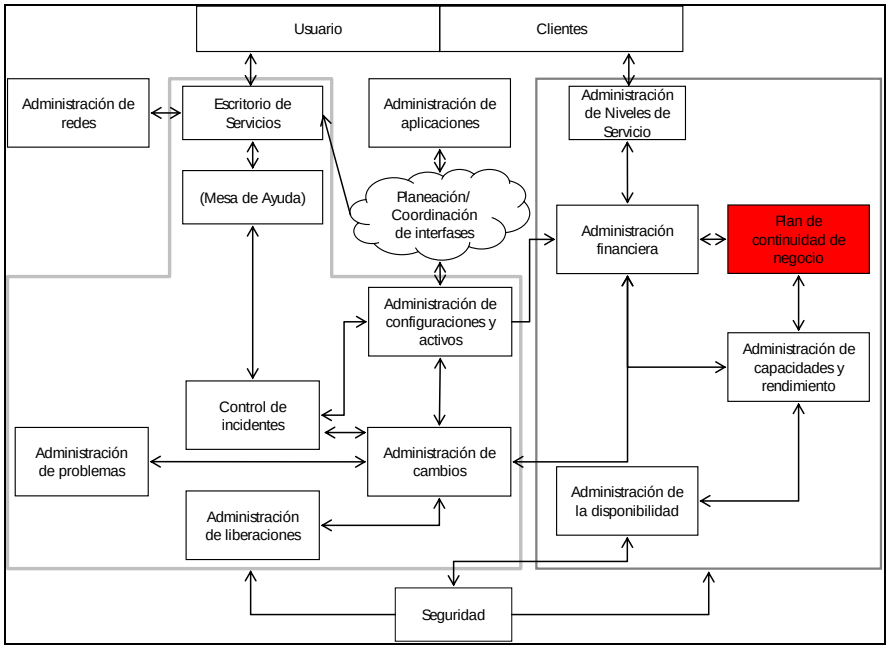


Figura 2-2: Proceso ITIL

El **objetivo** de la Administración de Continuidad de Servicios de TI es planear, cubrir y recuperarse de una crisis de TI que requiera que el trabajo se mueva a un sistema alterno de una manera transparente.

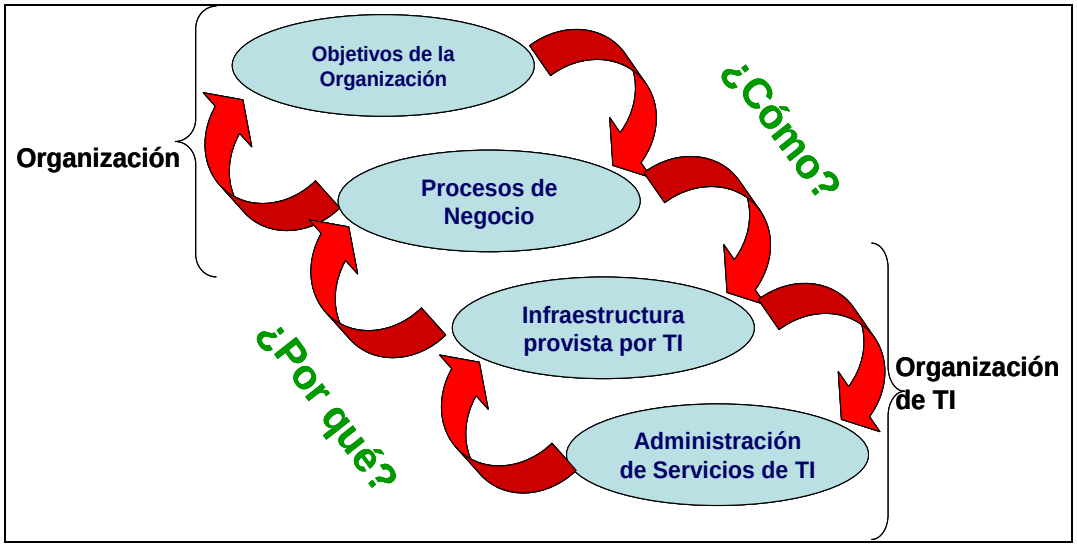


Figura 2-3: Organización y Objetivo ITIL

Hoy en día los ambientes de negocio son altamente competitivos, las organizaciones son juzgadas en su habilidad para continuar operando y proporcionando servicios. La administración de continuidad se preocupa por la habilidad de una organización para continuar proporcionando un predeterminado y acordado nivel de servicios de TI, para soportar los requerimientos mínimos del negocio.

La forma en cómo nos va a estar **beneficiando** la Administración de Continuidad de Servicios de TI es de la siguiente forma:

- Mejor administración de riesgos.
- Credibilidad organizacional.
- Ventaja competitiva.
- Recuperación de los sistemas de TI de una manera controlada.
- Interrupción mínima del negocio.

2.2.1 ALINEACIÓN CON EL NEGOCIO

A través de la implementación de IT Service Management en la organización de TI, se estará soportando los objetivos de TI de la entrega de los servicios que son requeridos por el negocio. Esta implementación no puede hacerse sin alinear la estrategia de TI con la estrategia del negocio. Además no se pueden entregar servicios de TI efectivos sin conocer acerca de las demandas, necesidades y deseos del cliente. ITSM soporta la organización de TI para alinear las actividades de TI y la entrega de los servicios con los requerimientos del negocio.

Una vez que los procesos de administración de servicios de TI están alineados con los objetivos de negocio, ITIL recomienda que se cuente con un programa de mejora continua o CSIP (Continuous Service Improvement Programme). Para esta mejora, deben de considerarse 3 aspectos:

- Procesos
- Infraestructura.
- Gente

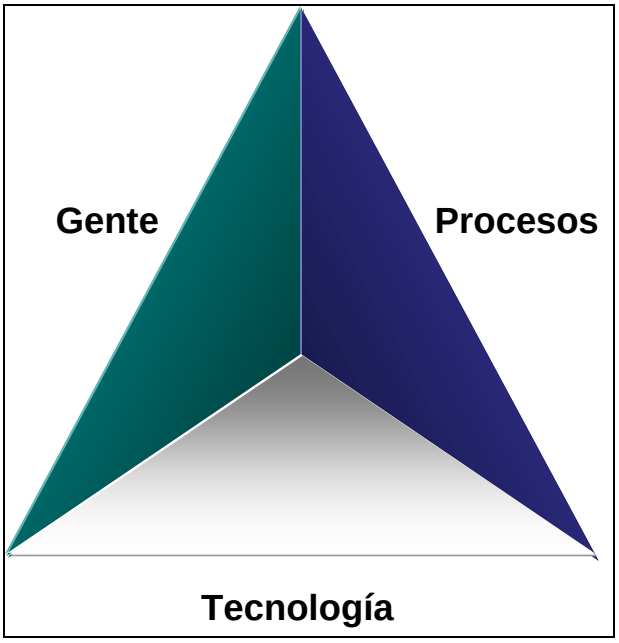


Figura 2-4: Relación con el Negocio

2.3 RELACIÓN DEL PROCESO DE ADMINISTRACIÓN DE CONTINUIDAD DE SERVICIOS DE TI CON OTROS PROCESOS

Como cada uno de los procesos de Administración de entrega y soporte de servicios, Administración de Continuidad de Servicios de TI tiene relación con otros procesos. La siguiente figura muestra esta relación.

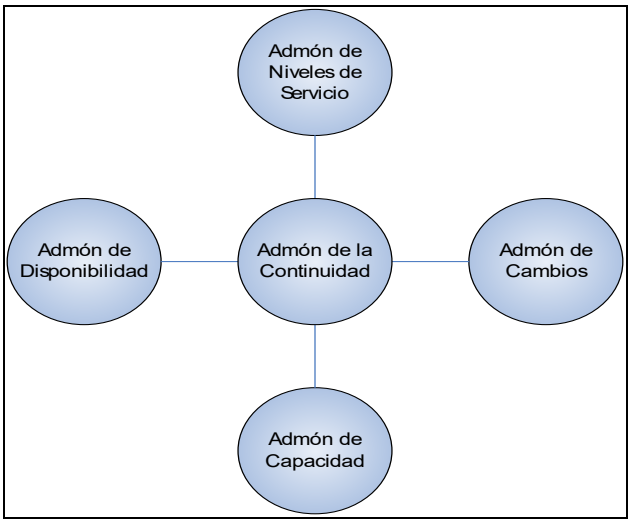


Figura 2-5: Continuidad de Servicios

La administración de continuidad interactúa con otras disciplinas de servicios de TI:

Administración del Nivel de Servicio. Entendiendo las obligaciones de la entrega de servicios de TI.

Administración de Disponibilidad. Medidas de reducción de riesgos para mantener el negocio en operación.

Administración de Configuración. Definiendo el núcleo de la infraestructura de TI.

Administración de Capacidad.-Cuidar que los requerimientos del negocio sean totalmente cubiertos gracias a los recursos apropiados de TI.

Administración de Cambios. Cuidar la exactitud del plan de contingencia estableciendo procesos y revisándolos regularmente.

Administración de Incidentes. Revisión de incidentes históricos relacionados con la continuidad.

ITIL postula que el servicio de soporte, la administración y la operación se realiza a través de cinco procesos:

1. Manejo de Incidentes
2. Manejo de problemas
3. Manejo de configuraciones
4. Manejo de cambios y
5. Manejo de entregas

2.4 PROCESO DE MANEJO DE INCIDENTES

Su objetivo primordial es restablecer el servicio lo más rápido posible para evitar que el cliente se vea afectado, esto se hace con la finalidad de que se minimicen los efectos de la operación. Se dice que el proveedor de debe de encargar de que el cliente no debe percibir todas aquellas pequeñas o grandes fallas que llegue a presentar el sistema. A este concepto se le llama disponibilidad (que el usuario pueda tener acceso al servicio y que nunca se vea interrumpido).
Para este proceso se tiene un diagrama que en cada una de sus fases maneja cuatro pasos básicos que son: propiedad, monitoreo, manejo de secuencias y comunicación.

En el proceso de manejo de incidentes vemos que se da como primera etapa la detección del incidente (es cuando el sistema presenta alguna anomalía o falla, y que esto se puede traducir en un error en el sistema o que el usuario no puede hacer algo y recurre a pedir ayuda); ya que lo tenemos identificado se hace una clasificación del incidente (vemos si el error que se presenta es conocido o si nunca se ha presentado) y de la mano va el soporte inicial (es el punto en el que el cliente llega a la mesa de servicio a solicitar ayuda, porque no sabe o no puede hacer algo); en caso de que el incidente sea conocido se hace el procedimiento de solicitud de servicio (se ejecutan los pasos a seguir según el manual de procedimientos para poder llegar a la solución de una forma viable y eficiente).

2.5 PROCESO DE MANEJO DE PROBLEMAS

El Objetivo de este proceso es prevenir y reducir al máximo los incidentes, y esto nos lleva a una reducción en el nivel de incidencia. Por otro lado nos ayuda a proporcionar soluciones rápidas y efectivas para asegurar el uso estructurado de recursos.
En este proceso lo que se busca es que se pueda tener pleno control del problema, esto se logra dándole un seguimiento y un monitoreo al problema.
El diagrama de este proceso es muy particular, ya que se maneja en dos fases: la primera está relacionada con lo que es el control del problema y la segunda es con el control del error.
En lo que respecta a la fase de control del problema: primero se tiene que identificar el problema en base a alguna sintomatología; ya que tenemos este antecedente, pasamos a la clasificación de los problemas (en este proceso al igual que en el proceso de manejo de incidentes tenemos que ver si es un problema conocido), en caso de ser conocido, se recurre al procedimiento de solicitud de servicio, donde se van a aplicar las soluciones de acuerdo a como están en el manual de procedimientos; y en caso de no ser conocido se tendría que hacer una fase de investigación para ver qué es lo que genera el problema y más tarde hacer un diagnóstico; ya que tenemos un diagnóstico tenemos que hacer un RFC (Request For Change o Solicitud de Cambio)
Esta solicitud de cambio implica que se va a tener que implementar la solución y finalmente se va a hacer una evaluación para ver si se resolvió el problema de raíz. En caso de que si se funcione esta solución se pasa a la documentación.

2.6 PROCESO DE MANEJO DE CONFIGURACIONES

Su objetivo es proveer con información real y actualizada de lo que se tiene configurado e instalado en cada sistema del cliente.

Este proceso es de los más complejos, ya que se mueve bajo cuatro vértices que son: administración de cambios, administración de liberaciones, administración de configuraciones y la administración de procesos diversos.
El nivel de complejidad de este modelo es alto, ya que influyen muchas variables y muchas de ellas son dinámicas, entonces al cambiar una o varias de ellas se afecta el sistema en general, lo que hace que sea muy difícil de manipular. Aunque es lo más parecido a la realidad, porque nuestro entorno es dinámico y las decisiones de unos afectan a otros.
Por ejemplo en lo que respecta a la administración de cambios vemos que se relaciona directamente con la administración de incidentes y de problemas, lo que conlleva una planeación, identificación, control, seguimiento del status, verificación y auditoria de configuraciones, lo que hace que haya muchas variables.

2.7 PROCESO DE CONTROL DE CAMBIOS

El objetivo de este proceso es reducir los riesgos tanto técnicos, económicos y de tiempo al momento de la realización de los cambios.
Este diagrama la parecer es muy fácil de seguir, pero en realidad no lo es, ya que entre etapa y etapa se da una fase de monitoreo para ver que no se han sufrido desviaciones de los objetivos.
Primero vemos que tenemos un registro y clasificación del cambio que se tiene que hacer, se pasa a la fase de monitoreo y planeación, si el rendimiento es satisfactorio se da la aprobación del cambio, y en caso de que el rendimiento sea malo se pasa a la fase de reingeniería hasta que el proceso funcione adecuadamente.

2.8 PROCESO DE MANEJO DE ENTREGAS

Su objetivo es planear y controlar exitosamente la instalación de Software y Hardware bajo tres ambientes: ambiente de desarrollo, ambiente de pruebas controladas y ambiente real.
Este proceso tiene un diagrama que marca la transición que se da de acuerdo a los ambientes por los que se va dando la evolución del proyecto.
En lo que respecta al ambiente de desarrollo vemos que se tiene que hacer la liberación de las políticas, la liberación de la planeación, el diseño lógico de la infraestructura que se va a implementar y la adquisición de software y hardware están entre los ambientes de desarrollo y de pruebas controladas; ya que se requiere que ambos hagan pruebas sobre ellos; en el ambiente de pruebas controladas vemos que se hace la construcción y liberación de las configuraciones (nivel lógico), se hacen las pruebas para establecer los acuerdos de aceptación; se da la aceptación total de versiones y de modelos, se arranca la planeación y finalmente las pruebas y comunicaciones; y en lo que es el ambiente real vemos que se da la distribución e instalación.
En la etapa del ambiente real es la que se ve de forma más concreta, ya que muchas veces no tenemos idea de todo lo que pasa hasta antes de la instalación.

2.9 CONCEPTOS BÁSICOS DE ITIL

ITIL, por sus siglas en inglés (Information Technology Infrastructure Librar) es una colección de documentos públicos, que basados en procesos y un marco de mejores prácticas de la industria, permite la Administración de Servicios de una organización de TI con calidad y a un costo justo.

ITIL tiene que ver con todos aquellos procesos que se requieren ejecutar dentro de las organizaciones para la administración y operación de la infraestructura de TI, de tal forma que se tengo una óptima provisión de servicios a los clientes bajo un esquema de costos congruentes con las estrategias del negocio.

ITIL cuenta con varias publicaciones, las cuales se muestran en la siguiente figura; estas permiten tener una liga entre la tecnología y el negocio.

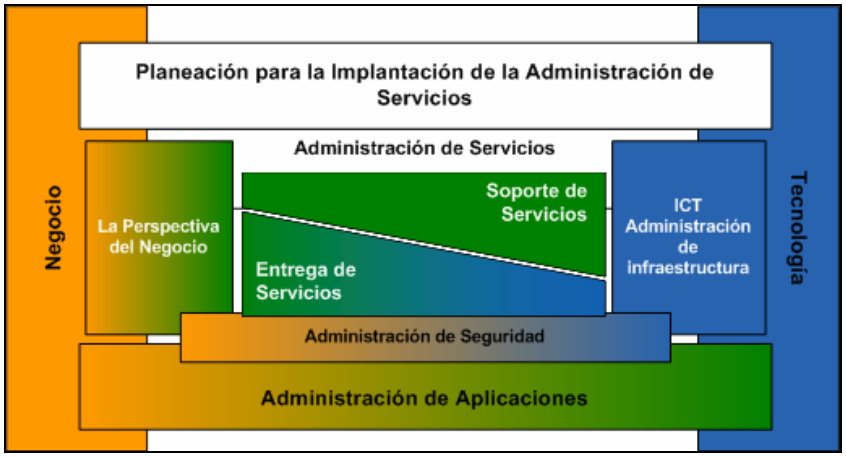


Figura 2-6: Tecnologías y Negocios

Cada una de estas publicaciones provee una guía de las mejores prácticas y el detalle de información de los procesos.

A continuación se dará una breve descripción de cada uno de una de las publicaciones que no se cubren:

2.10 PLANEACIÓN PARA LA IMPLEMENTACIÓN DE LA ADMINISTRACIÓN DE SERVICIO:

Temas y tareas involucradas en planeación, implementación y mejora de los procesos de Administración de Servicios dentro de una organización.

2.11 ICT ADMINISTRACIÓN DE INFRAESTRUCTURA

Abarca el tema de Tecnología de Información y Administración de la Infraestructura (ICTIM) y las relaciones con otras áreas, como la Administración de Servicio

2.12 PERSPECTIVA DEL NEGOCIO

Tiene como objetivo familiarizarse con la administración del negocio con los componentes de Administración de Servicios, Administración de Aplicaciones y la Administración de la Infraestructura, los cuales son necesarios para soportar los procesos de negocio.

2.13 ADMINISTRACIÓN DE APLICACIONES

Trata el tema de la administración de las aplicaciones desde las necesidades del negocio hasta el ciclo de vida de la aplicación.

2.14 ADMINISTRACIÓN DE SEGURIDAD

Detalla el proceso de planeación y administración de un definido nivel de seguridad en la información y servicios.

2.15 ENTREGA DE SERVICIOS

Cubre los procesos necesarios para la planeación y entrega de la calidad de los servicios de TI. Estos procesos son:

- Administración de Niveles de Servicio
- Administración Financiera
- Administración de Capacidad
- Administración de la Continuidad de Servicios de TI
- Administración de la Disponibilidad

2.16 CONCLUSIONES:

ITIL es una metodología que nos va a ayudar a que las cosas se puedan hacer de una forma más eficiente, ya que lo que se propone es que se adopten ciertas métricas y procedimientos que otros proveedores de IT adoptaron y que gracias a ellas son catalogadas como mejores prácticas.

El hecho de adoptar mejores prácticas implica que no tengamos que descubrir el hilo negro y que si alguien sabe cómo hacer las cosas y explotar los recursos nos podemos apoyar en el para que nosotros también podamos hacerlo. E mayor objetivo es que todos lleguemos a un nivel de eficiencia que se traduzca en una buena prestación de servicios.

2.17 ¿QUÉ SON NORMAS ISO 27001?

Es un estándar ISO que proporciona un modelo para establecer, implementar, utilizar, monitorizar, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Se basa en el ciclo de vida PDCA (Planear-Hacer-Verificar-Actuar; o ciclo de Deming) de mejora continua, al igual que otras normas de sistemas de gestión (ISO 9001 para calidad.

Este estándar es certificable, es decir, cualquier organización que tenga implantado un SGSI según este modelo, puede solicitar una auditoria externa por parte de una entidad acreditada y, tras superar con éxito la misma, recibir la certificación en ISO 27001.

El origen de la Norma ISO27001 está en el estándar británico BSI (British Standar Institution) BS7799, estándar que fue publicado en 1998 y era certificable desde entonces. Tras la adaptación pertinente, ISO 27001 fue publicada el 15 de Octubre de 2005.

Relación de la Norma ISO27001 con otros estándares de seguridad de la Información existen otros estándares internacionalmente aceptados relacionados con seguridad de la información como: COBIT, NIST, MAGERIT, entre otros, que la enfocan desde diferentes puntos de vista como controles de seguridad, buen gobierno, gestión de riesgo.

Sistema de Gestión de la Seguridad de la Información –SGSI Un SGSI es un Sistema de Gestión de la Seguridad de la Información o ISMS por sus siglas en inglés (Information Security Management System). Este sistema consiste de una serie de actividades de gestión que deben realizarse mediante procesos sistemáticos, documentados y conocidos por una organización o entidad.

2.18 ENFOQUE BASADO EN EL PROCESO PHVA

La seguridad de sistemas de seguridad de información, adopta un enfoque basado en procesos, para establecer, implementar, operar, hacer seguimiento, mantener y mejorar el Modelo de Seguridad de la Información y estar orientado a todos los actores y entidades involucradas:

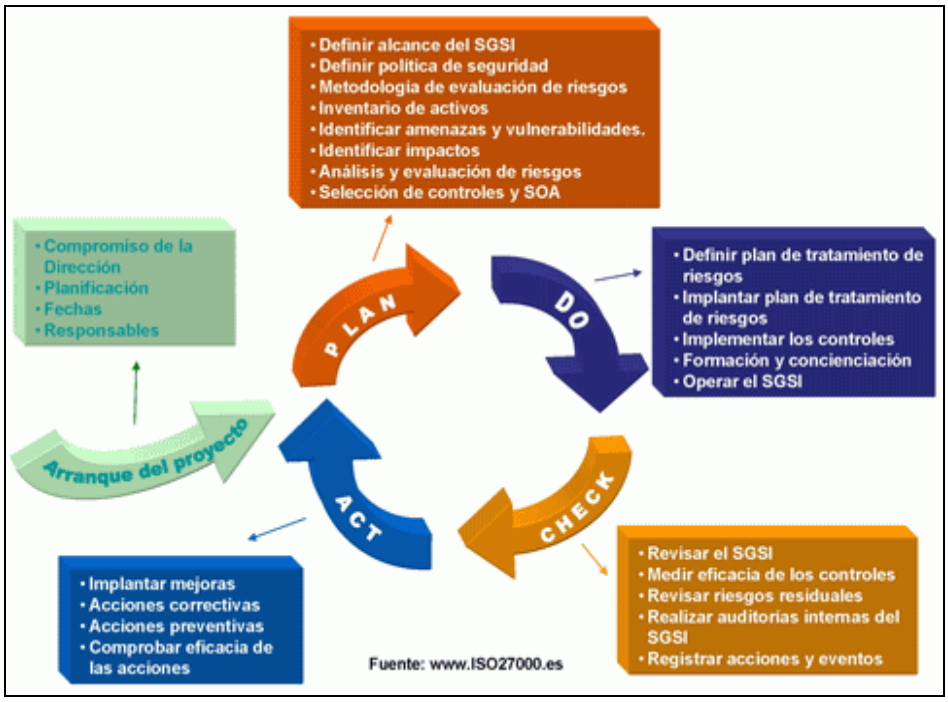


Figura 2-7: Ciclo PHVA

2.19 BENEFICIOS DE LA IMPLANTACIÓN DE UN SGSI

Aplica una arquitectura de gestión de la seguridad que identifica y evalúa los riesgos que afectan al negocio, con el objetivo de implantar contramedidas, procesos y procedimientos para su apropiado control, tratamiento y mejora continua.
Ayuda a las empresas a gestionar de una forma eficaz la seguridad de la información, evitando las inversiones innecesarias, ineficientes o mal dirigidas que se producen por contrarrestar amenazas sin una evaluación previa, por desestimar riesgos, por la falta de contramedidas, por implantar controles desproporcionados y de un costo más elevado del necesario, por el retraso en las medidas de seguridad en relación a la dinámica de cambio interno de la propia organización y del entorno, por la falta de claridad en la asignación de funciones y responsabilidades sobre los activos de información, por la ausencia de procedimientos que garanticen la respuesta puntual y adecuada ante incidencias o la propia continuidad del negocio.

2.20 ¿QUÉ SON NORMAS ISO 27002?

El documento del Estándar Internacional ISO/IEC 27002, después de la introducción, se divide en quince capítulos.

Figura 2-8: Términos y definiciones

De acuerdo al grafico observado se habla de un conjunto de términos y definiciones que se presentan al final de este documento, en el Glosario, que son las definiciones de:

- Activo
- Control
- Lineamiento
- Medios de procesamiento de la información
- Seguridad de la información
- Evento de seguridad de la información
- Incidente de seguridad de la información
- Política
- Riesgo
- Análisis de riesgo
- Evaluación del riesgo
- Gestión del riesgo
- Tratamiento del riesgo
- Tercera persona
- Amenaza
- Vulnerabilidad

Este Estándar contiene un número de categorías de seguridad principales, entre las cuales se tienen once cláusulas:

- a) Política de seguridad.
- b) Aspectos organizativos de la seguridad de la información.

- c) Gestión de activos.
- d) Seguridad ligada a los recursos humanos.
- e) Seguridad física y ambiental.
- f) Gestión de comunicaciones y operaciones.
- g) Control de acceso.
- h) Adquisición, desarrollo y mantenimiento de los sistemas de información.
- i) Gestión de incidentes en la seguridad de la información.
- j) Gestión de la continuidad del negocio.
- k) Cumplimiento.

2.21 GESTION DE LA CONTINUIDAD DE NEGOCIOS

La Gestión de Continuidad de Negocios es un proceso de gestión holístico que identifica potenciales impactos que amenazan la organización y provee una estructura para la aumentar la resistencia y la capacidad de respuesta de manera efectiva que salvaguardan los intereses de los stakeholders (interesados), su reputación, marca y valor creando actividades.
"A menudo me preguntan qué consejo puedo ofrecer que sería útil a la comunidad empresarial. Mi respuesta es simple pero efectiva, planes de continuidad de negocios frecuentemente revisados y probados".

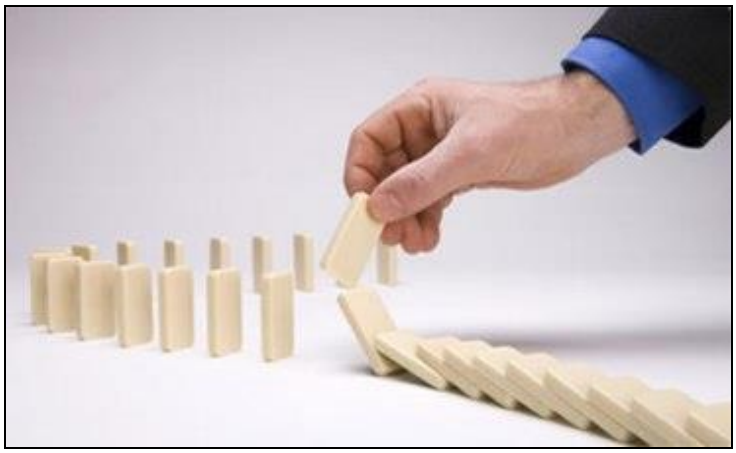


Figura 2-9: Continuidad de Negocios

Normalmente, durante la interrupción, imprevista de la actividad de una organización, se generan pérdidas financieras, sin embargo, el impacto más significativo es normalmente la pérdida de imagen corporativa o la pérdida de confianza que resulta de un incidente gestionado.
La gestión de la continuidad de negocio es un proceso holístico de gestión, que identifica los impactos de incidentes potenciales que amenaza una organización y proporciona u marco para desarrollar una respuesta eficaz y una capacidad de recuperación de la organización, que proteja los intereses de sus grupos de intereses, su imagen, el valor de su marca y sus actividades.
La GCN (Gestión de la continuidad de negocios) se desarrolla en la organización tanto verticalmente (niveles estratégico, táctico y operativo), como horizontalmente (en todas sus sedes y su cadena de valor, incluye la propia cadena de suministros).

2.22 PLAN DE CONTINUIDAD

2.23 INTRODUCCIÓN

Cuando se habla de la continuidad de negocio hay que establecer los requerimientos de continuidad; es esencial que una organización esté preparada para reactivar sus servicios en un mínimo de tiempo y así disminuir el impacto que causaría al negocio, para esto existen tres recursos principales para lograrlos:

2.24 IMPORTACIA DE LA CONTINUIDAD DE NEGOCIO

Figura 2-10: Descargas Eléctricas e Incendios

Una caída de la luz, una inundación, un incendio o un robo han de considerarse amenazas reales que deben ser tratadas de forma preventiva para evitar, en caso de que éstas sucedan, que las pérdidas sean tan graves que afecten a la viabilidad del negocio. Son múltiples las organizaciones que, independiente mente de su tamaño, fracasan o incluso desaparecen por la falta de procesos, mecanismos y técnicas que mitiguen los riesgos a los que están expuestas y garanticen una alta disponibilidad en las operaciones de su negocio.

De este modo, es necesario que las organizaciones establezcan una serie de medidas

Técnicas, organizativas y procedimentales que garanticen la continuidad de las actividades o procesos de negocio en caso de tener que afrontar una contingencia grave.

El primer recurso consiste en evaluar los riesgos que enfrenta la organización. Mediante el análisis de riesgos se identifican las amenazas a los activos, se evalúan las vulnerabilidades y probabilidad de ocurrencia, y se estima el impacto potencial.

El segundo recurso está constituido por los requisitos legales, normativos, reglamentarios y contractuales que deben cumplir la organización, sus socios comerciales, los contratistas y los prestadores de servicios.

El tercer recurso es el conjunto específico de principios, objetivos y requisitos para el procesamiento de la información, que ha desarrollado la organización para respaldar sus operaciones.

Los requerimientos de continuidad del negocio se identifican mediante una evaluación metódica de los riesgos de continuidad. Las erogaciones derivadas de la satisfacción de las necesidades de control deben ser equilibradas con respecto al impacto potencial de las fallas de continuidad en los negocios. Las técnicas de evaluación de riesgos pueden aplicarse a toda la organización, o sólo a partes de la misma, así como a los sistemas de información individuales, componentes de sistemas o servicios específicos cuando esto resulte factible, viable y provechoso.

2.25 DEFINICIÓN DE ANÁLISIS DE RIESGO

El análisis de riesgos es realizado para detectar los riesgos a los cuales están sometidos los activos de una organización, es decir, para saber cuál es la probabilidad de que las amenazas se concreten.
Las amenazas se pueden convertir en realidad a través de fallas de continuidad, que conocemos como vulnerabilidades y que deben ser eliminadas al máximo para que el ambiente que se desea proteger esté libre de riesgos de incidentes de continuidad.

Por lo tanto, la relación entre amenaza-incidente-impacto, es la condición principal a tomar en cuenta en el momento de priorizar acciones de continuidad para la corrección de los activos que se desean proteger.

2.25.1 OBJETIVOS DEL ANÁLISIS DE RIESGO

El análisis de riesgo tiene como objetivo: Estudiar los riesgos que soporto una determinada área relativa a las tecnologías de información y el entorno asociable con esta. Estimando la probabilidad de ocurrencia y el nivel de impacto que puede ocasionar

si el riesgo se llega a materializar. Recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos investigados.

2.25.2 CLASIFICACIÓN DE RIESGOS DE NEGOCIOS RELACIONADOS CON LA INFORMÁTICA

Los principales riesgos informáticos de los negocios son los siguientes:
Riesgos de utilidad: Estos riesgos se enfocan en tres diferentes niveles de riesgo:

- Los riesgos pueden ser enfrentados por el direccionamiento de sistemas antes de que los problemas ocurran.

- Técnicas de recuperación/restauración usadas para minimizar la ruptura de los sistemas.

- Backups y planes de contingencia controlan desastres en el procesamiento de la información.

Riesgos en la infraestructura: Estos riesgos se refieren a que en las organizaciones no tienen una estructura de información tecnológica práctica (hardware, software, redes, personas y procesos) para soportar adecuadamente las necesidades futuras y presentes de los negocios.

- Planeación organizacional: Los proceso en esta área aseguran la definición del impacto, definición y verificación de la tecnología informática en el negocio. Además, verifica si existe una adecuada organización (gente y procesos) asegura que los esfuerzos de la tecnología informática será exitosa.

- Administración de continuidad: Los procesos en esta área aseguran que la organización está adecuadamente direccionada a establecer, mantener y monitorizar un sistema interno de continuidad, que tenga políticas de administración con respecto a la integridad y confidencialidad de la información de la organización, y a la reducción de perdida de enlaces a niveles aceptables.

- Operaciones de red y computacionales: Los procesos en esta área aseguran que los sistemas de información y entornos de red están operados en un esquema seguro y protegido, y que las responsabilidades de procesamiento de información son ejecutados por personal operativo definido, medido y monitoreado.

- Información / Negocio: Los proceso en esta área están diseñados para asegurar que existe un plan adecuado para asegurar que la tecnología informática estará disponible a los usuarios cuando ellos la necesitan.

2.25.3 RIESGOS DE SEGURIDAD GENERAL

- Riesgos de choque de eléctrico:
- Niveles altos de voltaje.
- Riesgos de incendio: Inflamabilidad de materiales.
- Riesgos de niveles inadecuados de energía eléctrica.
- Riesgos de radiaciones: Ondas de ruido, de láser y ultrasónicas.
- Riesgos mecánicos: Inestabilidad de las piezas eléctricas.

2.25.4 ESTRUCTURA DEL ANÁLISIS DE RIESGO.

Para poder llevar a cabo un análisis de riegos se tiene que cubrir los siguientes puntos:

Objetivos del Análisis de riesgo.- El establecimiento de los objetivos del análisis es el primer paso que se debe realizar, por lo general los objetivos más comunes son:

- Identificar los riesgos aplicables para la organización.

- Identificar los riegos de mayor severidad, los que causen un mayor impacto sobre los activos de la organización.
- Establecimiento de controles que permitan mitigar los riesgos más severos.

Identificación de los riesgos.- Antes de enfrentar los riesgos, estos deben ser identificados. Esta tarea es permanente, pues nuevas amenazas están surgiendo constantemente. La identificación de riesgos es continua y depende de la red de comunicación dentro de la organización, generando un flujo constante de información acerca de las actividades de la organización.

Evaluación de los riesgos.- Es la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto sobre los activos de la organización. El resultado de la evaluación es la determinación de los riesgos más severos que se presentan en la organización.

Controles.- Una vez evaluados los riesgos e identificados cuales son los de mayor severidad se deben establecer ciertos controles que ayuden a solucionar o mitigar los riesgos.

2.26 ESTRATEGIA DE CONTINUIDAD

2.26.1 HOT SITE

Hot site es una página web compacta, construida a partir de modelos estandarizados. Son considerados publicidad, pues divulgan la empresa y sus productos. Tratase de una difusión inofensiva que, cuando hecha correctamente, son incontrolables máquinas de ventas, sin necesitar de un vendedor.
Hot site posee retorno instantáneo a bajos costos, con tasas significativas de respuesta. Posibilita a su empresa marcar presencia en la gran red, con costos accesibles y design profesional.
Entre las innúmeras ventajas podemos destacar:

Agilidad: su empresa o negocio entra en la Internet, en un plazo máximo de una semana.
Costo/beneficio: la mejor solución para exponer sus productos o servicios, con baja inversión, dentro de un portal con expresivo número de visitantes diarios.
Modernidad: su producto dentro de la vanguardia tecnológica.
Velocidad: un canal de comunicación instantáneo con sus clientes.

2.26.2 WARM SITES

Una manera común de ver las principales estrategias para la recuperación de desastres se basa en las definiciones de los principales fuera de sitio y recuperación de centro de que estas estrategias de uso. Las siguientes definiciones han existido por décadas, y varían dependiendo de quién usted habla, pero todavía proporcionan una buena manera de grupo de la recuperación primaria de diferentes estrategias de continuidad. Tenga en cuenta que las líneas entre las diferentes estrategias no están claramente definidos ya menudo se superponen.

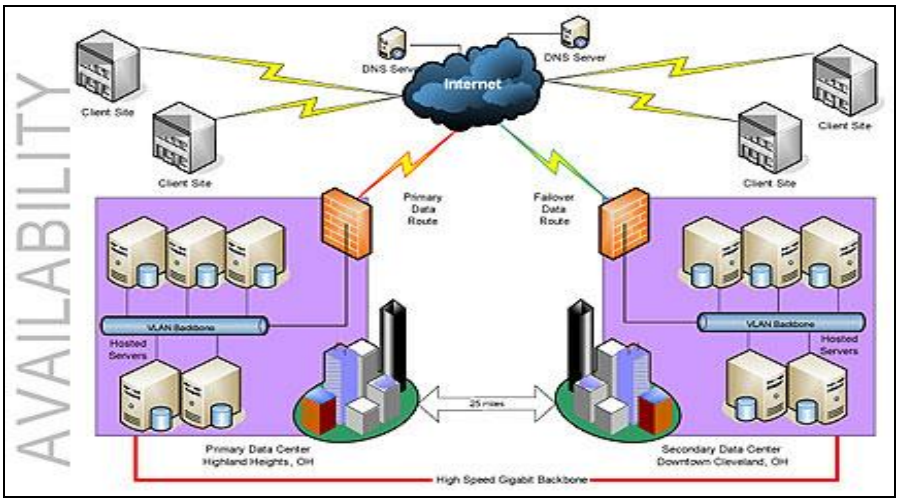


Figura 2-11: Warm Sites

2.26.3 EQUIPOS DE RESPALDO

Es un equipo o dispositivo capaz de suministrar potencia o energía frente a alguna interrupción del suministro normal de la misma, se usa para alimentar a un equipo electrónico o eléctrico, que si se detiene o se altera su funcionamiento por un problema en la alimentación eléctrica, resulta costoso, tanto en dinero como en tiempo, por pérdida de información o en daños en sus componentes.

Se compone de:

- Una batería cuya capacidad depende del tiempo durante el cual debe entregar energía cuando se corta la entrada del equipo UPS.
- Dispositivos de comunicación de red como: router, switch.
- Equipos de almacenamiento como servidores.

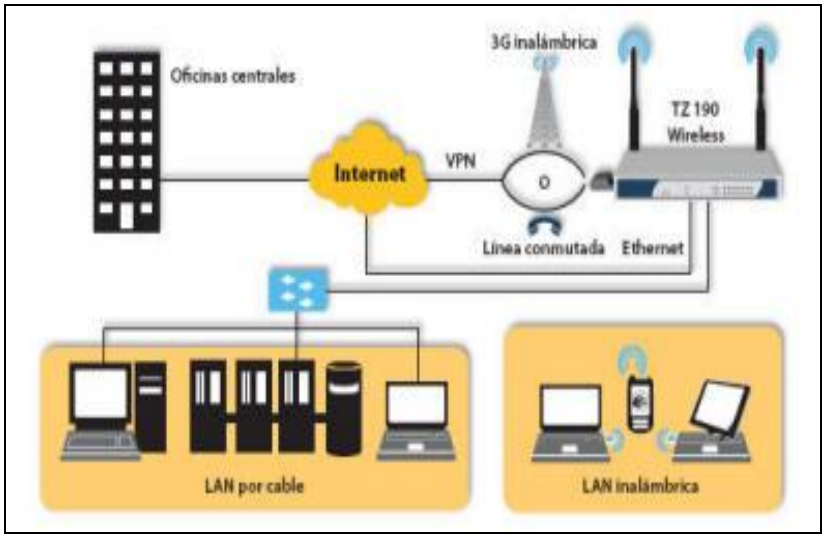


Figura 2-12: Equipos de Respaldos

2.27 ANÁLISIS DE IMPACTO

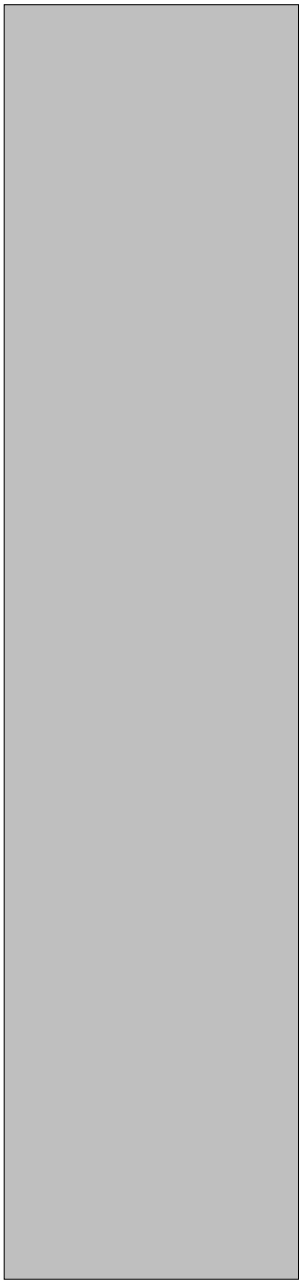
2.27.1 INTRODUCCIÓN

El Análisis de Impacto en el Negocio es un componente fundamental del plan de continuidad de una empresa. Incluye un componente exploratorio para encontrar algunas debilidades y un componente de planeación para desarrollar estrategias que permitan reducir el riesgo. El resultado del análisis es un reporte de análisis de impacto en el negocio, reporte que describe los riesgos potenciales para la empresa estudiada.

Una de los supuestos básicos sobre los cuales se fundamenta el análisis de impacto es que cada componente de la organización depende de la continuidad de los otros componentes, pero algunos son más críticos que otros y requieren mayor asignación de recursos en el momento de un desastre.

2.27.2 ¿PARA QUÉ SIRVE?

La seguridad de sistemas de seguridad de información, adopta un enfoque basado en procesos, para establecer, implementar, operar, hacer seguimiento, mantener y mejorar el Modelo de Seguridad de la Información y estar orientado a todos los actores y entidades involucradas:



CAPÍTULO 3
MARCO METODOLÓGICO

3 MARCO METODOLÓGICO

3.1 ACTIVIDADES DEL PROCESO DE ADMINISTRACIÓN DE CONTINUIDAD DE SERVICIOS DE ITIL

El proceso de Administración de Continuidad de Servicios de TI cuenta con 4 etapas que se ejecutan durante las actividades del proceso. Estas etapas se ilustran en la siguiente figura:

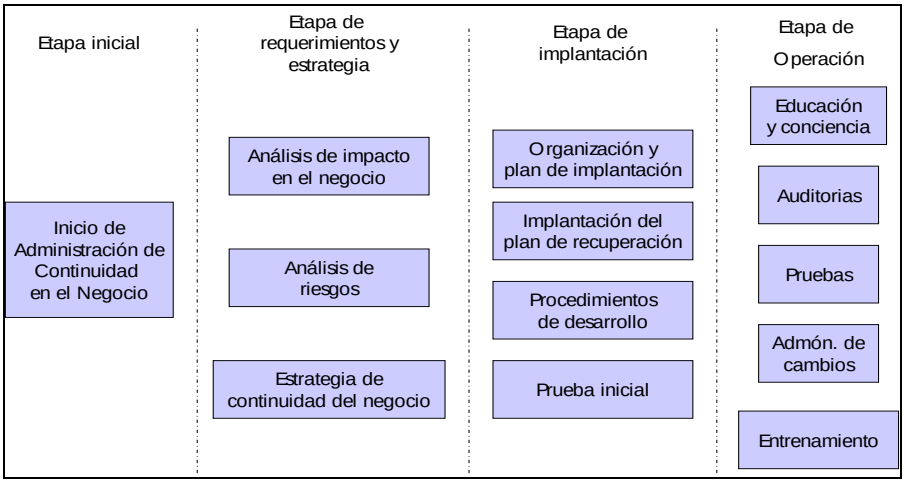


Figura 3-1: Actividades del proceso ITIL

3.1.1 ETAPA INICIAL

Las actividades consideradas en la primera etapa dependen de la extensión a las instalaciones de contingencia que se han aplicado en la organización. La única manera de implantar una administración de continuidad efectiva, es por medio de la identificación de los procesos críticos del negocio y del análisis y coordinación de la infraestructura y servicios de TI que los soportan.
La organización del proceso cubre todo el proceso y consiste de las siguientes actividades:

- Definición de políticas.
- Definición de términos de referencia y alcance.
- Recursos asignados.
- Definición de la organización del proyecto y estructura de control.
- Acuerdo del proyecto y plan de calidad.

3.1.2 ETAPA DE REQUERIMIENTOS Y ESTRATEGIA

Esta etapa proporciona la base de la administración de continuidad y es un componente crítico para determinar cuan bien sobrevivirá una organización a interrupciones del negocio o desastres y el costo en que se incurrirá. Si el análisis de requerimientos es incorrecto o se olvida información clave, podría tener graves consecuencias en la efectividad del mecanismo de la administración de continuidad.

- Análisis de impacto en el negocio.

- Procesos críticos del negocio.
- Daños potenciales o pérdidas.
- Grado de daño o pérdida y como se escalará.
- Habilidades del personal e instalaciones necesarios para activar las funciones críticas.
- Pérdidas financieras y costos adicionales.
- Evaluación de riesgo.
- Identificación de riesgos.
- Evaluación de niveles de vulnerabilidad y riesgo.
- Estrategia de continuidad del negocio.
- Medidas de reducción de riesgos.
- Eliminación de puntos de falla.
- Mayores controles de seguridad física y lógica.
- Opciones de recuperación.

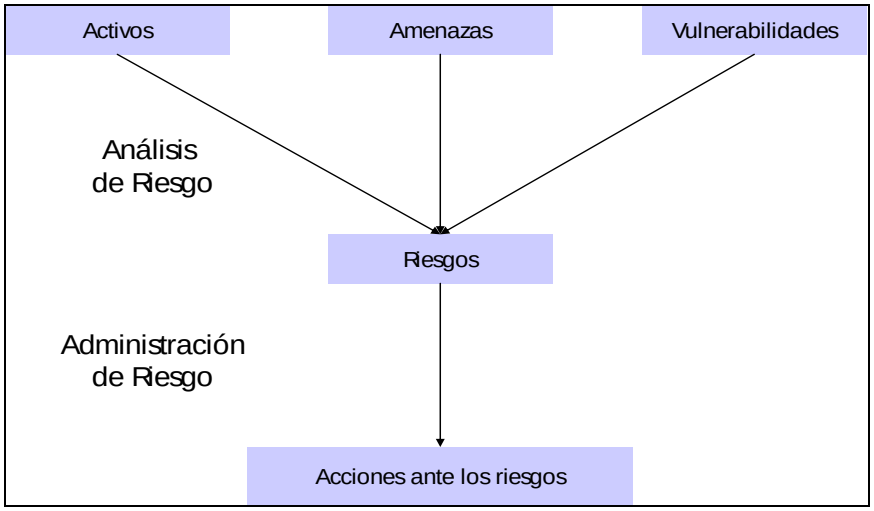


Figura 3-2: Etapas y Estrategias

3.1.3 ETAPA DE IMPLANTACIÓN

Esta etapa consiste de los siguientes procesos:

- Establecer la organización y desarrollar el plan de implantación.
- Implantar acuerdos de espera.
- Implantar medidas de reducción de riesgos.
- Desarrollar planes de recuperación de TI.
- Desarrollo de procedimientos.
- Realización de pruebas iniciales.

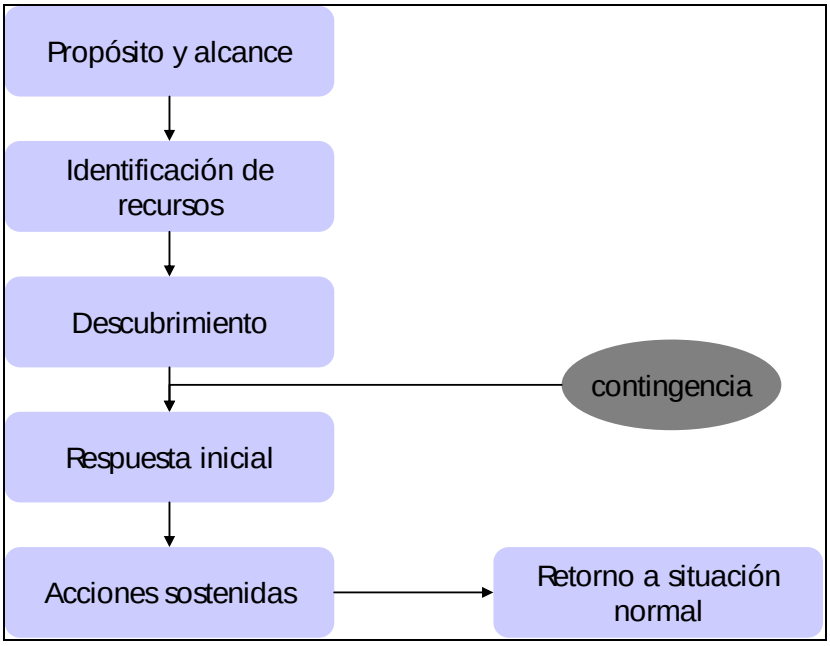


Figura 3-3: Procesos de implantación

3.1.4 ETAPA DE OPERACIÓN

Una vez culminada la implantación es necesario asegurar que el proceso sea mantenido como parte de lo usual del negocio. Esto se alcanza gracias a la administración operacional incluyendo:

- Educación y conocimiento.
- Entrenamiento.
- Revisión.
- Prueba.
- Control de cambios.
- Aseguramiento de calidad.

3.2 ANÁLISIS DE RIESGO PARA LA INMOBILIARIA

3.2.1 INTRODUCCIÓN

De acuerdo a la declaración de la aplicabilidad de la inmobiliaria, establecida en base a la delimitación del alcance definido en las entrevistas con las Principales Autoridades de la inmobiliaria: Ing. José Orlando López, Jefe de Servicios Tecnológicos; Ing. Juan

Carlos Alzate, Vicepresidente de Tecnología; Ing. Edwin Delgado, Administrador de redes, sobre los dominios de la norma ISO 27001 sobre los cuales se trabajara son: Gestión de la Continuidad del Negocio, por ende el análisis de riesgo se concentrara en el mismo, identificando los riegos aplicables dentro del dominio, realizando una evaluación de riesgo para determinar cuáles son las amenazas sobre las cuales hay que establecer controles.

3.2.2 OBJETIVOS DEL ANÁLISIS DE RIESGOS

Es objetivo que pretende alcanzar este análisis es conocer cuáles son los riegos de mayor severidad dentro del dominio de estudio para la continuidad del negocio de la inmobiliaria.

3.2.3 IDENTIFICACIÓN DE RIESGOS.

En este punto se desarrolló un inventario de riesgos producto de una investigación acerca de los mismos en Internet, el entorno de la inmobiliaria, entrevista con el personal de la empresa inmobiliaria y visitas realizadas en el data center.

El inventario consta de 4 riesgos, de los cuales mediante la clasificación y encasillamiento de los mismos dentro del dominio establecido en la declaración de aplicabilidad, se determinó que 4 son aplicables a la inmobiliaria.

DOMINIO	CANTIDAD
Gestión de continuidad del Negocio	4

Tabla 3-1: Resumen de identificación de Riesgos

3.2.4 EVALUACIÓN DE RIESGOS

En la evaluación de riesgos se manejan tres aspectos fundamentales como son: La probabilidad de ocurrencia, el nivel de impacto y la severidad. Para cada uno de estos se detalla a continuación el esquema con el que se trabajó.

3.2.5 PROBABILIDAD DE OCURRENCIA

No existe un estándar definido para la escala del nivel de ocurrencia. Para la clasificación de los riesgos más probables se utilizó la siguiente estructura:

Calificación	Nivel de Ocurrencia
Alta	3
Media	2
Baja	1

Tabla 3-2: Calificación de riesgo de acuerdo al nivel de ocurrencia

De acuerdo a la clasificación anterior se considera a los riesgos más probables a los que obtengan un nivel de ocurrencia de 3, y a los menos probables los que obtengan un nivel de ocurrencia 2 ó 1.

3.2.6 NIVEL DE IMPACTO

No existe un estándar definido para la escala del nivel de impacto. Para la clasificación de los riesgos de mayor nivel de impacto se utilizó la siguiente estructura:

Calificación	Nivel de Impacto
Alta	3
Media	2
Baja	1

Tabla 3-3: Calificación de riesgo de acuerdo a su nivel de impacto

De acuerdo a la clasificación anterior se considera a los riesgos que causan un mayor nivel de impacto sobre los activos a los que obtengan un nivel de 3, el nivel de impacto 2 se considera como un impacto medio sobre el activo, y los que obtengan un nivel de impacto de 1 son considerados de menor impacto.

3.2.7 SEVERIDAD

Para la obtención de la severidad de los riesgos se utilizó la siguiente igualdad:

Severidad = Nivel de Ocurrencia x Nivel de Impacto

De acuerdo a la igualdad anterior y a los niveles de ocurrencia e impacto, se pueden presentar 9 posibles combinaciones siendo la de menor valor de severidad 1 y la de mayor valor de severidad 9. Para la clasificación de la severidad para los riesgos se aplicó el siguiente criterio, la división de acuerdo a tres niveles de severidad: Riesgos de severidad baja.- Acumula el 33% de los valores de severidad. Es decir los que obtenga un valor de severidad comprendido entre 1 y 3.

Riesgos de severidad media.- Entre el 33% y 66% de los valores de severidad. Es decir los que obtenga un valor de severidad entre 3 y 6. Riesgos de severidad alta.- Mayor al 66% de los valores de severidad. Es decir los que obtenga un valor de severidad mayor a 6.

Nivel de Severidad	Etiqueta	Mínimo	Máximo
Severidad Baja	B	1	3
Severidad Media	M	3	6
Severidad Alta	A	6	9

Tabla 3-4: Clasificación de riesgos de acuerdo a al nivel de severidad

De acuerdo con la clasificaron anterior se establecerán controles para los riesgos de mayor severidad o severidad alta.

3.2.8 EJECUCIÓN DE LA EVALUACIÓN DE RIESGO

A continuación en la Tabla 4.5, se detalla la estimación de los niveles de ocurrencia e impacto de los riesgos aplicables al data center realizados en un taller de manera conjunta entre Luis Cepeda, Byron Zamora, Jhonny Plúas y el Ing. Edwin Delgado Administrador de redes de la inmobiliaria.

Las celdas resaltadas indican aquellos riesgos con calificaciones mayores que fueron considerados como los de mayor severidad para la ejecución del presente trabajo y se resumen en la Tabla 3.5

3.2.9 CRITICIDAD DE PROCESOS

No existe un estándar definido para la escala de criticidad de procesos. Para la clasificación de los procesos de mayor nivel de criticidad se utilizó la siguiente estructura:

Calificación	Nivel de Criticidad
POCO CRÍTICO	1
MEDIO CRÍTICO	2
CRÍTICO	3
MUY CRÍTICO	4
INDISPENSABLE	5

Tabla 3-5: Calificación de procesos de acuerdo a su nivel de criticidad

De acuerdo a la clasificación anterior se considera a los procesos que causan un mayor nivel de criticidad sobre los procesos a los que obtengan un nivel de 5, el nivel de criticidad 4 se considera como nivel de criticidad media sobre el proceso, y los que obtengan un nivel de criticidad menor igual a 3 se considera como nivel de criticidad menor sobre el proceso.

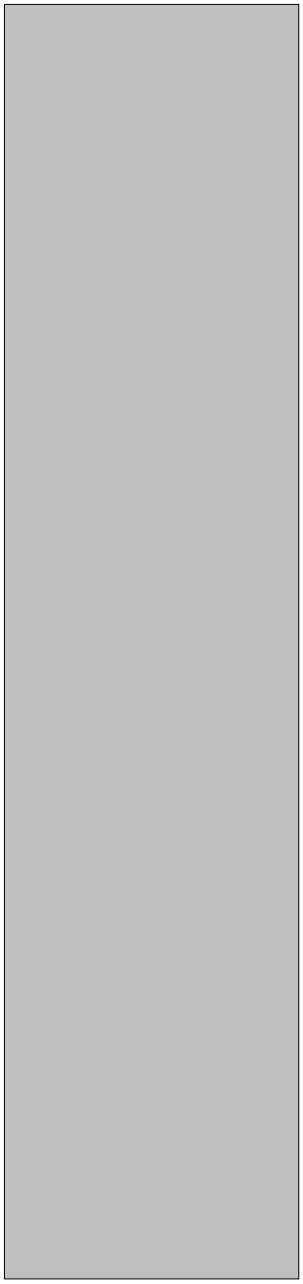
3.3 CONTROLES DE APLICABILIDAD

Aspectos de la seguridad de la información de la gestión de la continuidad comercial.					
ISO 27001: 2005 CONTROLES		**Objetivo:** contrarrestar las interrupciones de las actividades comerciales y proteger los procesos comerciales críticos de los efectos de fallas o desastres importantes o desastres en los sistemas de información y asegurar su reanudación oportuna.			
		Controles actuales	**Considerar**	**Control**	**Lo Aplicado**
GESTIÓN DE LA CONTINUIDAD DE NEGOCIOS	**14.1.1**	**SI**	Incluir seguridad de la información en el proceso de gestión de continuidad comercial	Se debe desarrollar y mantener un proceso gerencial para la continuidad del negocio a través de toda la organización para tratar los requerimientos de seguridad de la información necesarios para la continuidad comercial de la organización.	Se determinó mediante un análisis de la situación actual de la empresa la necesidad de un plan de continuidad de negocio.
	14.1.2	**SI**	Continuidad Comercial y evaluación del riesgo	Se deben identificar los eventos que causan interrupciones en los procesos comerciales, junto con la probabilidad e impacto de dichas interrupciones y si consecuencias para la seguridad de la información.	Acogiéndonos a lo indicado por el control de la norma ISO27001, se realizó un cuadro indicativo en donde se determinó las amenazas, vulnerabilidades, probabilidad e impacto sobre los procesos comerciales de la empresa inmobiliaria.

Tabla 3-6: Controles de Aplicabilidad

Aspectos de la seguridad de la información de la gestión de la continuidad comercial.					
ISO 27001: 2005 CONTROLES		**Objetivo:** contrarrestar las interrupciones de las actividades comerciales y proteger los procesos comerciales críticos de los efectos de fallas o desastres importantes o desastres en los sistemas de información y asegurar su reanudación oportuna.			
		Controles actuales	**Considerar**	**Control**	**Lo Aplicado**
GESTIÓN DE LA CONTINUIDAD DE NEGOCIOS	**14.1.3**	**SI**	Desarrollar e implementar planes de continuidad incluyendo seguridad de la información	Se deben desarrollar e implementar planes para mantener o restaurar las operaciones y asegurar la disponibilidad de la información en el nivel requerido y en las escalas de tiempo requeridas después de la interrupción o falla en los procesos comerciales críticos.	Se detalló un plan de continuidad comercial adecuado para la empresa inmobiliaria que le permita operaciones comerciales luego de haber sufrido una interrupción.
	14.1.4	**SI**	Marco referencial para la planeación de la continuidad comercial	Se debe mantener un solo marco referencial de planes de continuidad comercial para asegurar que todos los planes sean constante y para tratar consistentemente los requerimientos de la seguridad de la información e identificar los prioridades de pruebas y mantenimiento	Se definió un marco referencial en donde se indica el enfoque del proyecto y la metodología mediante la cual serán evaluados los procesos críticos de la empresa inmobiliaria; así como también la aplicación de planes de continuidad y pruebas contra ciertas amenazas.
	14.1.5	**SI**	Prueba Mantenimiento y re-evaluación de planes de continuidad comercial	Los planes de continuidad comercial se deben probar y actualizar regularmente para asegurar que estén actualizados y sean efectivos	El alcance del proyecto elaborado no contempla la puesta en marcha y ejecución de los planes sugeridos, sin embargo hay conclusiones y recomendaciones son válidas para que dado el momento puedan ser aplicadas por la empresa.

Tabla 3-7: Controles de Aplicabilidad



CAPÍTULO 4
EJECUCIÓN

4 EJECUCIÓN

4.1.1 ETAPA INICIAL

Iniciamos identificando los activos del Data Center (Centro de Cómputo) y su ubicación de la inmobiliaria para lo cual se llevó a cabo una reunión con el encargado del Data Center Ing. Edwin Delgado, Luis Cepeda y Jhonny Plúas del cual se obtuvo el siguiente inventario de activo:

ACTIVOS	
EQUIPO	**UBICACIÓN**
SERVIDOR CDC_DBASE	Edificio principal
SERVIDOR SAMBDATA	
SERVIDOR ABMAIL	
SERVIDOR APLICATION_SERVER	
SERVIDOR ANTIVIRUS	
SERVIDOR CITRIX	
SERVIDOR BALACKBERRY	
SERVIDOR ABMAIL	
SWHITCH	
ROUTER	
MODEM	
CENTRAL TELEFONICA	

Tabla 4-1: Identificación y ubicación de activos

Con los activos identificados se realizó la identificación de los procesos críticos y el hardware donde se ejecutan, en consenso con el Ing. Edwin Delgado, Jhonny Plúas, Byron Zamora identificado la criticidad de los mismos para la inmobiliaria, y a continuación se muestra la tabla de procesos y su criticidad:

PROCESO	NIVEL CRÍTICO	APLICACIÓN	HARDWARE
VENTAS	5	SIGI	CDC_DBASE, ALMAIL
PROYECTOS	3	SIGI	CDC_DBASE, ALMAIL
FINANCIERO	4	SIGI,GP	CDC_DBASE, SAMBDATA, ALMAIL
CONTABLE	3	GP	SAMBDATA, ALMAIL
NOMINA	2	EVOLUTION	SAMBDATA, ALMAIL
CREDITO Y COBRANZA	4	SIGI	CDC_DBASE, ALMAIL
COMUNICACIÓN EMPRESARIAL	5	EXCHANGE	ABMAIL

Tabla 4-2: Procesos críticos de los activos

4.2 ETAPA DE REQUERIMIENTOS Y ESTRATEGIA

A continuación, se detalla la estimación de los niveles de ocurrencia e impacto de los riesgos aplicables al data center (Centro de Computo) realizados en un taller de manera conjunta entre Luis Cepeda, Byron Zamora, Jhonny Plúas y el Ing. Edwin Delgado Administrador de redes de la inmobiliaria, adicionalmente se detalla la estrategia aplicada ante los riesgos encontrados.

Las celdas resaltadas indican aquellos riesgos con calificaciones mayores que fueron considerados como los de mayor severidad para la ejecución del presente trabajo para lo cual se creó un ***Plan de Continuidad de Negocio*** que se lo adjunta en el **ANEXO 2**.

ACTIVO	PROCESO	VULNERABILIDAD	AMENAZA	RIESGO	IMPACTO	POSIBILIDAD DE OCURRENCIA	SERVIDAD	DAÑOS AL NEGOCIO	RTO (Recovery times objetives)	ESTRATEGIA CONTINUIDAD
SERVIDOR CDC_DBASE	Ventas,Financiero,Contable,Proyectos,Credito y Cobranza	Fallas en climatización del data center	Daño irreparable del servidor	Paralización de servicio	3	1	3	$20,000	2HRS	Hot Sites
		Varias personas tienen clave de administrador para acceso al servidor	Personas con intenciones negativas pueden sabotear el servidor	Paralización de servicio	3	2	6			
		Falta de mantenimiento físico al servidor	Apagados frecuentes del servidor	Paralización de servicio	3	2	6			
		Falta de espacio en disco duro	Crecimiento del log	Paralización de servicio	3	3	9			
		Fallos de equipos de enlace	Perdida de enlace	Paralización de servicio	3	2	6			
		Acceso no controlado al data center	Personas mal intencionadas pueden sabotear el data center	Paralización de servicio	3	2	6			
		No existe un proceso de actualización de software para los servidores	Alguna de las actualizaciones puede causar daños críticos en los servicios del servidor	Paralización de servicio	3	2	6			

Tabla 4-3: Requerimientos y Estrategias del Servidor CDC_DBASE

ACTIVO	PROCESO	VULNERABILIDAD	AMENAZA	RIESGO	IMPACTO	POSIBILIDAD DE OCURRENCIA	SERVIDAD	DAÑOS AL NEGOCIO	RTO (Recovery times objetives)	ESTRATEGIA CONTINUIDAD
SERVIDOR SAMBDATA	GP	Fallas en climatización del data center	Daño irreparable del servidor	Paralización de servicio	2	1	2	$10,000	8HRS	Warm Sites
		Varias personas tienen clave de administrador para acceso al servidor	Personas con intenciones negativas pueden sabotear el servidor	Paralización de servicio	2	2	4			
		Falta de mantenimiento físico al servidor	Apagados frecuentes del servidor	Paralización de servicio	2	2	4			
		Acceso no controlado al data center	Personas mal intencionadas pueden sabotear el data center	Paralización de servicio	2	3	6			
		No existe un proceso de actualización de software para los servidores	Alguna de las actualizaciones puede causar daños críticos en los servicios del servidor	Paralización de servicio	2	3	6			

Tabla 4-4: Requerimientos y Estrategias del Servidor SAMBDATA

ACTIVO	PROCESO	VULNERABILIDAD	AMENAZA	RIESGO	IMPACTO	POSIBILIDAD DE OCURRENCIA	SERVIDAD	DAÑOS AL NEGOCIO	RTO (Recovery times objetives)	ESTRATEGIA CONTINUIDAD
SERVIDOR ABMAIL	Correo	Fallas en climatización del data center	Daño irreparable del servidor	Paralización de servicio	3	1	3	$8,000	2HRS	Hot Sites
		Varias personas tienen clave de administrador para acceso al servidor	Personas con intenciones negativas pueden sabotear el servidor	Paralización de servicio	3	2	6			
		Falta de mantenimiento físico al servidor	Apagados frecuentes del servidor	Paralización de servicio	3	2	6			
		Falta de espacio en disco duro	Crecimiento del log	Paralización de servicio	3	3	9			
		No existe un proceso de actualización de software para los servidores	Alguna de las actualizaciones puede causar daños críticos en los servicios del servidor	Paralización de servicio	3	2	6			

Tabla 4-5: Requerimientos y Estrategias del Servidor ABMAIL

ACTIVO	PROCESO	VULNERABILIDAD	AMENAZA	RIESGO	IMPACTO	POSIBILIDAD DE OCURRENCIA	SERVIDAD	DAÑOS AL NEGOCIO	RTO (Recovery times objetives)	ESTRATEGIA CONTINUIDAD
SERVIDOR APLICATION_SERVER	MEDUSA.NET	Fallas en climatización del data center	Daño irreparable del servidor	Paralización de servicio	2	1	2	$1,500	16 HRS	Warm Sites
		Varias personas tienen clave de administrador para acceso al servidor	Personas con intenciones negativas pueden sabotear el servidor	Paralización de servicio	2	2	4			
		Falta de mantenimiento físico al servidor	Apagados frecuentes del servidor	Paralización de servicio	2	2	4			
		Falta de espacio en disco duro	Crecimiento del log	Paralización de servicio	2	3	6			
		No existe un proceso de actualización de software para los servidores	Alguna de las actualizaciones puede causar daños críticos en los servicios del servidor	Paralización de servicio	2	2	4			

Tabla 4-6: Requerimientos y Estrategias del Servidor de Aplicaciones

ACTIVO	PROCESO	VULNERABILIDAD	AMENAZA	RIESGO	IMPACTO	POSIBILIDAD DE OCURRENCIA	SERVIDAD	DAÑOS AL NEGOCIO	RTO (Recovery times objetives)	ESTRATEGIA CONTINUIDAD
SERVIDOR CITRIX	VENTAS	Fallas en climatización del data center	Daño irreparable del servidor	Paralización de servicio	2	1	2	$5,000	4 HRS	Warm Sites
		Varias personas tienen clave de administrador para acceso al servidor	Personas con intenciones negativas pueden sabotear el servidor	Paralización de servicio	2	2	4			
		Falta de mantenimiento físico al servidor	Apagados frecuentes del servidor	Paralización de servicio	2	2	4			
		No existe un proceso de actualización de software para los servidores	Alguna de las actualizaciones puede causar daños críticos en los servicios del servidor	Paralización de servicio	1	2	2			

Tabla 4-7: Requerimientos y Estrategias del Servidor Citrix - Ventas

ACTIVO	PROCESO	VULNERABILIDAD	AMENAZA	RIESGO	IMPACTO	POSIBILIDAD DE OCURRENCIA	SERVIDAD	DAÑOS AL NEGOCIO	RTO (Recovery times objetives)	ESTRATEGIA CONTINUIDAD
SERVIDOR ANTIVIRUS	ANTIVIRUS	Fallas en climatización del data center	Daño irreparable del servidor	Paralización de servicio	1	1	1	$3,000	16hrs	Warm Sites
		Varias personas tienen clave de administrador para acceso al servidor	Personas con intenciones negativas pueden sabotear el servidor	Paralización de servicio	1	2	2			
		Falta de mantenimiento físico al servidor	Apagados frecuentes del servidor	Paralización de servicio	1	2	2			
		No existe un proceso de actualización de software para los servidores	Alguna de las actualizaciones puede causar daños críticos en los servicios del servidor	Paralización de servicio	1	2	2			

Tabla 4-8: Requerimientos y Estrategias del Servidor de Antivirus

ACTIVO	PROCESO	VULNERABILIDAD	AMENAZA	RIESGO	IMPACTO	POSIBILIDAD DE OCURRENCIA	SERVIDAD	DAÑOS AL NEGOCIO	RTO (Recovery times objetives)	ESTRATEGIA CONTINUIDAD
SERVIDOR BLACKBERRY	CORREO MOVIL	Fallas en climatización del data center	Daño irreparable del servidor	Paralización de servicio	1	1	1	$5,000	8HRS	Warm Sites
		Varias personas tienen clave de administrador para acceso al servidor	Personas con intenciones negativas pueden sabotear el servidor	Paralización de servicio	1	2	2			
		Falta de mantenimiento físico al servidor	Apagados frecuentes del servidor	Paralización de servicio	1	2	2			
		No existe un proceso de actualización de software para los servidores	Alguna de las actualizaciones puede causar daños críticos en los servicios del servidor	Paralización de servicio	3	2	6			

Tabla 4-9: Requerimientos y Estrategias del Servidor Blackberry – Correo Móvil

ACTIVO	PROCESO	VULNERABILIDAD	AMENAZA	RIESGO	IMPACTO	POSIBILIDAD DE OCURRENCIA	SERVIDAD	DAÑOS AL NEGOCIO	RTO (Recovery times objetives)	ESTRATEGIA CONTINUIDAD
SERVIDOR ALBMAIL	FILE	Fallas en climatización del data center	Daño irreparable del servidor	Paralización de servicio	1	1	1	$2,500	4HRS	Warm Sites
		Varias personas tienen clave de administrador para acceso al servidor	Personas con intenciones negativas pueden sabotear el servidor	Paralización de servicio	1	2	2			
		Falta de mantenimiento físico al servidor	Apagados frecuentes del servidor	Paralización de servicio	1	2	2			
		Falta de espacio en disco duro	Apagados frecuentes del servidor	Paralización de servicio	2	2	4			
		No existe un proceso de actualización de software para los servidores	Alguna de las actualizaciones puede causar daños críticos en los servicios del servidor	Paralización de servicio	3	2	6			

Tabla 4-10: Requerimientos y Estrategias del Servidor ABMAIL - File

ACTIVO	PROCESO	VULNERABILIDAD	AMENAZA	RIESGO	IMPACTO	POSIBILIDAD DE OCURRENCIA	SERVIDAD	DAÑOS AL NEGOCIO	RTO (Recovery times objetives)	ESTRATEGIA CONTINUIDAD
SWITCH	RED	Fallas en climatización del data center	Administración mal intencionada del dispositivo	Paralización de servicio	3	2	6	$15,000	1HRS	Contar con Equipo de Respaldo
ROUTER	RED	Varias personas tienen la clave de routers	Administración mal intencionada del dispositivo	Paralización de servicio	3	2	6	$1,000	1HRS	

Tabla 4-10: Requerimientos y Estrategias de Router y Switch

ACTIVO	PROCESO	VULNERABILIDAD	AMENAZA	RIESGO	IMPACTO	POSIBILIDAD DE OCURRENCIA	SERVIDAD	DAÑOS AL NEGOCIO	RTO (Recovery times objetives)	ESTRATEGIA CONTINUIDAD
MODEM	INTERNET	Fallas en climatización del data center	Daño irreparable del dispositivo	Paralización de servicio	3	2	6	$15,000	1HRS	Contar con Equipo de Respaldo
CENTRAL TELEFONICA	COMUNICACIONES	Fallas en climatización del data center	Daño irreparable del dispositivo	Perdida de comunicación interna y externa	2	2	4	$ 3,000	4HRS	
		Varias personas conocen la clave de la central telefónica	Administración mal intencionada de la central	Perdida de comunicación interna y externa	3	2	3	$2,000		

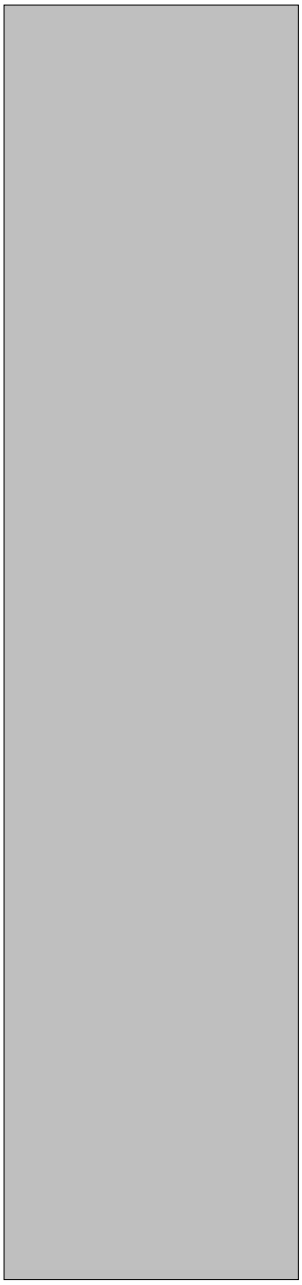
Tabla 4-10: Requerimientos y Estrategias de Modem y Central Telefónica

4.3 ETAPA DE IMPLEMENTACIÓN

Debido a que este tema es elaborado como proyecto de graduación no se lo implementara en la inmobiliaria, dejando así la documentación para la implementación por parte de la inmobiliaria, sin embargo se deja elaborado el Plan de Continuidad de Negocio para que pueda ser ejecutado en caso de siniestros en el Anexo2.

4.4 ETAPA DE OPERACIÓN

Luego de la implementación del plan de continuación de negocio la Inmobiliaria tiene como tarea la capacitación y entrenamiento del personal responsable de ejecutar el plan de continuidad de negocio, adicionalmente deberá hacer un control de cambio sobre el pan de continuidad de negocio.
Se anexa un plan de pruebas detallado para que los responsables del plan lo ejecuten en el Anexo 3.



CAPÍTULO 5
CONCLUSIONES Y RECOMENDACIONES

5. CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

La seguridad de la información se ha convertido actualmente en una de las mayores preocupaciones de las organizaciones debido a que la información es un activo crítico cuyo riesgo de pérdida podría llevar a soportar muchas consecuencias negativas para la organización, como pérdidas financieras, pérdida de imagen o inclusive la quiebra.

La seguridad de la información es una medida para incrementar el éxito de los negocios. El implementar un Sistema de Gestión de gestión de continuidad de negocios, tal como el que plantea la norma ISO 27002, puede ayudar que una organización cumpla favorablemente los incentivos de mercadotecnia, los financieros y las preocupaciones de empeño para ayudar a lograr oportunidades de crecimiento.

La norma ISO 27002 proporciona una base para la Gestión de Continuidad de Negocios, de forma tal que se puede aplicar a cualquier requisito del plan de continuidad y debe ser ajustable a futuros reglamentos y requisitos brindando una metodología para la administración de los riesgos que pueden afectar la información de la organización.

Un Sistema de Gestión de Seguridad de la Información se basa en el ciclo Planificar, Hacer, Verificar, Actuar que permite mantener un proceso de mejora continua del sistema, brindando una seguridad razonable que los riesgos que pueden afectar a la seguridad de la información, pueden ser administrados de manera eficiente en todo momento.

La empresa inmobiliaria no está libre de ataques que comprometan la seguridad de la información y de las debidas consecuencias que éstas podrían ocasionar.

5.2 RECOMENDACIONES

Se recomienda que durante todas las fases del plan de continuidad de negocios se cuente con el apoyo correspondiente por parte de las altas autoridades de la empresa inmobiliaria y del personal a su cargo.

Concienciar a todos los empleados de la empresa sobre la importancia de la seguridad de la información.

Es importante que la dirigencia de la empresa inmobiliaria, en el caso de adoptar éste y futuros trabajos de diseño del Sistema de Gestión de Seguridad de la Información para su implementación, realicen previamente una revisión del análisis de riesgos debido a que éstos cambian constantemente y puedan presentarse nuevos riesgos que no existían durante la realización del presente trabajo o de otros que se realicen en el futuro.

Se recomienda realizar un cronograma detallado para la implementación de los controles determinados durante el desarrollo del presente trabajo, basado en la propuesta de implementación.

Se recomienda una constante evaluación del Sistema de Gestión de Seguridad de la Información mediante auditorías externas, las cuales forman parte de la metodología de

CAPÍTULO 6
PLAN DE CONTINUIDAD DEL NEGOCIO

6. PLAN DE CONTINUIDAD DEL NEGOCIO

6.1 CONTACTOS EN CASO DE EMERGENCIA

Tipo de Amenaza	Contacto	Número Teléfono (Trabajo)
Sismo o Terremoto	Bomberos Defensa Civil	232-5128 242-1020
Huracanes / Tornados		
Inundaciones		
Amenazas de Bombas	Policía Antibombas	
Incendios		
Crimen Computacional		
Disturbio / Vandalismos	Policía Nacional	243-6548
Sabotaje / Huelga laboral	Seguridad Privada	911
Asaltos / Toma de Instalaciones	Rescate y Emergencia	

Tabla PCN-1 Contactos de Emergencias

6.2 CONTACTO EN CASO DE EMERGENCIA INTERNA

Tipo de Amenaza	Contacto	Número Teléfono (Trabajo)	Número Teléfono (casa)	Número Teléfono (celular)
Tecnológicos				
Alteración de datos	Jefe de CST	2839000 Ext. 2919	245-0051	087399562
Fallas de hardware	Jefe de Soporte	2839000 Ext. 2916	256-3456	097652366
Código malicioso				
Fuera de servicio en telecomunicación	Administrador IT	2839000 Ext. 2917	245-6551	084556515
Fuera de servicio en centro de cómputo matriz				
Infraestructura				
Fallas Energía Eléctrica	Administración General	2839000 Ext. 2917	258-9312	085323533
Fuga de agua				

Tabla PCN-2 Contactos del Equipo de Continuidad del Negocio

La actualización del Plan de Continuidad del Negocio, ha sido por los directivos:

Nombre	Cargo	Fecha y Firma de Aprobación
Mario Alberto Bayas Nicola	Gerente General	29/03/2011
Javier Rafael Méndez Reinoso	Gerente Financiero	29/03/2011
Juan Fernando Altamirano Sánchez	Vicepresidente de Tecnología	29/03/2011

Tabla PCN-3 Directorio Responsable

6.3 ANÁLISIS DEL IMPACTO DEL NEGOCIO

- Ejecutar todo el ciclo del proceso de Continuidad al menos una vez por año.

6.4 PLAN ESTRATÉGICO

- Revisar el Plan Estratégico al menos una vez al año.
- Actualizar el Plan Estratégico.
- Incorporar los cambios identificados en el Análisis de Impacto del Negocio (BIA).

6.5 PLAN DE CONTINUIDAD DEL NEGOCIO

- Asegurar que todas las unidades de negocio tienen o tendrán acceso al hardware, software y personal designado según requerimientos o planificación.

- Identificar y actualizar la información de los miembros titulares y suplentes de los equipos, y grupos designados en el plan.

- Verificar que cada miembro de equipo acepte y apruebe su rol y responsabilidades definidas en el plan.

- Revisar periódicamente que los sitios alternos designados para el funcionamiento de las facilidades/equipos críticos, y asegurar que se encuentren en óptimas condiciones.

- Revisar periódicamente los requerimientos de recursos y equipos y la asignación de los miembros de cada equipo.

- Determinar los procedimientos específicos para declaración de desastre.

- Identificar a los responsables del mantenimiento del Plan de Continuidad del Negocio.

- Capacitar al personal con las estrategias de recuperación y los procedimientos desarrollados para la continuidad de operaciones en contingencia.

- Efectuar pruebas periódicas de las estrategias desarrolladas en el Plan de Continuidad del Negocio.

6.6 MANTENIMIENTO Y DISTRIBUCIÓN DEL PLAN DE CONTINUIDAD DEL NEGOCIO

Un Plan de Continuidad del Negocio es un documento "vivo" que deber ser revisado y actualizado periódicamente para reflejar los cambios organizacionales y del negocio. Este plan debe ser mantenido por el personal designado. Es importante que estas personas conozcan que:

- Los cambios en la organización y los procedimientos internos de las áreas pueden causar un impacto en el Plan de Continuidad del Negocio.

- Cambios en el personal, causan un impacto en las conformaciones de los diferentes equipos y grupos, tanto del Plan de Continuidad del Negocio.

- Los involucrados de las empresas para cada función crítica ***deben ayudar*** a mantener actualizado el Plan de Continuidad del Negocio:

- Protegiendo todos los activos del área bajo su responsabilidad.

- Comunicando la importancia de esta responsabilidad a su staff.

- Participando activamente en los procesos de planificación y evaluación del Plan.

- Manteniendo a su staff actualizado sobre los procedimientos de mantenimiento del plan.

- Asegurando que los procedimientos y actividades en este plan sean ejecutados apropiadamente en caso de ser necesario.

- Capacitando al personal en los procedimientos de contingencia desarrollados para mantener la continuidad de las operaciones.

- Participando en las pruebas anuales y dando sugerencias para el mejoramiento del mismo

Para facilitar el mantenimiento del documento, un **"Responsable BCP"** debería ser designado **por cada unidad de negocios**. Esta persona será responsable de mantener y asegurar que todas las actividades de preparación sean realizadas.

6.7 VISIÓN GENERAL DEL PLAN DE CONTINUIDAD DEL NEGOCIO

6.7.1 DECLARACIÓN DE POLÍTICA

Es política de la Inmobiliaria tomar los pasos apropiados para mantener operativos los procesos críticos en caso de ocurrir un desastre mayor en las instalaciones.

Un desastre mayor es una interrupción no anticipada de las operaciones del negocio por un periodo inaceptable de tiempo. El propósito del Plan de Continuidad del Negocio es el de proporcionar a la organización los medios para cumplir con esta política de una forma efectiva y organizada.

El Plan de Continuidad del Negocio es una guía para la recuperación de funciones Críticas o procesos de negocios definidos por la administración. El Plan de Continuidad del Negocio incluye las estrategias de recuperación para todas las funciones críticas.

El propósito de este documento consiste en los siguientes:

- Estar preparado para tantas contingencias como se pueda y desarrollar tantos procedimientos necesarios para sobrevivir a un desastre, antes de que éste ocurra.

- Definir roles e identificar al personal clave que manejará el proceso de recuperación y restauración del negocio después del desastre.

- Identificar a los contratistas, proveedores y recursos necesarios que participen en el proceso de continuidad del negocio

- Establecer procedimientos para mantener informados a los empleados y al público en general sobre la evolución del desastre ocurrido y las acciones tomadas.

6.8 FASES DEL PLAN DE CONTINUIDAD DEL NEGOCIO

El Plan de Continuidad del Negocio consiste de cuatro fases: (1) Preparación, (2) Respuesta Durante la Emergencia, (3) Recuperación y (4) Restauración de Operaciones, cada una con sus propios objetivos. El éxito del Plan de Continuidad del Negocio depende de las actividades y responsabilidades de (1) Preparación, tales como la revisión y actualización de los planes de continuidad. La duración de cada fase dependerá de la naturaleza de evento y su efecto sobre las funciones críticas del negocio.

1. **Responsabilidades Preparación:** Estas acciones de mantenimiento preliminares son tomadas antes de que ocurra cualquier evento. Su propósito es preparar una variedad de escenarios de desastre para asegurar el éxito de la respuesta.

2. **Respuesta Durante la Emergencia:** Estas son acciones inmediatas tomadas durante el evento desplegado. Su propósito es el de proteger la vida, seguridad. Una vez que se lo ha logrado, la prioridad cambia a la mitigación del daño y la preservación de la propiedad. Se decidirá si se debe declarar un desastre basados en evaluaciones detalladas del impacto del evento sobre las funciones críticas de negocio.

3. **Operaciones de Recuperación:** Esas acciones comienzan tan pronto se ha declarado un desastre. El objetivo de recuperación es la continuidad de las funciones críticas. Esta fase continúa hasta que la recuperación de las instalaciones se termine y las operaciones estén listas para volver a la normalidad.

4. **Operaciones de Restauración:** Esta fase incluye las tareas requeridas para reconstruir las instalaciones dañadas y restaurar la funcionalidad del negocio en su sitio de origen. La restauración ocurre de forma paralela con las operaciones de recuperación. Esto involucra la reconstrucción, reparación y restablecimiento del negocio al nivel en que se encontraban antes del desastre.

6.9 ALCANCE DEL PLAN

El Plan de Continuidad del Negocio debe definir el alcance del desastre para el que ha sido diseñado. Mientras los tipos de desastre son demasiado numerosos para nombrarlos por completo, los efectos pueden ser categorizados en dos escenarios generales:

Evento localizado – Un evento que interrumpe las operaciones de procesamiento, y hace que los servicios principales no se encuentre disponible para su uso. Ese escenario requerirá de la reubicación total o parcial de las operaciones críticas del negocio a un Sitio de Recuperación Alterno. La negación de acceso al edificio (ejemplo: debido a un acto terrorista) es también considerado un desastre localizado.

6.10 ORGANIZACIÓN DE LA RECUPERACIÓN

Para facilitar la recuperación ordenada y rápida de las funciones críticas, se ha definido a los Equipos de Recuperación para supervisar y realizar las actividades necesarias para seguir operando en contingencia, los cuales cruzan las barreras de la organización y afectan a todo el personal y a las funciones de negocios. Los equipos de recuperación creados son:

Equipo	Fase de participación		
	Respuesta Durante la Emergencia	Recuperación	Restauración
Equipo de Continuidad de Negocio (ECN).	✓	✓	✓
Tecnología y Seguridad de Información • Equipo técnico (ET)	✓	✓	✓

Tabla PCN-4 Organización de la Recuperación

El primer equipo en responder a un evento será el Equipo de Continuidad de Negocio (ECN). El ECN es responsable por evaluar la situación y activar el Plan de Continuidad del Negocio. El ECN será activado por el Líder quien debe ser contactado por cualquier empleado de la empresa (o cualquier persona) sobre el evento ocurrido. La decisión concerniente a cuáles equipos serán activados bajo cada fase será tomada por el ECN y estará basada en la naturaleza específica del evento.

6.11 TECNOLOGÍA Y SEGURIDAD DE INFORMACIÓN

El Equipo de Continuidad de Negocio (ECN) trabajará en conjunto con el Equipo Técnico para evaluar el daño en las instalaciones y la extensión del mismo. El Equipo Técnico, trabajará en conjunto para determinar medios alternativos de telecomunicaciones o de acceso a la red, en caso de ser necesario. Este Equipo deberá activar el Data Center (Centro de Cómputo) Alterno si se requiere, una vez que sea indicado por el ECN, según los procedimientos elaborados por el área de Tecnología.

6.12 EQUIPOS DE RECUPERACIÓN

EQUIPO	SITIO DE REUBICACIÓN	TRABAJAR A DISTANCIA (**)
Equipo de Continuidad del Negocio (ECN)	**OFICINAS SAMBORONDON**	**X**
Equipo Técnico	**OFICINAS ALBORADA**	**X**

Tabla PCN-5 Equipos de Recuperación

6.13 EQUIPO DE OPERACIONES

GRUPO	PROCESOS CRÍTICOS DEL NEGOCIO	SITIO DE REUBICACIÓN	CAPAZ DE TRABAJAR A DISTANCIA (**)
Equipo Técnico	Administrador de Red Técnicos de Soporte	OFICINAS ALBORADA	**X**

Tabla PCN-6: Equipo de Operaciones

6.14 PROCEDIMIENTOS DE RECUPERACIÓN – EMPRESA INMOBILIARIA

Existen 4 componentes que conforman el Plan de Continuidad del Negocio de la Empresa Inmobiliaria:

- Procedimientos de acciones inmediatas en caso de desastre.
- Procedimientos para recuperación de operaciones en los sitios alternos de procesamiento.
- Procedimientos para evaluación de daños y restauración del sitio.
- Procedimientos para retornar las operaciones en un sitio permanente.

6.15 PROCEDIMIENTOS DE ACCIONES INMEDIATAS EN CASO DE DESASTRE

Esta sección define los procedimientos a ser seguidos para cualquier evento que pudiera causar una interrupción de las funciones críticas del negocio. El término "Desastre" aplica a interrupciones de emergencia de servicios importantes (ejemplo: electricidad, telecomunicaciones) o cualquier cosa que cause la destrucción total o parcial de las instalaciones.

6.16 EVENTO OCURRE MIENTRAS LAS INSTALACIONES ESTÁN OCUPADAS

En caso de que ocurra un evento de falla en los sistemas/equipos mientras las instalaciones están ocupadas, todo el personal presente debe recordar que la más alta prioridad es el preservar las vidas y la integridad de las personas del área. El personal notificará el evento ocurrido. Si los miembros del ECN no pueden ser localizados, el superior que esté disponible en ese momento asumirá el rol de Líder del ECN y comenzarán el proceso de responder al evento.

Si se presenta un evento que interrumpa los servicios, se deben realizar los siguientes pasos para todo el personal afectado:

Responsable	Actividad
Vendedor	Confirmar si el problema es de aplicativo
Vendedor	Si confirma paso anterior, ir al siguiente, sino descartar
Vendedor	Notificar al ECN fallo presentado
ECN	Escalar a departamento técnico para la verificación del problema
Equipo Técnico	Registra el evento e inicia la investigación
Equipo Técnico	Una vez que el equipo técnico ha identificado el problema pasa el informe de daños al ECN.
ECN	Revisa el informe y procede a poner en marcha el plan de continuidad de negocio por medio del Equipo técnico
Equipo Técnico	Se dividirá en dos para atender el sitio principal y otro movilizarse al sitios alterno para preparar la recuperación de los servicios críticos correo y ventas
Equipo Técnico	Inicia con la identificación de la naturaleza del problema

- Determinar la naturaleza del problema.

Responsable	Actividad
Equipo Técnico	Una vez identificado la naturaleza del problema e identificado los servicios perdidos
Equipo Técnico	Confirma si dentro de los servicios perdidos están Ventas y Correo si es así ir al siguiente paso sino terminar el proceso e informar.
Equipo Técnico	Pedirá al Administrador de Red el ultimo respaldo de las bases de datos que prestan los servicios de ventas y correo de la inmobiliaria
Administrador de Red	Copiara los respaldos de las base de datos en la unidad externa designada exclusivamente para estos eventos
Administrador de Red	Se contactará con soporte el soporte técnico que este designado para transportar el respaldo de las base de datos de Ventas y Correo
Soporte Técnico	Se encarga de transportar los respaldos al sitio alterno donde se encontrara parte del Equipo Técnico preparando los equipos en el sitio alterno para recuperar los servicios de ventas y correo.

Tabla PCN-7: Eventos con Instalaciones Ocupadas

6.17 PROCEDIMIENTOS PARA RECUPERACIÓN DE PROCESAMIENTO EN LOS SITIOS ALTERNOS

Una vez en el sitio alterno de procesamiento, el Equipo Continuidad de Negocio y Equipo Técnico, debe iniciar las actividades para restaurar los sistemas y aplicaciones críticas, según lo establecido en el **Plan de Recuperación de Desastres (DRP), Desarrollado por el Equipo Técnico y el ECN de la Inmobiliaria**.

Una vez que los servicios tecnológicos han sido recuperados en el Centro de Cómputo Alterno el ECN debe notificar a todo el personal la disponibilidad de los servicios y que el sitio alterno de recuperación de operaciones es la Localidad de Alborada

Actividad	Responsable
Equipo Técnico	Parte del equipo técnico que se desplazó al sitio alterno prepara los servidores y enlaces que restablecerán los procesos de ventas y comunicación (Correo)
Equipo Técnico	Se encargara de poner en red los servidores de respaldo de Base de datos para Ventas y de Correo para restablecer los servicios críticos
Equipo Técnico	Ejecutará procedimiento de switcheo de enlaces y restauración de respaldos en los servidores para restablecer procesos de Ventas y Comunicación (Correo) administrado por el Administrador de Red.

Tabla PCN-8: Recuperación Sitios Alternos

- Procedimiento de restauración de respaldos

Responsable	Actividad
Equipo Técnico	Toma el ultimo respaldo de la base de datos de Ventas y el ultimo respaldo de Correo
Equipo Técnico	Procede de a levantar los respaldos en los servidores
Equipo Técnico	Una vez terminado el levantamiento de los respaldos en los servidores se informa al administrador de red
Administrador de Red	Verifica que los servidores estén en línea y operativo, adicionalmente que los enlaces alternos estén funcionales
Administrador de Red	Informa al ECN para que notifique a la Inmobiliaria de que ya se puede seguir laborando

Tabla PCN-9: Restauración de Respaldos

6.18 PROCEDIMIENTOS PARA EVALUACIÓN DE DAÑOS

Una vez ocurrido el siniestro el administrador de red deberá evaluar y hacer un informe de los daños e n hardware y software del Data Center (Centro de Cómputo) mismo que será enviado por el **ECN** para la respectiva toma de acciones.

Responsable	Actividades
Administrador de Red	Se dirige al Data Center (Data Center) a revisar los equipos
Administrador de Red	Hace un informe de todos los daños identificados
Administrador de Red	Si es daños de Software, verifica si puede solucionarlo caso contrario da comunica al ECN para poner en marcha el plan de continuidad de negocio.
Administrador de Red	Si es daños de Software, verifica si puede solucionarlo caso contrario da comunica al ECN para poner en marcha el plan de continuidad de negocio.
Administrador de Red	Si es daños de Hardware y Software, verifica si puede solucionarlo caso contrario da comunica al ECN para poner en marcha el plan de continuidad de negocio.
ECN	Pone en marcha Plan de Continuidad de Negocio

Tabla PCN-10: Evaluación de Daños

6.19 PROCEDIMIENTO PARA RETOMAR LAS OPERACIONES EN UN SITIO PERMANENTE

Una vez que el sitio permanente ha sido habilitado/rehabilitado, se deberá preparar la mudanza de las operaciones y procesos en este sitio. Este retorno debe ser programado un fin de semana para no interrumpir los procesos que se ejecutan con los clientes.

Responsable	Actividad
ECN	Una vez restablecido el Data Center (Centro de Computo) principal informa a la inmobiliaria que se procederá a retornar los servicios del Data Center (Centro de Computo) Alterno
ECN	Pide al Equipo Técnico que preparen los equipos nuevos y respaldos para restaurar el servicio desde el Data Center (Centro de Computo)
Equipo Técnico	Pide los respectivos respaldos para la restauración de Ventas y comunicación (Correo) al Administrador de Red
Administrador de Red	Se encargara de pedir los respaldos en un disco duro externo de uso exclusivo para estos casos al soporte técnico designado
Soporte Técnico	Se encarga de transportar del sitio Alterno al sitio principal los respaldos y entrega al Equipo Técnico
Equipo Técnico	Se encarga de subir los respaldos en los servidores en informa al Administrador de Red
Administrador de Red	Se en encarga de confirmar de que tos este operativo y los enlaces en línea en el sitio permanente
Administrador de Red	Informa de que se finalizó con la restauración del servicio al ECN
ECN	Comunica a la Inmobiliaria que ya se restablecieron las operaciones normales de la misma.

Tabla PCN-11: Operaciones en sitio Permanente

Figura PCN-1: Diagrama Secuencia de Operaciones

6.20 EQUIPOS CONTINGENTES

A continuación describiremos el organigrama de los equipos del Plan de Continuidad del Negocio.

6.21 ORGANIGRAMA – EQUIPOS PLAN DE CONTINUIDAD DEL NEGOCIO

Figura PCN-2: Plan de Continuidad ECN

6.22 PLAN DE PRUEBAS Y MANTENIMIENTO DEL PLAN

6.23 PLAN DE PRUEBAS

6.23.1 PROPÓSITO

A fin de que el **Plan de Continuidad del Negocio** provea una capacidad real de recuperación en el caso de un desastre, el mismo debe ser probado. El propósito de la prueba es la retroalimentación que se logre obtener para ajustar el Plan y/o corregir las desviaciones que el mismo presente sobre lo que realmente se requiera, dentro de las pruebas se incluyen los siguientes objetivos:

- Validar (e identificar ajustes requeridos) a los procedimientos y estrategias del plan.
- Obtener información acerca de los tiempos de implementación de la recuperación (para demostrar qué tan rápido, por ejemplo, puede recuperarse una aplicación crítica).
- Demostrar el rendimiento de los sistemas y aplicaciones que se encuentran en el Centro de Cómputo Alterno, en comparación al rendimiento durante la operación normal.

- Demostrar el diseño e implementación adecuado del Plan de Continuidad del Negocio.

- Familiarizar a los equipos definidos en el Plan de Continuidad con sus roles definidos.

Antes de probar el Plan de Continuidad del Negocio es fundamental conocer los factores críticos de éxito de la prueba:

No existe "prueba fallida": El objetivo de la prueba no es exclusivamente demostrar que el plan funciona, sino obtener retroalimentación acerca de cómo funciona; por lo tanto, toda prueba es "válida". Lo principal de una prueba no es que finalice sin problemas, sino revisar los resultados y los problemas hallados y usar ambos para actualizar o modificar los procedimientos del Plan de Continuidad del Negocio.

No es necesaria una "prueba en producción": un motivo usual para no probar el Plan de Continuidad del Negocio es el temor a paralizar la empresa a efectos de simular las condiciones de desastre. De hecho, casi nunca se paraliza realmente el procesamiento informático durante un ejercicio de prueba. La prueba se conduce de forma concurrente con el procesamiento normal, ya sea de manera independiente o en paralelo, con el fin de obtener datos comparativos entre el procesamiento normal y el degradado. A efectos de que el personal que participa en la prueba no afecte el normal desarrollo de sus tareas por estar involucrado en la prueba, se deberá prever la misma para períodos de menor actividad o fuera de horas pico, en turnos de trabajo alterno o durante fines de semana.

No es correcta una "única prueba completa": otro motivo usual para postergar la prueba del Plan de Continuidad del Negocio es el supuesto que una prueba no tiene validez si no contempla la totalidad de la empresa. Sin embargo, ésta es recién la última fase del plan de pruebas. El Plan de Continuidad del Negocio fue desarrollado en capítulos y a efecto de probar los mismos, es necesario incluir en el plan de pruebas todos los procesos del Plan de Continuidad del Negocio.

La prueba no garantiza "estar listos" para un desastre, sino solamente "estar preparados". La diferencia reside en que el primero supone que un Plan de Continuidad del Negocio garantizará, "por sí mismo", a la empresa la recuperación de un desastre (otorgará un conjunto de acciones completas a ser seguidas fielmente en caso de una emergencia). Esto no es cierto: un desastre real contiene muchos elementos impredecibles y un Plan de Continuidad del Negocio no puede nunca preverlos todos. En el mejor de los casos, el resultado de una prueba habrá familiarizado al personal con un grupo de estrategias básicas y que han demostrado funcionar bajo circunstancias controladas, para lidiar con una interrupción imprevista.

6.24 FRECUENCIA DE LAS PRUEBAS

El **Equipo Responsable de las Pruebas** tiene a su cargo el establecimiento de un cronograma de pruebas el cual se definirá de acuerdo a los capítulos o componentes del plan, las pruebas de todos los componentes del plan se deberán cumplir en el lapso de un año, dicho cronograma debe incluir las fechas y los responsables de cada capítulo a ejecutar. Además, cada vez que se realice un cambio mayor, que podría afectar alguno de los componentes claves del Plan de Continuidad del Negocio, se realizará una prueba de la parte afectada.
Se puede ajustar un plan de pruebas sujeto a los parámetros que se definen en el adjunto, donde se establecen de forma general las consideraciones de cada prueba de forma que se logre probar todos los componentes del plan sin que esto implique hacer una prueba completa al mismo.

6.25 DESIGNACIÓN DEL EQUIPO DE PRUEBAS

El personal responsable de realizar las pruebas del Plan de Continuidad del Negocio debe ser nombrado por el Equipo de Continuidad de Negocio y deben ser usuarios claves de las áreas de negocio de la Inmobiliaria:

Área	Nombre	Cargo
Ventas – (una persona)	Madeleine Mendoza	Gerente de Ventas
Contable – (una persona)	Juan Perez	Contador General
Procesos Internos - Líder del Equipo	Pablo Granados	Jefe de IT (Infraestructura tecnológica)
Negocios – (una persona)	Daniel Soto	Gerente General
Operaciones – (una persona)	Luis Mata	Jefe de Operaciones
Financiero – (una persona)	Vanessa Jacome	Gerente Financiera
Sistemas – (una persona)	Manuel Moreno	Jefe de ST (Servicios Tecnológicos)

Tabla PCN-12: Designación de Equipos de Prueba

6.26 TIPOS DE PRUEBAS

6.27 PRUEBAS ESTÁTICAS

Las pruebas estáticas sólo involucran la revisión y actualización escrita de los componentes del plan. Las pruebas estáticas serán realizadas para lo siguiente:

- Verificar la información del personal contacto.
- Verificar la información de los proveedores y contratistas.

6.28 PRUEBAS DE VALIDACIÓN

Las pruebas de validación son usadas para verificar los procedimientos usados por las personas o los equipos. Esas pruebas involucran por lo general discusiones de grupo sobre la efectividad de los procedimientos a medida en que ellos aplican a los objetivos del equipo. Las pruebas de validación serán realizadas para lo siguiente:

- Como un método de evaluación del plan inicial para nuevos planes de continuidad del negocio.
- Al momento de la adición o revisión de objetivos y actividades de cada equipo.
- Cuando han ocurrido cambios substanciales a los procedimientos operativos.

6.29 PRUEBAS DE SIMULACIÓN

Una prueba de simulación es una representación de las condiciones de desastre. Los participantes son presentados ante un escenario de desastre y se les pide describir en detalle su respuesta combinada para este evento. Las respuestas en caso de desastre son limitadas únicamente aquellos procedimientos documentados en el Plan de Continuidad del Negocio. Esto permite a los participantes verificar la fidelidad del presente plan sin confiar en las acciones no documentadas. Esas pruebas podrían o no ser anunciadas.

Para promocionar la confianza en la capacidad de la Inmobiliaria para recuperarse de cualquier situación de emergencia, los escenarios deberían ser variados.

Debería designarse un observador para qué tome nota del desempeño de los diferentes grupos. El observador identificará los problemas que ocurren como resultado de una información faltante, incompleta o errada. Una vez que el escenario esté completo, el grupo revisará las deficiencias y propondrá las revisiones apropiadas.

Esta forma de evaluación es útil al determinar la capacidad de reacción de un equipo para responder a los diferentes escenarios. Sustituyen a las Pruebas Dinámicas o "en vivo" cuando aquellas no resultan viables.

6.30 PRUEBAS DINÁMICAS O EN VIVO

Las pruebas dinámicas son operativas en naturaleza. Las pruebas dinámicas son requeridas únicamente cuando los procedimientos de recuperación no pueden ser desarrollados de manera apropiada con los otros tres tipos de prueba.

Ejemplos de pruebas en vivo:

- Recreación del ambiente dentro de la instalación actual o en la instalación provisional en paralelo con el procesamiento de datos existentes.

- Planes que involucran a proveedores externos.

En la medida en que estos ejercicios puedan por si mismos conducir a una interrupción significativa en las operaciones normales, deberían ser únicamente conducidas con la planificación y notificación anticipada y la total aprobación y cooperación de la Alta Gerencia.

6.31 LINEAMIENTOS DE LA PRUEBA

Todos los usuarios deberán ser notificados si se está realizando una evaluación. Únicamente las pruebas de simulación podrían no ser anunciadas y entonces sólo después de suficientes pruebas previas la gerencia las aprobaría.
Todas las pruebas sin importar si son anunciadas o no deberían ser preparadas de forma adecuada por adelantado. Debería desarrollarse un programa de evaluación con marcos de tiempo establecidos para cada paso del proceso. Una sola persona debería ser responsable por coordinar el programa de evaluación.
Un programa de evaluación extensivo debería incluir:

- Procedimientos generales para la ejecución de la prueba.
- Procedimientos de contingencia, en caso de que haya algún problema.
- Puntos de terminación de la prueba, sin importar si una tarea ha sido completada.
- Procedimientos de cierre de operaciones.
- Procedimiento de recuperación de operaciones.
- Recuperación de registros de vida, suministros de información, etc.

6.32 MANTENIMIENTO DEL PLAN DE CONTINUIDAD DEL NEGOCIO

6.32.1 PROPÓSITO DEL MANTENIMIENTO

El Equipo de Mantenimiento organizará la revisión y actualización del plan cada seis meses o anualmente. A su vez la Vicepresidencia de Sistemas, así como los líderes de cada equipo, son responsables de comunicar los cambios (disparadores) que se han producido y que demanden de una actualización del Plan de Continuidad del Negocio.

6.32.2 DESIGNACIÓN DEL EQUIPO DE MANTENIMIENTO

El personal responsable de realizar el mantenimiento del Plan de Continuidad del Negocio será nombrado por el Equipo de Continuidad del Negocio y deben ser usuarios claves de las áreas de negocio de la inmobiliaria.

Nombre	Cargo	Área
Mario Alberto Bayas Nicola	Gerente General	Gerencia de la Inmobiliaria
Javier Rafael Mendez Reinoso	Gerente Financiero	Financiero
Juan Fernando Altamirano Sanchez	Vicepresidente de Tecnología	Tecnología

Tabla PCN-13: Designación Equipo de Mantenimiento

6.32.3 TABLA DE DISPARADORES DE MANTENIMIENTO

A efectos de facilitar la tarea de mantenimiento del plan, hemos desarrollado un detalle de los cambios que potencialmente son "disparadores de mantenimiento" y los aspectos del Plan de Continuidad del Negocio que se verían afectados.

Cambio en el ambiente	Aspecto afectado en el Plan
Modificación importante a una aplicación	• Aplicaciones y base de datos del sitio alterno • Hardware del sitio alterno de procesamiento • Requerimientos de comunicación de dat • Procedimientos de recuperación del sitio alterno
Aplicación nueva	• Aplicaciones y base de datos del sitio alterno • Hardware del sitio alterno de procesamiento • Requerimientos de comunicación de datos • Procedimientos de recuperación del sitio alterno
Cambios en el hardware	• Hardware del sitio alterno • Sistema operativo del sitio alterno • Inventario de equipos de computación • Análisis y estimación del daño
Cambios en equipos de comunicación	• Requisitos de comunicaciones en el sitio alterno, inventario de equipos de comunicación de datos • Análisis y estimación del daño.
Cambios en el software del sistema	• Sistema operativo en el sitio alterno.
Cambios en la seguridad física	• Procedimientos de emergencia
Cambios en el sitio alterno de Procesamiento	• Viabilidad del sitio alterno de procesamiento • Procedimientos de arranque y/o operaci • Procedimientos de recuperación del sitio alterno.
Cambios al personal (ingresos, egresos, cambios en funciones) o cambios a la estructura organizativa del personal	• Notificaciones en procedimientos de emergencia, equipos de recuperación, responsables por aplicaciones críticas, distribución del plan • Directorio telefónico para contingencias.
Cambios en proveedores de servicios	• Notificaciones en procedimiento de emergencia, • Directorio telefónico para contingencias
Cambios en procedimientos de operación	• Procedimientos de alternos de operación de las áreas de negocio afectadas
Cambios en estrategias o negocios	• Aplicaciones críticas o sus tiempos tolerables de interrupción

Tabla PCN-14: Disparadores de Mantenimiento

Todo mantenimiento realizado al Plan de Continuidad del Negocio, ya sea producto de un cambio activado por "disparador de mantenimiento", cambio activado por revisión periódica o cambio producto de una corrección o mejora luego de una prueba del plan, se registrará en una Tabla de historia de mantenimiento.

6.32.4 REVISIÓN PERIÓDICA

Se realizarán revisiones periódicas del Plan de Continuidad del Negocio al menos dos veces al año. El objetivo de estas revisiones es identificar cambios ocurridos en todos los elementos que componen el plan. La revisión puede ser de dos tipos:

- **Revisión física de recursos**
  Visita al sitio alterno con evaluación de inventario de equipos y suministros.
  Almacenamientos externos de respaldo y formularios.

  Acceso a servidores.

- **Revisión lógica de la Información del Plan**

  Verificación de listados de miembros de equipos con cada uno sus datos.
  Verificación de proveedores de servicios.
  Verificación de procedimientos de alternos de operación de las áreas de negocios.
  Verificación de procedimientos de recuperación del sitio alterno de procesamiento.
  Verificación de prioridades y aplicaciones críticas.
  Verificación de software y datos de las aplicaciones críticas.
  Verificación de vigencia de seguro y otros contratos.
  Cambios en planes y proyectos informáticos al corto/mediano plazo.

6.32.5 PROCEDIMIENTO PARA MANTENIMIENTO

- Toda vez que se active un "disparador de Mantenimiento" el funcionario a cargo de esa área notificará al líder del Equipo de Mantenimiento del Plan de Continuidad del Negocio, a fin de activar el procedimiento de mantenimiento.

- Toda vez que, producto de una revisión periódica, el líder del Equipo de Mantenimiento del Plan de Continuidad del Negocio tenga conocimiento de un cambio, activará el procedimiento de mantenimiento.

- El líder del Equipo de Mantenimiento del Plan de Continuidad del Negocio estudia el cambio y sus ramificaciones y establece la incidencia en el Plan de Continuidad del Negocio. Si existe incidencia, actualiza el plan. Deja constancia en la Tabla de Historia de Mantenimiento. Distribuye copias de la actualización a todas las instancias pertinentes.

- El líder del Equipo de Mantenimiento del Plan de Continuidad del Negocio estudia si el cambio da motivo a otras acciones complementarias, como por ejemplo capacitación de personal. En caso de ser así, coordina la ejecución de estas acciones. Deja constancia en la Tabla de Historia de Mantenimiento.

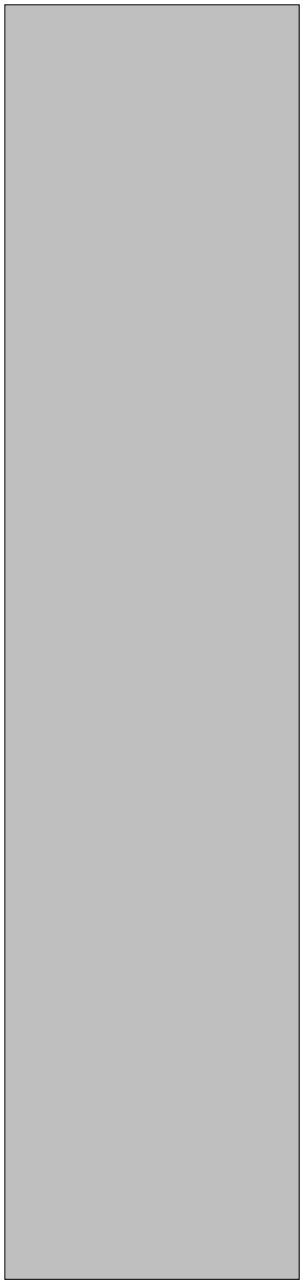
- El líder del Equipo de Mantenimiento decidirá si es necesario probar la actualización realizada. En caso de serlo, realiza la prueba, adaptando el procedimiento de prueba a la magnitud de esta prueba. Deja constancia en la Tabla de Historia de Mantenimiento.

6.32.6 TABLA DE HISTORIA DE MANTENIMIENTO

- Origen de la revisión: "disparador de mantenimiento", revisión periódica, prueba del Plan de Continuidad del Negocio.
- Fecha de la revisión.
- Cambios ocurridos.
- Elementos Plan de Continuidad del Negocio afectados.
- Fecha actualización.
- Elementos Plan de Continuidad del Negocio actualizados.
- Fecha de la prueba.
- Elementos Plan de Continuidad del Negocio probados.
- Otras acciones y comentarios.

6.32.7 DISTRIBUCIÓN DEL PLAN DE CONTINUIDAD DEL NEGOCIO

- A cada miembro del Equipo de Continuidad del Negocio.
- A cada miembro de los equipos conformados en el Plan de Continuidad del Negocio.
- A la Vicepresidencia de Tecnología.
- A los responsables del Data Center (Centro de Cómputo).
- En el sitio alterno de procesamiento.
- En sitio externo de almacenamiento de respaldos.



CAPÍTULO 7
ANEXOS

Métricas de evaluación - alcance de las pruebas del plan sobre una base incrementalmente compleja						
	Parámetros de cada Prueba					
	Prueba 1	**Prueba 2**	**Prueba 3**	**Prueba 4**	**Prueba 5**	**Prueba 6**
Equipos que participan	35%	60%	50%	100%	100%	100%
Tipo de prueba	Dinámica	Simulación	Dinámica	Dinámica	Estática	Dinámica
Controlada	Si	Si	Si	Si	Si	Si
Imprevisto	No	No	No	No	No	Si
Día de prueba	No laborable	No laborable	No laborable	No laborable	No laborable	Laborable
Procesos a recuperar	15%	15%	70%	Plan de evacuación	100%	100%
Plan de evacuación	No	No	No	Si	No	Si
Duración de la prueba	Aprox. 4 horas	Aprox. 6 horas	Aprox. 7 horas	Aprox. 3 horas	Aprox. 8 horas	Aprox. 10 horas

- **COMPLEJIDAD** **+**

Tabla Anexo-1: Parámetros de cada Prueba

METRICAS DE EVALUACIÓN - ALCANCE DE LA PRUEBA DEL PLAN - INCREMENTO DE COMPLEJIDAD DE LAS PRUEBAS								
	EQUIPOS QUE PARTICIPAN	TIPO DE PRUEB	CONTROLADA	IMPREVISTO	DIA DE PRUEBA	PROCESOS A RECUPERAR	PLAN DE EVACUACIÓN	DURACION DE LA PRUEBA
FECHAS PROPUESTAS								
29/10/2006	ECN Y ET	PRUEBA DINAMICA	CONTROLADA	NO	Día no laborable	VENTAS Y CORREO	NO	APROX. 4 HORAS
FECHA 1	35%	PRUEBA DE SIMULACION	CONTROLADA	NO	Día no laborable	35%	NO	APROX. 6 HORAS
FECHA 2	50%	PRUEBA DINAMICA	CONTROLADA	NO	Día no laborable	50%	NO	APROX. 12 HORAS
FECHA 3	70%	PRUEBA DE VALIDACION	CONTROLADA	NO	Día no laborable	70%	NO	APROX. 10 HORAS
FECHA 4	40%	PRUEBA DE SIMULACION	NO CONTROLADA	NO	Día no laborable	PRUEBA DEL PLAN DE EVACUACION	SI	APROX. 2 HORAS
FECHA 5	100%	PRUEBA ESTATICA	NO CONTROLADA	NO	Día no laborable	100%	NO	APROX. 6 HORAS
FECHA 5	100%	PRUEBA DINAMICA	NO CONTROLADA	SI	Día laborable	100%	NO	APROX. 6 HORAS

Tabla Anexo-1: Métricas de Evaluación

	FECHA DE LA PRUEBA						
TIPO DE PRUEBA	**27/04/2011**	**29/04/2011**	**30/04/2011**	**02/05/2011**			
CONTROLADA	X	X	X				
NO CONTROLADA				X			

Tabla Anexo-3: Tipo de Prueba

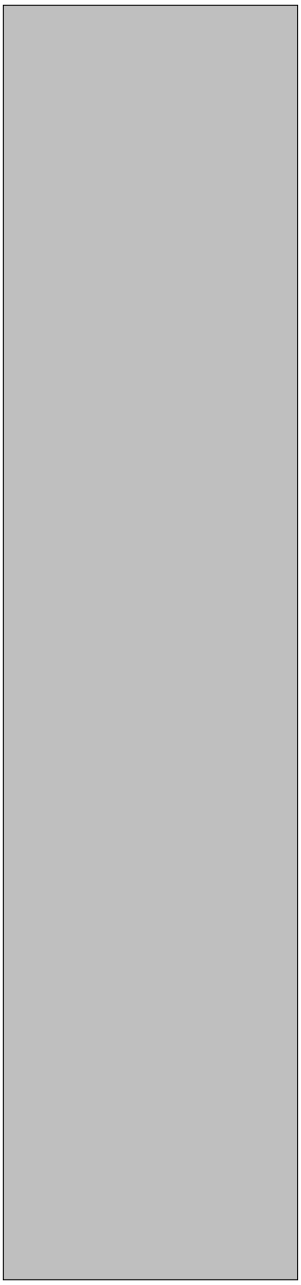
	FECHA DE LA PRUEBA					
DIA DE PRUEBA	**27/04/2011**	**29/04/2011**	**30/04/2011**	**02/05/2011**		
LU, MA, MIE, JUE, VIE, SAB.	X		X	X		
DOM, FERIADOS.		X				
LU, MA, MIE, JUE, VIE.						

Tabla Anexo-3: Día de Prueba

	FECHA DE LA PRUEBA						
DURACION DE LA PRUEBA	**27/04/2011**	**29/04/2011**	**30/04/2011**	**02/05/2011**			
PRUEBA < 1 DIA	X			X			
1 < PRUEBA < 7		X	X				
PRUEBA > 7 DIAS							

Tabla Anexo-3: Duración de la Prueba

7.1 ENLACE DE COMUNICACIÓN GENERAL



BIBLIOGRAFÍA

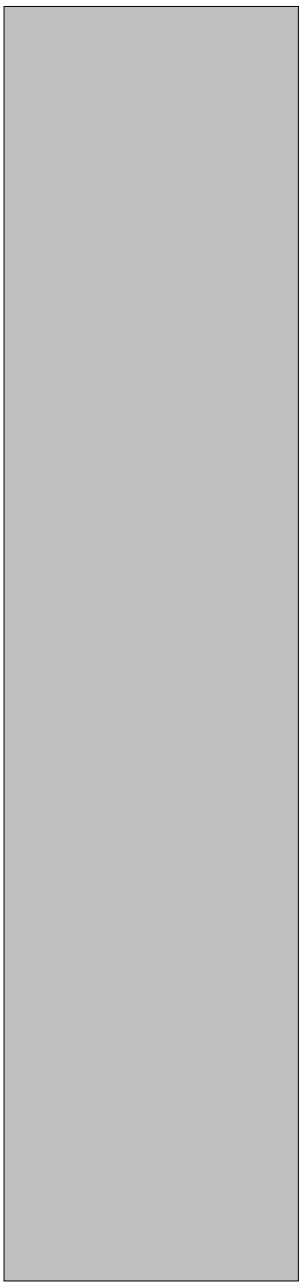
BIBLIOGRAFÍA

Documentos:

- Norma ISO 17799:2000 – International Standar Organization
- Diplomado de Auditoria Informática: Material de estudio
- ¿Qué es la norma ISO 17799? – BSI Management System
- Brochure ISO 17799 - BSI Management System
- iso-27001-2005
- Auditoria de Systems Innovation Group S.L.
- ESA Security Seguridad de la Información
- Infraestructura ITIL (*Information Technology Infrastructure Librar*) Asesores Delta

Enlaces de Internet:

- www.ciudadceleste.com
- www.iso.org
- http://www.s21sec.com/s21sec/ser_iso.jsp
- http://www.iso27001security.com/html/iso270001.html
- www.gesteopolis.com
- http://www.iso27000.es/download/doc_iso27000_all.pdf
- http://es.wikipedia.org/wiki/ISO/IEC_27001
- http://www.plannegocios.com/?gclid=CJnKtJaN0KgCFZRd7Aodz1XHlg
- http://es.wikipedia.org/wiki/Plan_de_continuidad_del_negocio
- http://auditoriasistemas.com/plan-de-continuidad-de-negocio/
- http://www.esa-security.com/web/servicios/plan.htm
- http://es.scribd.com/doc/30511024/Metodologia-ITIL
- http://es.wikipedia.org/wiki/ITIL
- http://www.computing.es/Noticias/201011260022/SEGURIDAD-Solo-el-167-de-las-pymes-espanolas-cuenta-con-un-Plan-de-Continuidad-de-Negocio.aspx
- http://seguridadenamerica.com.mx/2010/09/huracanes-derrames-de-crudo-y-la-continuidad-del-negocio/
- http://seguridadenamerica.com.mx/seccion/contra-incendios/
- http://seguridadenamerica.com.mx/seccion/descargas-electricas/
- http://iso-17799.safemode.org/index.php?page=PDCA_Cycle



GLOSARIO

GLOSARIO

Para propósitos de este proyecto y comprensión del trabajo de investigación realizado, se aplican los siguientes términos y definiciones:

Activo: cualquier cosa que tenga valor para la organización.

Disponibilidad:
La propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada.

Confidencialidad:
La propiedad que esa información esté disponible y no sea divulgada a personas, entidades o procesos no autorizados.

Seguridad de Información:
Preservación de la confidencialidad, integridad y disponibilidad de la información; además también pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, no-repudio y confiabilidad.

Evento de Seguridad de la Información:
Una ocurrencia identificada del estado de un sistema o red indicando una posible violación de la política de seguridad de la información o falla en las salvaguardas, o una situación previamente desconocida que puede ser relevante para la seguridad.

Incidente de seguridad de la información:
Un solo o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una significativa probabilidad de comprometer las operaciones comerciales y amenazan la seguridad de la información.

Sistema de Gestión de Seguridad de la Información:
Esa parte del sistema gerencial general, basado en un enfoque de riesgo comercial; para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.

Integridad:
La propiedad de salvaguardar la exactitud e inteligencia de los activos.

Riesgo Residual:
Es el riesgo remanente después del tratamiento del riesgo.

Aceptación del riesgo:
Decisión de aceptar un riesgo.

Análisis del riesgo:

Uso sistemático de la información para identificar fuetes y para estimar el riesgo.

Valuación del riesgo:
Proceso general de análisis del riesgo y valuación del riesgo.

Evaluación del riesgo:
Proceso de comparar el riesgo estimado con el criterio de riesgo dado para determinar la importancia del riesgo.

Gestión del riesgo:
Actividades coordinadas para dirigir y controlar una empresa con relación al riesgo.

Vulnerabilidad:
Son los elementos que al ser explotados por amenazas afectan la confidencialidad, disponibilidad e integridad de información de un individuo o empresa.

Tratamiento del riesgo:
Proceso de tratamiento de la selección e implementación de medidas para modificar el riesgo.

Enunciado de aplicabilidad:
Enunciado documentado que describe los objetivos de control y los controles que son relevantes y aplicables al SGSI de la empresa.

NOTA: los objetivos de control y controles se basan en los resultados y conclusiones de los procesos de tasación del riesgo y los procesos de tratamiento del riesgo, los requerimientos legales o reguladores, las obligaciones contractuales y los requerimientos comerciales de la empresa para la seguridad de la información.