Escuela de Contadores Auditores de Santiago
Instituto Profesional

"La DISPONIBILIDAD DE LA TECNOLOGÍA como eje fundamental de la gestión de los riesgos de la empresa que se sustenta en el uso intensivo de la información como herramienta de competitividad y diferenciación"

"Trabajo correspondiente a la 2ª fase"
"del Seminario de Titulación"

Seminario N° 56, Semestre Otoño 2009

Profesor Guía: Max Wachholtz A.

Integrantes : Alejandra González Flores
Jessica Inostroza Espinoza
Cheryll Jorquera Pérez
Isabel Pavez Vásquez
Alejandra Rivas Soto

Santiago, 15 de Julio de 2009

ÍNDICE

IMPORTANTE

EL PRESENTE INFORME FUE ELABORADO POR LAS ALUMNAS NOMBRADAS EN PORTADA CON APOYO DOCENTE, COMO REQUISITO PARA EL PROCESO DE TITULACION QUE LA ESCUELA DE CONTADORES AUDITORES DE SANTIAGO EXIGE A SUS ALUMNOS . ES UNA RECOPILACION COMENTADA DE MATERIAL EXISTENTE EN LA ACTUALIDAD, CUYA UNICA Y EXCLUSIVA FINALIDAD ES SERVIR DE MATERIAL DE APOYO DOCENTE Y ACADEMICO PARA ALUMNOS DE ESCUELA DE CONTADORES AUDITORES DE SANTIAGO Y EN CASO ALGUNO PARA LUCRAR POR SU DIFUSION, DEBEN SER RESPETADOS LOS DERECHOS DE AUTOR CORRESPONDIENTES. POR FAVOR REMITIRSE A LAS CITAS BIBLIOGRAFICAS INCLUIDAS AL FINAL DEL INFORME.

1.- AGRADECIMIENTOS

A nuestros familiares, amigos y compañeros, por haber sido nuestro cimiento en la formación personal, ya que sin su constante apoyo y ánimo, no habríamos sido capaces de afrontar y persistir en la obtención del término de nuestros estudios.

A la institución que nos albergó desde los inicios de nuestra carrera "Escuela de Contadores Auditores de Santiago", que junto a sus docentes guiaron nuestros pasos hacia la excelencia profesional.

Queremos agradecer de forma especial a nuestro profesor guía, Max Wachholtz A. por su apoyo, disposición y compromiso con nuestro trabajo.

Finalmente a todas las personas que a lo largo de este camino nos han apoyado y también a aquellas que hemos omitido involuntariamente, va nuestro agradecimiento.

2.- PROLOGO

En la actualidad el avance de la tecnología es muy amplio, ya que tiene un crecimiento constante en la medida que las compañías dependen cada vez más de las tecnologías de la información para sus procesos de negocio, lo cual implica una mayor atención e importancia a la gestión de los riesgos asociados con los sistemas de TI.

Al abordar la temática que guía esta investigación, nuestro principal objetivo fue interiorizarnos con detenimiento sobre la base de la disponibilidad de la información y su importancia en la actualidad, debido al constante avance de la tecnología.

La disponibilidad es fundamental para la continuidad del negocio, por lo que es necesario salvaguardarlo ante amenazas que puedan afectarlo, así como también la seguridad de la información, todo lo anterior, se convierte en un requisito básico de las empresas ante el desarrollo continuo de la tecnología.

El desarrollo de este informe no estuvo exento de dificultades, los problemas que tuvimos que enfrentar fueron variados, siendo el principal la abundante información referida al tema, el cual nos obstaculizó en la identificación de los tópicos importantes para el desarrollo de la investigación, desviándonos constantemente en el enfoque de Disponibilidad.

3.- INTRODUCCIÓN

El propósito de este documento es presentar la formulación de la *disponibilidad de la tecnología*, cuya administración correcta de los recursos informáticos asegura el acceso de los usuarios a la información de manera rápida y efectiva de la compañía, ante cualquier eventualidad.

A su vez, el término *disponibilidad* hace referencia a la probabilidad de que un servicio funcione adecuadamente en cualquier momento. Más adelante nos avocaremos a este concepto y otros relacionados con el mismo, como lo es la *alta disponibilidad* definiéndola como una serie de medidas tendientes a garantizar la disponibilidad del servicio, es decir, que éste funcione al cien por ciento.

El avance tecnológico nos ha facilitado un acceso más directo sobre diversos temas. En la medida que las compañías dependen cada vez más de las tecnologías de la información para sus procesos de negocio, se está empezando a dar mayor importancia a la gestión de los riesgos asociados con los sistemas de TI.

Por otra parte, la *Administración de la disponibilidad* se encarga de asegurar que los servicios estén disponibles, lo cual establece una estrecha relación de este término con la administración de la capacidad y de la gestión de la disponibilidad y como ésta última es responsable de optimizar y monitorear los servicios de TI para que funcionen sin interrupciones en forma íntegra cumpliendo con los contratos de los proveedores (SLAs) y obteniéndose todo ello a un costo aceptable. El objetivo es aseverar que los servicios de TI estén disponibles y funcionen correctamente según los requerimientos de los clientes y usuarios, en base al marco de los SLAs establecidos.

A lo largo de este escrito mencionaremos cuáles son los riesgos que afectan a la disponibilidad, las contra medidas para evitar los problemas de continuidad y planes de contingencia asociados a la continuidad de las operaciones de la empresa, evitando que los sucesos que se presenten no afecten sus procesos críticos para que puedan seguir prestando los servicios necesarios a los usuarios.

Además explicaremos diversos casos en que las empresas requieren administrar de una manera determinada el uso de la tecnología, lo cual permita mantener sus operaciones críticas disponibles cuando los usuarios lo requieran.

4.- DISPONIBILIDAD DE LA TECNOLOGÍA DE INFORMACIÓN

En la anterioridad, la velocidad de los negocios y el uso que se le daba a la tecnología existente nos permitía tener un tiempo de recuperación ante un evento en el cual estuviéramos sin sistemas de información por un período prolongado, pero hoy el constante avance de la tecnología y la dependencia creciente de ésta, nos hace exigir como clientes una disponibilidad absoluta de nuestros proveedores tecnológicos, para con esto acceder rápidamente a la información.

Para entender lo anterior debemos conocer los conceptos referentes a disponibilidad, detallados a continuación:

"Disponibilidad" El tiempo de actividad normal que esperan los clientes que el servicio funcione sin interrupciones. Siendo el ideal el 100%, ya sea para los usuarios internos y externos que utilizan la información que entrega la empresa.

"Fiabilidad" medida del tiempo durante el cual los servicios han funcionado correctamente de forma ininterrumpida durante un período de tiempo dado. Esto se denomina "continuidad del servicio".

"Mantenibilidad": capacidad de mantener el servicio operativo y recuperarlo en caso de interrupción, pudiendo ser modificado para corregir fallas y mejorar el funcionamiento en las actividades.

"Capacidad de Servicio" determina la disponibilidad de los servicios internos y externos contratados. Cuando un servicio TI es subcontratado en su totalidad la disponibilidad y la capacidad de servicio son términos equivalentes. (1)

"Servicio de Tecnología de Información"
Es un conjunto de recursos que son provistos a los clientes para soportarlos en la operación de una o más áreas del negocio.

Servicio de soporte se presenta generalmente en el día a día operacional y el soporte de los servicios de TI, mientras que entrega de servicios mira al largo plazo para la planificación y mejora la provisión de servicios de TI. (2)

(1) Apunte Gestión de la disponibilidad (ver bibliografía)

(2) Apunte Profesor Miguel Ángel Elizondo TIA

"La alta disponibilidad" consiste en asegurar que los servicios de TI estén disponibles siempre que los clientes y usuarios deseen hacer uso de ellos, eliminando los factores que trabajan en contra del ideal de 100% de disponibilidad. Si es un negocio que sólo esta abierto al público de 8 de la mañana a 6 de la tarde, y en este horario puede cumplir con todo el procesamiento de la información, la disponibilidad durante este período se considera 100%. Por el contrario de la empresa a la que nos referimos se trata de un Banco el que su página Web debe estar disponible las 24 horas del día, los 7 días a la semana, tendrá que disponer de los sistemas de información durante el mismo período para alcanzar el 100% de disponibilidad.

La Alta Disponibilidad se divide en 2 tipos:

1.- Alta disponibilidad de Hardware: Esta consiste en la Redundancia de Hardware, es decir, si se produce un fallo de hardware en alguna de las máquinas (falla fuente de poder, punto de red, cable o tarjeta de red, falla de controladora de discos, switch, etc.), y si nuestra configuración del equipamiento computacional lo permite, podremos cambiar nuestro hardware en caliente (HotSwap), sin tener que bajar los servicios de nuestra empresa.

2.- Alta disponibilidad de Aplicaciones: Si se produce un fallo de las aplicaciones de alguna de las máquinas, el software de alta disponibilidad es capaz de re-arrancar automáticamente los servicios que han fallado en cualquiera de las otras máquinas. Y cuando la máquina que ha fallado se recupera, los servicios son nuevamente migrados a la máquina original. Esta capacidad de recuperación automática de servicios permite garantizar la integridad de la información, ya que no hay pérdida de datos. Y además evita molestias a los usuarios, que no tienen por qué notar que se ha producido un problema.

La planeación para obtener una alta disponibilidad se centra en los sistemas de respaldo y procesamiento, almacenamiento y acceso, los cuales deben estar diseñados en forma adecuada y probados exhaustivamente, antes que los mismos se pongan en funcionamiento. Dado que una aplicación que no ha sido probada adecuadamente puede convertirse fácilmente en el eslabón más delgado del sistema y convertirse en la causal de no contar con el acceso continúo a los sistemas críticos y/o una rápida recuperación en caso de que ocurra una falla en el servidor.

4.1.- DEPENDENCIA DE LA DISPONIBILIDAD DE TECNOLOGÍA

La dependencia tecnológica es directamente proporcional al uso cotidiano que hagamos de ella. Con el desarrollo de la tecnología las opciones que ésta ofrece no son sólo las de integrar las aplicaciones de una empresa, sino que además pueden incorporarlas, para que forme parte de una cadena de valor.

Adicionalmente, todo el procesamiento puede ser en línea, en tiempo real, por lo cual esta dependencia de la tecnología no da pie a que los sistemas fallen, es decir, las empresas dependen de sus sistemas de información para poder operar, así como también dependen de los sistemas de sus proveedores para que las operaciones que hoy se efectúan en conjunto puedan fluir sin inconvenientes.

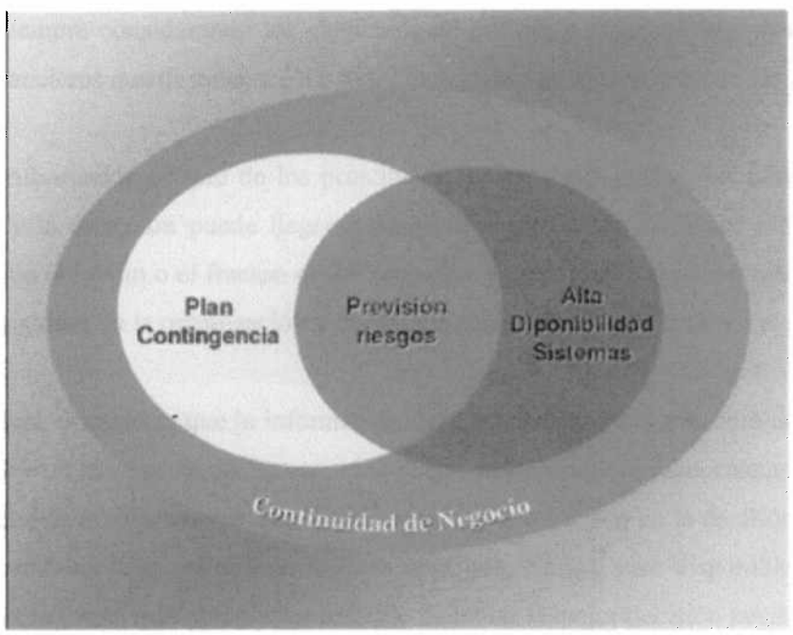
Actualmente, el ritmo de vida es más acelerado que hace unos años, por esta razón los clientes exigen una disponibilidad absoluta de los proveedores tecnológicos que en la actualidad usan para manejarse, por lo tanto, es casi indispensable que ellos funcionen en un 100%, para así desarrollar las actividades del día a día. Esto va a ser más aplicable a quienes se manejen con mayor tecnología, significando mayor dependencia de estos servicios. Lo anterior ocurre tanto en el ámbito personal como empresarial y puede afectar de distinta manera, según el tipo y forma de información que se requiera.

La dependencia tecnológica la podemos encontrar en todo tipo de empresas, por ejemplo en compañía de aviación, donde todo gira alrededor de sistemas de información, no sólo en los aviones, sino todos los procesos que son necesarios para la operación de la línea: reservas, plan de vuelo, control de combustible, etc. Es tan importante la operación de los sistemas de información, que una interrupción prolongada de los mismos puede hacer que se detenga la operación de la compañía representando pérdidas millonarias.

Lo mismo sucede en otros sectores, como la Banca, la fabricación o los servicios. En el primer caso, lo que manejan los bancos es información relacionada con el movimiento de dinero y una variada gama de procesos; en el sector de fabricación, la tecnología de información se utiliza para los procesos de producción, pero también para procesos como el de diseño, programación de producción, control de inventarios, distribución y otros; el sector de servicios hace también un uso intensivo de las TI. Por ejemplo, las compañías de electricidad, gas y otros servicios utilitarios, necesitan de sistemas para manejar sus procesos críticos, como pueden ser la mantención de la continuidad del servicio, la facturación y los cobros.

Con el constante avance de la tecnología y al existir mayor disponibilidad se depende aún más de los terceros, lo que aumenta los riesgos en la organización. Si no se tienen analizados los riesgos existentes y programados planes que puedan minimizar estos, la empresa no podría optimizar sus recursos ante eventualidades, ni tener una solución inmediata para poder corregirlas o bien minimizar el impacto que puedan tener en sus operaciones.

A la vez, todos los avances tecnológicos imponen un cambio necesario al interior de las empresas para garantizar la disponibilidad de sus servicios de información, no sólo bajo planes de recuperación de desastres, lo que normalmente se efectúa a través de un plan de contingencia, sino bajo la premisa de "no parar", desarrollado dentro del concepto de "continuidad del servicio".



Fuente página Web: http://www.swgreenhouse.com/Productos/Vision/ContNegocios.html

4.2.- IMPORTANCIA EN LA EMPRESA

Los sistemas y la tecnología de Información son de gran aporte a las empresas, teniendo en cuenta su continuo cambio y desarrollo en la actualidad. A través del uso de TI se han logrado importantes mejoras, tal como la automatización de procesos operativos, la suministración de información necesaria para la toma de decisiones y lo más importante, el logro y obtención de ventajas competitivas y/o reducción de las ventajas de los rivales.

La tecnología de información ha complementado a la empresa como herramienta para los sistemas, siendo también asociada a las comunicaciones, integración y tecnología de equipos en las organizaciones, entre otros. Pero a la vez, de ningún modo ha dejado de lado el factor humano que debe existir en la empresa para manejarse con la tecnología; tener una buena estructura, la que permita desarrollar las actividades de la organización de forma eficiente y oportuna; el equipamiento, ya sea de infraestructura, de software y hardware, siempre considerando los elementos de política y regulaciones, además de los recursos financieros que destinen a estas actividades, para la consecución de sus objetivos.

La información es uno de los principales recursos que poseen las empresas en la actualidad, y la dirección puede llegar a pensar que puede ser un factor crítico para la determinación del éxito o el fracaso de la compañía, ya que puede ser determinante para la toma de decisiones de la organización y de la continuidad que pueda tener en el tiempo.

Se debe considerar que la información debe estar disponible a la hora de tomar una determinación en la empresa, de no ser así se puede emitir opiniones incorrectas debido a la disponibilidad de la información que tenga la persona involucrada en la decisión. Por tanto, la empresa requiere que la información sea oportuna, clara y esté disponible cuando se requiera y de la forma más completa, con el fin de tomar la mejor decisión posible.

Así, las organizaciones deben considerar que la información este disponible en cualquier momento que se solicite, tanto para usuarios internos como externos que utilizan este tipo de medio.

La disponibilidad comienza a ser importante para la empresa cuando se tiene dependencia para realizar las actividades de la compañía. Al no haber disponibilidad puede provocar diversos inconvenientes en la organización, tanto para los clientes como para las personas que trabajan en ella, estos problemas pueden ser: dificultades de acceso a la información, entrega de servicios eficientes y adecuados a los clientes ó tener un tiempo de respuesta coherente para el servicio, entre otros. Esto va a depender de las necesidades específicas que tenga cada una de las organizaciones.

La disponibilidad en la empresa debe considerarse cuando se quiere cumplir sus objetivos, deseando entregar un servicio eficiente a los usuarios de ésta, pensando claramente en que el costo sea razonable respecto a los beneficios que se van a tener con la inversión entregada.

No sólo se debe considerar la disponibilidad cuando existan problemas que ya conoce la empresa (internos), sino que también se debe tomar en cuenta, por ejemplo los factores externos que puedan afectarlo, tal como: cambios climáticos, catástrofes, inundaciones, regulaciones, legislación, globales, etc., ya que si no se posee un plan de contingencia, éstos factores pueden producir inconvenientes en la entrega del servicio. La falta de un plan de contingencia que considere los diversos factores internos y externos que pueden afectar a una empresa puede ocasionar los siguientes problemas:

- Pérdida de clientes
- Pérdida de imagen
- Pérdida de ingresos por beneficios
- Pérdida de ingresos por ventas y cobros
- Pérdida de ingresos por producción
- Pérdida de competitividad
- Pérdida de credibilidad en el sector

La Pérdida de cliente e imagen, puede ocurrir por no disponer de la información necesaria en el momento que el usuario lo solicite y esto significar que por falta de disponibilidad se cambie de proveedor. Lo anterior, repercutirá en la imagen que se brinde a los clientes, dando una desfavorable impresión del servicio y arriesgándose a que los usuarios inconformes divulguen que la empresa no es confiable.

Todo lo anterior se verá reflejado en los estados financieros, debido a que la pérdida de clientes implica directamente la disminución de ingresos de la empresa.

En el peor de los casos podemos decir que se pierde la credibilidad de la compañía y al no tomar las medidas necesarias para mejorarla puede llegar a obtener pérdidas extremadamente grandes que conlleven al cierre de la empresa por los malos resultados.

En consecuencia, la disponibilidad en las empresas está estrictamente relacionada con una dependencia a la tecnología, y cada vez afecta más a las áreas de negocio, porque la tecnología mejora los servicios, pero a la vez los hace más vulnerables, sobre todo si no se toman las medidas precautorias para tener respuesta rápida ante una eventualidad.

5.- ADMINISTRACIÓN DE DISPONIBILIDAD.

La administración de disponibilidad presenta como principal objetivo asegurar que los servicios de TI funcionen correctamente y de acuerdo con los contratos establecidos con los clientes, siendo respaldada por indicadores claves, los cuales son; Disponibilidad, Fiabilidad, Mantenibilidad y Capacidad de Servicio.

A su vez esta relacionada con otros procesos de la Infraestructura de Tecnologías de la Información (ITIL), los que son; Administración del Nivel de Servicio, Administración de la Continuidad, Administración de Finanzas, Administración de Capacidad, Administración del Cambio, este tema es tratado en mayor profundidad en el capitulo 8.

ITIL, se refiere a un marco de referencia para la administración de servicios[3]; esto significa que todos los procesos tienen un gran objetivo:

- Planificar
- Entregar y Soportar los Servicios de TI

Se debe tener presente que la disponibilidad depende del correcto diseño de los servicios TI, así como también de su correcto mantenimiento y la calidad de los servicios internos y externos acordados.

Las responsabilidades de la administración de la Disponibilidad incluyen:

- Determinar en conjunto con los clientes los requisitos de disponibilidad.
- Para los servicios TI se debe garantizar el nivel de disponibilidad establecido.
- Monitorear la disponibilidad de los sistemas TI.
- Aumentar los niveles de disponibilidad, para esto se proponen mejoras en la infraestructura y servicios TI.

Al cumplir con estas responsabilidades nos vemos beneficiados en aspectos tales como: mejora en la calidad del servicio; costo de mantenimiento y tiempo de caída reducido; los recursos de TI son utilizados con mayor eficiencia; cumplimiento de los niveles de disponibilidad acordados.

(3) Artículo ITIL y la administración de servicios de TI por Judit La Guardia

Como toda actividad, la administración de la disponibilidad no esta exenta de dificultades con las que topa al momento de su realización, entre las cuales podemos mencionar: el monitoreo incorrecto de la disponibilidad real del servicio, falta de compromiso con el proceso dentro de la organización TI, herramientas de software y personal inadecuado, objetivos de disponibilidad no alineados con las necesidades de la empresa, falta de coordinación con los otros procesos, entre otras.

Actividades de Administración de la Disponibilidad

Entre las actividades a desarrollar se encuentran:

- Identificación de sistemas y servicios claves en la organización.
- Determinar los requisitos de disponibilidad reales para los sistemas y servicios del negocio.
- Desarrollar un plan de disponibilidad donde se estimen las necesidades de disponibilidad futura a corto y medio plazo.
- Realizar informes sobre la Disponibilidad TI, la que se debe monitorear y a su vez mejorarla.
- Monitorear la disponibilidad de los servicios de TI.
- Mantenimiento del servicio en operación y recuperación del mismo en caso de fallo.

La Administración de Disponibilidad es un proceso, el cual al ser utilizado inteligentemente y sistemáticamente, puede producir beneficios sin tener que recurrir a un desembolso de capital significativo, para esto hace uso de varias estrategias con el fin de maximizar la disponibilidad sin quebrar económicamente a la empresa.

Una ayuda para mantener un alto nivel de disponibilidad es el entendimiento de las siguientes características de la alta disponibilidad:

Redundancia

En fuentes de poder, múltiples procesadores, memoria segmentada y discos redundantes, con el fin de eliminar lo más que se pueda, cualquier punto único de falla que pueda interrumpir la disponibilidad del servicio.

Ejemplo: Dos servidores que funcionen en lugares diferentes, cuando uno no este disponible el otro funcione de modo que se tenga el acceso continuo a los datos cuando se realice una función crítica dentro de la empresa.

Reputación

Buscar el prestigio de los proveedores claves que entreguen seguridad, calidad y disponibilidad en el servicio.

Confiabilidad

La confiabilidad de los equipos y de los programas se puede verificar por referencias de clientes y analistas de industria. Además es siempre recomendable el monitoreo permanente a través del personal de operaciones, soporte y técnicos del proveedor, también es posible realizar benchmarking con otros departamentos de TI.

Facilidad de Reparación

En sistemas muy sofisticados, se pueden establecer centros de diagnóstico remoto que permite detectar fallas, y montar medidas que la eviten.

Restablecimiento

Este punto hace referencia a la habilidad para sobreponerse a una falla momentánea, sin que esta repercuta en la disponibilidad para el usuario final.

Ejemplo: Ante la eventualidad que haya un corte de luz, para mantener la continuidad de los servicios y que no afecte la disponibilidad de la información se deben tener medidas de contingencia como generadores de energía secundaria.

Robustez

Un proceso robusto resistirá una variedad de ataques, tanto internos como externos, que podrían fácilmente interrumpir y dañar la disponibilidad en un ambiente más débil. Esta característica requiere un alto nivel de documentación y entrenamiento para absorber cambios técnicos a las plataformas, productos, servicios y clientes; cambios de personal cuando hay rotación y expansión, y cambios en los negocios cuando hay nuevos objetivos, adquisiciones, y fusiones.

6.- BENEFICIOS DE LA ADMINISTRACION DE DISPONIBILIDAD.

La administración de la disponibilidad de información genera beneficios a la organización, dependiendo de la manera en que se encuentra alineada la estrategia principal de la empresa con las estrategias de TI, la cual debe generar un desarrollo positivo y posible de cuantificar con los objetivos principales, en una manera o estructura dinámica de la cual sea posible generar iniciativas de negocio, capaz de soportar y ayudar a la innovación en TI, de las siguientes formas:

- Los servicios de TI son administrados para la consecución de objetivos específicos de disponibilidad.
- Mejorar la calidad del servicio debido a los controles implementados.
- Existe una menor necesidad de soporte reactivo a problemas o catástrofes que pudieran ocurrir.
- El costo de mantenimiento y tiempo de caída es reducido al mínimo.
- Los recursos de TI son utilizados con mayor eficiencia.

Al efectuar una buena administración, se pueden realizar técnicas de administración estratégica, como por ejemplo Benchmarking Tecnológico, el cual utiliza la comparación en empresas de similares características que se destacan por su gran capacidad tecnológica y del que se han desarrollado ventajas comparativas. Para aplicar esta técnica al proceso de administración en tecnología se requiere identificar algunos parámetros que nos puedan servir como referencia al realizar algún tipo de comparación con la administración de la disponibilidad, esto nos lleva al ejercicio del aprendizaje, el cual puede reducir efectivamente los posibles vacíos de eficiencia, ayudando a los objetivos que persiguen las mejoras en el proceso de administración de disponibilidad.

Administración de Servicios de TI

En esta parte de la administración de la disponibilidad de servicios de TI, debe proveer de personal calificado, de procesos e infraestructuras para administrar los servicios de TI con niveles de calidad y disponibilidad altos, para lo cual se tiene que tener presente maximizar la inversión a través de la externalización de servicios de alta calidad alineados con las metas y objetivos principales de manera de mejorar la calidad para mantener un presupuesto adecuado, siendo elaborado en los tiempos adecuados y comprometidos.

Algunos de los beneficios que se pueden dar al efectuar una buena administración o gestión de servicios de TI son:

- El cumplimiento de niveles de servicios por la calidad y soporte más confiable.
- Mejoras en seguridad, velocidad, y disponibilidad del servicio por las operaciones basadas en una estructura de procesos definida.
- Disminución y control de costos por una administración y operación centralizada.
- Mayor confianza en los procesos.

7.- CÁLCULO DE LA DISPONIBILIDAD

Se refiere a la disponibilidad que se debe entregar a los usuarios, respecto al servicio prestado, es decir, si ocurre alguna eventualidad debe tener un mínimo de tiempo de pérdida de la aplicación, para que el cliente no presente mayores inconvenientes en las actividades que realiza a través de este. Al no tener planes de contingencia que puedan minimizar las eventualidades ocurridas en la entrega del servicio, los usuarios tendrán la obligación de ver otras alternativas que satisfagan sus exigencias de forma eficiente y con mayor disponibilidad frente a los requerimientos que efectúen, ya sea usuarios internos o externos.

El Cálculo de la disponibilidad se refiere a efectuar una ecuación donde a través del tiempo acordado de servicio y el de caída del servicio nos entrega un porcentaje, el cual nos indica cual es la disponibilidad a otorgar al cliente respecto al servicio que se entrega. Este porcentaje nos va a entregar el valor que la empresa debe considerar como ocioso, porque no se pueden efectuar operaciones, ya sea tanto por usuarios externos como internos, lo que provoca una pérdida de oportunidades frente a los usuarios que necesitan la información disponible en el momento indicado.

En este cuadro se muestra la fórmula a aplicar para obtener el porcentaje de disponibilidad:

Cálculo de la Disponibilidad

$$\%\ \text{Disponibilidad} = \frac{\text{TAS} - \text{TC}}{\text{TAS}} \times 100$$

$$\text{TAS} - \text{TC} = (40 - 1)/40 \times 100$$

$$= 97.5\%$$

TAS = Tiempo Acordado de Servicio
TC = Tiempo de caída durante el TAS

Tiempo Promedio de Parada (Downtime)

Tiempo promedio de duración de una interrupción de servicio, e incluye el tiempo de detección, respuesta y resolución.

Tiempo Medio entre fallos (Uptime)

Tiempo medio durante el cual el servicio está disponible sin interrupciones.

Tiempo Medio entre incidentes

Es el tiempo medio transcurrido entre incidentes que es igual a la suma del tiempo medio de de parada y el tiempo medio entre fallos.

Esta información es necesaria para ayudar a formular los objetivos de disponibilidad de los componentes de TI y los servicios, además este cálculo puede utilizarse como entrada de cualquier herramienta para modelar la disponibilidad. Cuando se realicen negociaciones para definir objetivos de disponibilidad con los usuarios, es necesario hacerlos conciente de las implicaciones técnicas y económicas que esta tiene.

Para entregar los niveles de disponibilidad requerida para un servicio de TI, es necesario enfocarse en todos los componentes de la infraestructura de TI diseñados para apoyar el servicio. La disponibilidad de cada componente influye en la disponibilidad total que proporciona la infraestructura.

Por ejemplo, si el servicio es **24/7** y en el último mes el sistema ha estado caído durante 4 horas por tareas de mantenimiento la disponibilidad real del servicio fue:

$$\% \text{ Disponibilidad} = \frac{(720 - 4)}{720} \cdot 100 = 99{,}4\ \%$$

En el ejemplo se puede determinar cuanto es el porcentaje de disponibilidad ante una falla del servicio de 4 horas, sobre 720 hrs. que corresponde al servicio total.

En respuesta a esto tenemos un resultado de 99,4% de Disponibilidad, el que va a depender mucho de la empresa en que nos encontremos, si el porcentaje de disponibilidad es aceptable o no, de acuerdo a los objetivos y servicios que entregue a los clientes y necesidades que los usuarios (internos o externos) soliciten a la organización.

Podemos mencionar que las fallas en el servicio son un dolor de cabeza para las organizaciones, ya que estas provocan inconvenientes en la disponibilidad de los servicios.

Cabe destacar los diferentes tipos de fallas:

- **Totales:** Son aquellas que causan incapacidad total del equipo.
- **Parciales:** Son definidas como tales, aquellas que causan la degradación del servicio pero no incapacitan el funcionamiento total del equipo.
- **Súbitas:** Son aquellas que ocurren instantáneamente.
- **Progresivas:** Es cuando el equipo presenta síntomas y por lo que la falla se presenta gradualmente.

Disponibilidad Inherente (%DI)

Representa el porcentaje del tiempo que un equipo está en condiciones de operar durante un período de análisis, teniendo en cuenta solo los paros no programados. El objetivo de este indicador es medir la disponibilidad Inherente de los equipos, con la finalidad de incrementarla, ya que en la medida que esto ocurra, significará que se disminuye el tiempo de los paros por falla o paros no programados del equipo.

Disponibilidad Operacional (%DO)

Representa el porcentaje de tiempo que el equipo quedó a disponibilidad del área de operación para desempeñar su función en un período de análisis.

Teniendo en cuenta el tiempo que el equipo está fuera de operación por paros programados y no programados. El objetivo de este indicador es medir el desempeño de los equipos y la eficiencia en la gestión de mantenimiento, de manera conjunta, comparándolos contra los objetivos y metas del negocio, con la finalidad que operación tenga cada vez más tiempo el equipo disponible y que éste pueda realizar la función para la que fue diseñado.

Alrededor de un 40 por ciento del tiempo de inactividad de las aplicaciones se debe a una comprobación inadecuada, a una administración de cambios deficiente y a la ausencia de un control continuo de los errores. Otro 40 por ciento se debe a errores operativos producidos por la ausencia de procedimientos rigurosos y a errores de copia de seguridad y/o restauración. La confiabilidad del hardware ha mejorado durante los últimos años que menos del 10 por ciento del tiempo de inactividad se debe a problemas de hardware. El 10 por ciento restante del tiempo de inactividad se debe a problemas de entorno y a problemas de otro tipo.

En términos generales, se puede decir que la disponibilidad es una medida de la frecuencia con la que se puede utilizar la aplicación. Para ser más exactos, la disponibilidad es un cálculo porcentual del tiempo en que la aplicación está realmente disponible para controlar las solicitudes de servicio en comparación con el tiempo de ejecución total disponible previsto. El cálculo formal de la disponibilidad incluye el tiempo de reparación, ya que una aplicación que se está reparando no está disponible.

7.1.- EJEMPLOS DE CÁLCULO DE DISPONIBILIDAD

Ejemplo para fecha de disponibilidad:

Se ha introducido un plazo de entrega previsto de 3 días y un tiempo para tratamiento de entradas de mercancías de 2 días. El período 1 del calendario de planificación empieza el martes 01/03 y dura hasta el lunes 14/03; el período 2 del calendario de planificación empieza el martes 15/03 y dura hasta el lunes 28/03. Esto significa que la entrega se realiza los martes cada dos semanas. El plazo de entrega previsto significa que se deberá informar al proveedor de la cantidad necesaria por lo menos 3 días antes de la fecha de entrega.

Durante el primer período, se planifican dos necesidades:
Necesidad 1, de 100 piezas, el día 03/03.
Necesidad 2, de 70 piezas, el día 08/03.
Durante el segundo período, también se han planificado dos necesidades:
Necesidad 1, de 150 piezas, el día 14/03.
Necesidad 2, de 90 piezas, el día 16/03.

Según la lógica anterior (para establecer la fecha de disponibilidad = inicio del período), el sistema agrupa todas las necesidades en el período 1 y crea una propuesta de pedido para el inicio del período, es decir para el 01/03. La fecha de disponibilidad de esta propuesta de pedido es el 01/03, según la interpretación anterior de las fechas extremas del período. A partir de aquí, el sistema programa hacia atrás, es decir, se resta el tiempo para tratamiento de entradas de mercancías, resultando una fecha de entrega el 28/02. A continuación, el sistema resta el plazo de entrega previsto de tres días, lo que resulta en una fecha de liberación del 24/02. Las necesidades se agrupan entre las fechas extremas del período dando como resultado un lote de 170 piezas para el 01/03 y otro lote de 240 piezas para el 15/03.

Ejemplo de fecha de entrega:

La siguiente situación es el resultado del ejemplo anterior: la fecha de entrega del primer período es el 01/03 y la fecha de entrega del segundo período es el 15/03. Esto quiere decir que, incluyendo el tiempo para tratamiento de entradas de mercancías, la necesidad el día 15/03 no puede ser cubierta completamente porque la fecha de disponibilidad de la propuesta de pedido en el segundo período es el 17/03. Por tanto, la necesidad del 15/03 se debe añadir al lote por períodos con la fecha de entrega 01/03. Así, para el primer período, se agrupan tres necesidades: la necesidad del día 03/03, la del día 08/03, y la del 15/03 por un total de 320 piezas. La propuesta de pedido del 15/03 se crea para 90 piezas.

8.-RELACIÓN DEL PROCESO DE ADMINISTRACIÓN DE DISPONIBILIDAD CON OTROS PROCESOS

Existe una estrecha relación entre la administración de disponibilidad y otros procesos de TI, ya que el objeto es que los planes de disponibilidad se ajusten a las necesidades reales del negocio.

Para cumplir con lo expuesto anteriormente se debe disponer de toda la información necesaria sobre la infraestructura de la tecnología de Información, interrupciones del servicio y estrategias de uso. Es por esto que la administración de disponibilidad mantiene una adecuada relación con otros servicios de TI, como lo es con el caso de la gestión de niveles de servicio, donde una administración adecuada de la disponibilidad facilitará el cumplimiento de los niveles de servicios acordados con los clientes en los acuerdos de nivel de servicio (SLA). Asimismo, la administración de la disponibilidad cooperará con la administración de la continuidad para garantizar la continuidad de los procesos de negocio críticos en caso de desastre. Por lo que respecta a la administración de la capacidad, la administración de la disponibilidad proporcionará una información muy útil para elaborar el Plan de Capacidad. Por último, la administración de la disponibilidad advertirá a la gestión financiera acerca del costo de la indisponibilidad.

Ampliando lo mencionado se analiza en mayor detalle como la administración de disponibilidad se relaciona con otros procesos de Infraestructura de Tecnologías de la Información (ITIL).

Administración del Nivel de Servicio:

Una entrada de la administración de disponibilidad al nivel de servicio es una evaluación de la disponibilidad que puede ser entregada para un nuevo servicio de TI y negociar el acuerdo, una salida de la administración del nivel de servicio a la administración de disponibilidad es el detalle de los acuerdos que habilitan la medición correcta de la disponibilidad, así como de los reportes.

Administración de la Continuidad:

La evaluación detallada del impacto en las funciones vitales del negocio depende de la disponibilidad de la infraestructura. Otra relación es el criterio de diseño de la recuperación y la disponibilidad para mantener el negocio en operación, previniendo o minimizando el impacto de fallas mediante el uso de CFIA (evaluación de impacto de falla en un componente).

Administración de Capacidad:

Administración de disponibilidad le proporciona una completa evaluación del impacto en componentes de infraestructura para nuevos servicios de TI definiendo donde se aplicarán técnicas de disponibilidad para proporcionar resistencia a fallas. Por su parte entrega el plan de capacidades detallando la capacidad que se requiere asociada a la provisión de infraestructura adicional.

¿Porque utilizar ITIL para la administración de servicio?

Porque brinda un conjunto detallado de mejores prácticas, consistente y coherente con un enfoque hacia la administración de los procesos de TI y además promueve un enfoque de calidad para alcanzar la eficacia y eficiencia en el uso de los sistemas de información para el negocio.

9.- ROLES Y RESPONSABILIDADES [4]

Deben existir encargados de mantener la administración de la disponibilidad, los cuales tienen ciertos roles y responsabilidades que cumplir para lograr los objetivos del cargo, de los cuales se mencionarán a continuación:

Rol de Administrador de Sistema

Responsables de resolver incidentes sobre los sistemas de información y sus datos, sus responsabilidades son:

- Solucionar incidentes y problemas reportados sobre los sistemas de información.
- Mantener las aplicaciones al día y con su última versión vigente.
- Mantener el uso de espacios en discos de la aplicación.
- Monitorear la capacidad y disponibilidad de las aplicaciones y de la infraestructura.
- Configuración de reglas de acceso y parámetros propios de las aplicaciones.
- Verificar dependencias entre los procesos de los sistemas informáticos.

Este cargo es importante ya que debe mantener los sistemas de información y con esto cumplir con la disponibilidad que solicitan los usuarios.

Rol de Backup & Restore

Es responsable de realizar y custodiar los respaldos de información de los sistemas de información. En caso de ser necesario es responsable de la restauración de la información.

Sus actividades principales son:

- Asegurar el cumplimiento de la política de respaldos.
- Verificar la efectividad de los respaldos efectuados.
- Custodiar los medios magnéticos utilizados para los respaldos. (Cintas y Cartriges).
- Mantener un inventario de los medios magnéticos y de su respectivo contenido:
  - Archivos almacenados.
  - Fecha de vigencia (Fecha de Proceso).
  - Fecha de expiración

(4) Apunte Profesor Miguel Ángel Elizondo TIA

10.- RIESGOS EN TI

El crecimiento acelerado de las tecnologías de la información (TI), han originado creciente número de oportunidades así como un creciente número de amenazas.

Hoy en día existe un alto nivel de inversión en tecnologías, lo que genera un efecto multiplicador importante en caso que dichas amenazas se materialicen, dado que las pérdidas probables se ven incrementadas en la misma proporción al aumento de la inversión.

Definición de riesgo

Riesgo se puede definir como aquella eventualidad que imposibilita el cumplimiento de un objetivo. De manera cuantitativa el riesgo es una medida de las probabilidades de incumplimientos o demasía del objetivo planeado. Lo que lleva a dos tipos de consecuencias: ganancias o pérdidas. (5)

Generalmente en lo que se refiere a tecnología de riesgo se plantea solamente como una amenaza.

Otra definición de Riesgo

Es una combinación de un evento fuera de lo normal, y las consecuencias de tal evento sobre los activos, las personas, el entorno, la institución, sus sistemas o su información. (6)

Incertidumbre: El acontecimiento que caracteriza al riesgo puede o no puede ocurrir.

Pérdida: Si el riesgo se convierte en una realidad, ocurrirán consecuencias no deseadas o pérdidas.

Cuando se analizan los riesgos es importante cuantificar el nivel de incertidumbre (a menor incertidumbre mayor posibilidad de mitigar el riesgo) y el grado de pérdidas asociado con cada riesgo.

(5) Apunte Introducción a Riesgo Informático Leonardo Sena y Simón Tenzer 2004

(6) Apunte seminario N° 56 profesor Max Wachholtz A.

10.1.- FUENTES DE RIESGO [7]

ADMINISTRACIÓN

Falta de estrategia
Debilidad
Visión
Falta de información de decisiones

PERSONAS

Error humano, falta honestidad
Capacidades y competencia
Estructuras organizacionales
Motivación
Incentivos inapropiados

PROCESOS

Excesivo Volumen/Capacidad reducida
Marco de control débil

Ineficiencias y errores de procesos
Eventos inusuales

SISTEMA TRANSACCIONES

Baja inversión en Sistemas
Deficiente Integridad, seguridad y exactitud
Datos Inconsistentes
Interfaces manuales

FUENTES EXTERNAS

Desastres naturales
Terceros
Entorno de Negocios
Cambios a Legislación y Regulaciones

NUEVAS ACTIVIDADES

Cambios a la estrategia
Reingeniería e integración
Nuevos productos
Aumento de la sofisticación

NORMAS, LEYES, REGULACIONES

Contratos
Poderes
Responsabilidades

Tipos de Negocio
Interlocutores
Globalización

(7) Apunte seminario N° 56 profesor Max Wachholtz A.

10.2.- VULNERABILIDADES, AMENAZAS Y CONTRAMEDIDAS

Hay tres conceptos involucrados cuando se habla de la seguridad de un sistema informático.

1.- Vulnerabilidad

Punto o aspecto del sistema que es susceptible de ser atacado dañando la seguridad del mismo. Representan las debilidades o aspectos falibles o atacables, inseguros en el sistema informático.

La seguridad es la facultad de estar cubierto ante algún riesgo o amenaza. Desde este punto de vista la seguridad total es muy difícil de lograr, ya que implicaría identificar y describir todos los riesgos y amenazas a que puede verse expuesto el sistema. Lo que se manifiesta en los sistemas es la inseguridad o vulnerabilidad. Siendo imposible hablar de un sistema informático totalmente seguro, ya que el uso de la tecnología hace vulnerable al sistema en forma inherente.

2.-Amenazas

Una amenaza se define como un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus servicios.

A la hora de analizar los riesgos hay que evaluar las distintas amenazas que pueden provenir de las más diversas fuentes. Entre éstas se incluyen las agresiones humanas entre las que tenemos; malintencionados, que pueden deberse a personal interno o externo; o no intencionadas, y los desastres naturales.

Dependiendo de la organización y el proceso analizado, serán aplicables distintos tipos de amenazas. Las amenazas tendrán una probabilidad de ocurrencia que dependerá de la existencia de una vulnerabilidad que pueda ser explotada, para materializarse en un incidente.

Ejemplos de Amenazas, Vulnerabilidades y Riesgos Asociados a la Disponibilidad

Una vulnerabilidad común es contar con antivirus no actualizados, lo cual permitirá al virus actuar y ocasionar daños. Si el antivirus estuviese actualizado la amenaza (virus) si bien potencialmente seguiría existiendo no podría materializarse.

La consecuencia al no estar protegidos frente al ataque del virus es la pérdida de información, mal funcionamiento del software, pérdidas de equipos que afectarían la disponibilidad de la información de usuarios internos y externos.

Naturales

Se refiere al grado en que el sistema puede verse afectado por desastres naturales o ambientales que pueden dañar al sistema, tales como el fuego, inundaciones, rayos, terremotos, o quizás más comúnmente, fallos eléctricos o picos de potencia. Además están el polvo, la humedad o la temperatura excesiva son aspectos a tener en cuenta.

Ejemplo:
Amenaza, si ocurriera un terremoto en el lugar que se encuentran las instalaciones de la empresa.
Vulnerabilidad, no contáramos con centros de cómputos duplicados.
Riesgo Asociado, pérdida de la infraestructura física, además de toda la información crítica que utiliza la entidad, lo que provocaría no poder mantener la disponibilidad de la información y con esto la continuidad de las operaciones de la empresa.

Hardware y del Software

Se refiere a la posibilidad de robar o dañar los discos, cintas, listados de impresoras, etc.

Desde el punto de vista del hardware, algunos dispositivos pueden ser más vulnerables que otros, por lo tanto ciertos sistemas requieren la posesión de algún tipo de herramienta o tarjeta para poder acceder a los sistemas.

Ejemplo:
Amenaza, robos y daños de dispositivos de respaldo.
Vulnerabilidad, no contar con medidas de protección de acceso a la empresa.
Riesgo Asociado, pérdida de respaldos almacenados en cintas, discos, etc., lo que afectaría a la disponibilidad.

Desde el punto de vista del software ciertos fallos o debilidades del sistema hacen más fácil acceder al mismo y lo hacen menos fiable. En este tema se incluyen todos los bugs en los sistemas operativos, u otros tipos de aplicaciones que permiten atacarlos.

Ejemplo:
Amenazas, uso de software por personal no autorizado.
Vulnerabilidad, política de seguridad de información inadecuada.
Riesgo Asociado, mal uso de información confidencial, modificaciones, eliminación, de la información, lo que produce pérdida de fiabilidad e ineficiencia de disponibilidad de la información.

3.- Contramedida

Técnicas de protección del sistema contra las amenazas.

La seguridad informática se encarga de la identificación de las vulnerabilidades del sistema y del establecimiento de contramedidas que eviten que las distintas amenazas posibles exploten dichas vulnerabilidades. Una máxima de la seguridad informática es que: "No existe ningún sistema completamente seguro". Existen sistemas más o menos seguros, y más o menos vulnerables, pero la seguridad nunca es absoluta.

Tipos de medidas de seguridad o Contramedidas

Diseñar sistemas mediante criterios de seguridad es complejo, pues las amenazas son en muchos casos poco cuantificables y muy variados. La aplicación de medidas para proteger el sistema implica un análisis y cuantificación previa de los riesgos o vulnerabilidades del sistema. La definición de una política de seguridad y su implementación es a través de una serie de medidas.

Las medidas de seguridad que pueden establecerse en un sistema informático son de cuatro tipos fundamentales:
Físicas, lógicas, administrativas y legales.

Medidas Físicas

Aplican mecanismos para impedir el acceso directo o físico no autorizado al sistema. También protegen al sistema de desastres naturales o condiciones medioambientales adversas. Se trata fundamentalmente de establecer un perímetro de seguridad en nuestro sistema.

Existen tres factores fundamentales a considerar:

1.- El acceso físico al sistema por parte de personas no autorizadas.

2.- Los daños físicos por parte de agentes nocivos o contingencias.

3.- Las medidas de recuperación en caso de fallo.

Concretando algo más los tipos de controles que se pueden establecer, estos incluyen:

- Control de las condiciones medioambientales (temperatura, humedad, polvo, etc.)

Relación con disponibilidad

Esta medida permite mantener el correcto funcionamiento de hardware y software, lo que conlleva al resguardo de información para que esta pueda estar disponible a los usuarios.

- Prevención de catástrofes (incendios, tormentas, cortes de fluido eléctrico, sobrecargas, etc.)

Relación con disponibilidad

Permite la continuidad del servicio frente a eventualidades, como por ejemplo ante un corte de electricidad, su contramedida es tener un generador que permita mantener la disponibilidad de información.

- Sistemas de recuperación (copias de seguridad, redundancia, sistemas alternativos geográficamente separados y protegidos, etc.)

Relación con disponibilidad

Permiten garantizar la disponibilidad al contar con copias de seguridad. A más criticidad de la información, los respaldos se realizarán con mayor periodicidad.

Medidas Lógicas

Incluye las medidas de acceso a los recursos, información y al uso correcto de los mismos, así como a la distribución de las responsabilidades entre los usuarios. Se refiere más a la protección de la información almacenada.

Entre los tipos de controles lógicos que es posible incluir en una política de seguridad podemos destacar los siguientes:

- Uso de la criptografía para proteger los datos y las comunicaciones.

Relación con disponibilidad

Permite obtener una alta disponibilidad de información fiable y mantener su confidencialidad.

- Uso de cortafuegos (Firewall) para proteger una red local de Internet.

Relación con disponibilidad

Permite mantener protegida la información ante ataques de virus los que la dañarían y provocarían que disminuyera la disponibilidad de ésta.

Otras medidas de acción frente a problemas de disponibilidad

Backups

Obtención y almacenamiento de los respaldos de información.

En una empresa para realizar Backups se deben establecer procedimientos para la obtención de copias de seguridad de todos los elementos de software necesarios para mantener la correcta ejecución de los sistemas o aplicaciones. Por lo cual debe contar con:

Backups del Sistema Operativo

En caso de tener varios Sistemas Operativos o versiones, se debe contar con una copia de cada uno de ellos.

Ejemplo: una empresa que manejaba DOS debe tener versiones que permitan recuperar la información que tenían en dichos sistemas, además de contar con el respaldo del sistema que se tiene en la actualidad.

Backups del Software Aplicativo

Considerando tanto los programas fuentes, como los programas objetos correspondientes, y cualquier otro software o procedimiento que también trabaje con la data, para producir los resultados con los cuales trabaja el usuario final. Se debe considerar también las copias de los listados fuentes de los programas definitivos, para casos de problemas.

Dejar respaldos del programa fuente en caso de posteriores modificaciones y actualizaciones.

Ejemplo: Cambio de personal, correspondiente al área de TI, frente a esta eventualidad la empresa debe contar con el respaldo del programa fuente para que el nuevo personal pueda efectuar las actualizaciones, mantener el servicio y continuar con las operaciones.

Backups de los Datos

Bases de Datos, Índices, tablas de validación, passwords, y todo archivo necesario para la correcta ejecución del Software Aplicativo.

Ejemplo: la realización de copias desde respaldos de información, las cuales son guardadas en distintos espacios físicos, con una identificación clara, para que al momento de solicitar el respaldo efectuado este pueda ser utilizado y rápidamente encontrado.

Backups del Hardware

Se puede implementar bajo dos modalidades:

Modalidad Externa

Mediante convenio con otra organización que tenga equipos similares o mayores y que brinden la seguridad de poder procesar nuestra Información, y ser puestos a nuestra disposición, al ocurrir una contingencia y mientras se busca una solución definitiva al siniestro producido. Este tipo de convenios debe tener tanto las consideraciones de equipamiento como de ambientes y facilidades de trabajo que cada organización se compromete a brindar, y debe de ser actualizado cada vez que se efectúen cambios importantes de sistemas que afecten a cualquiera de las organizaciones.

Modalidad Interna

Si tenemos más de un local, en ambos debemos tener señalados los equipos, que por sus características técnicas y capacidades, son susceptibles de ser usados como equipos de emergencia del otro local, debiéndose poner por escrito (igual que en el caso externo), todas las actividades a realizar y los compromisos asumidos.

En ambos casos se deberá probar y asegurar que los procesos de restauración de Información posibiliten el funcionamiento adecuado de los Sistemas. En algunos casos puede ser necesario volver a recompilar nuestro software aplicativo bajo plataformas diferentes a la original, por lo que es imprescindible contar con los programas fuentes, al mismo grado de actualización que los programas objeto.

Políticas (Normas y Procedimientos de Backups)

Se debe establecer los procedimientos, normas, y determinación de responsabilidades en la obtención de los Backups mencionados anteriormente, debiéndose incluir:

- Periodicidad de cada Tipo de Backup.

Es importante tener respaldos de los procesos críticos, porque es necesario para la continuidad de la empresa, como las transacciones diarias bancarias, que son efectuadas durante un proceso nocturno, para que al día siguiente se encuentre disponible la información para todos los usuarios.

- Respaldo de Información de movimiento entre los períodos que no se sacan Backups (backups incrementales). Haciendo una copia de resguardo con todos aquellos archivos que hayan sido modificados desde el último backup.

- Almacenamiento de los Backups en condiciones ambientales óptimas, dependiendo del medio magnético empleado. Los resguardos que se realicen con la información deben estar protegidos para que al utilizarlos estén en condiciones óptimas para rescatar la información.

- Reemplazo de los Backups, en forma periódica, antes que el medio magnético de soporte se pueda deteriorar (reciclaje o refresco). Estar en constante alerta de que los dispositivos de respaldo estén en óptimas condiciones para que en el futuro se encuentren disponibles para su uso.
- Almacenamiento de los Backups en locales diferentes donde reside la información primaria (evitando la pérdida si el desastre alcanzo todo el edificio o local).

- Pruebas periódicas de los Backups (Restore), verificando su funcionalidad, a través de los sistemas, comparando contra resultados anteriores confiables.

Contramedidas frente al OUTSOURCING

El incremento en la utilización de nuevas tecnologías, así como el uso cada vez mayor de nuevos aparatos y más sofisticados ha hecho que muchas empresas se vean incapaces de gestionar de manera correcta sus recursos informáticos. Y es que, además de saber gestionarlos de forma adecuada, el mantenimiento de los equipos y de la infraestructura informática implica, en numerosas ocasiones un elevado costo que las compañías son incapaces de asumir.

Así, la opción pasa por los servicios: es decir, que empresas expertas, conocedoras de las máquinas, los programas y las redes gestionen todo esta estructura de forma correcta y a un costo apropiado.

En la actualidad, es común contratar a un proveedor para que proporcione apoyo a las actividades de negocio, ya que al ser especialistas entregan mayor calidad de servicio y permite reducir costos que realizándolas internamente.

Puede ser outsourcing selectivo, en el que se cede a un proveedor un área o proceso determinado, u outsourcing global, en el que la compañía externaliza la totalidad de sus funciones tecnológicas.

Al contratar Outsourcing se deben considerar los siguientes aspectos:

Monitorear a sus proveedores externos

Si las funciones TI de una empresa se encuentran a cargo de proveedores externos, debe controlar el servicio ofrecido por sus proveedores para obtener una disponibilidad óptima del servicio que nos entregan.

Para reducir los riesgos de seguridad asociados con el outsourcing, se sugieren las siguientes indicaciones:

- Buscar proveedores externos dueños de una certificación SAS 70 o ISO 27001, que prueba de manera independiente que operan con los controles de seguridad adecuados y aseguren la disponibilidad.

- Trabajar con proveedores dedicados a empresas grandes y medianas, que cuentan con los recursos suficientes para auditar a los proveedores de manera cuidadosa, debido a que los pequeños proveedores tienen limitaciones en este aspecto.

Opiniones de Outsourcing respecto a la Disponibilidad

- Para Rosa Cruz, directora comercial de Servicios de Sun Microsystems "la disponibilidad de los datos y las aplicaciones es hoy, el verdadero activo crítico de los negocios. Más cuando hablamos de compañías con grandes entornos informáticos en las que es necesaria una gestión de datos que cubra todo el ciclo de vida de la información, eliminando la complejidad de los sistemas y garantizando la disponibilidad de los mismos. Cualquier compañía que trabaje con sistemas de información debe prestar especial atención a la seguridad y total disponibilidad de todas sus plataformas: desde servidores pequeños hasta grandes centros de datos con completos entramados de software, pasando por áreas tan críticas como la Gestión de Identidad o la securización de los sistemas".

- IBM, "es necesario definir y acordar niveles de servicio (SLAs), que se acuerdan conjuntamente entre el cliente y el proveedor y establecen indicadores y objetivos de calidad que se controlan con métricas auditables.

Son el mecanismo que permite controlar el servicio y conocer si éste se ajusta a los objetivos firmados en el contrato. Es importante que los SLAs estén bien definidos a través de los indicadores y objetivos, y que éstos sean cuantificables y fáciles de medir. Adicionalmente se establece un proceso de revisión periódica con el fin de mejorar el servicio y adaptarlo a la evolución de las necesidades del negocio".

10.3.- GESTIÓN DE RIESGO DE DISPONIBILIDAD

Riesgo de Disponibilidad

Los Riesgos se asocian con la interrupción de los sistemas a corto plazo donde las técnicas de restitución/recuperación se pueden utilizar para minimizar el alcance de la interrupción. También son asociados con desastres que causan interrupciones en el procesamiento de la información a largo plazo y que se centran en controles como backups y planes de contingencia.

La capacidad de la empresa para continuar con sus operaciones y procesos críticos puede depender en gran medida de la disponibilidad de determinados sistemas de información. Si no se dispusiera de sistemas críticos o importantes por un período prolongado, la compañía experimentaría dificultades para continuar con sus operaciones, ya que si estos no están disponibles para dar soporte a determinadas operaciones pueden provocar pérdidas de ingresos, flujos de cajas y rentabilidad, pérdidas de ventajas competitivas, insatisfacción de clientes y pérdida de participación de mercado, problemas de imagen, incremento de costos e incluso multas y sanciones.

Aspectos a considerar en la gestión del riesgo.

- Identificación del Sistema o Proceso
- Identificación de las Amenazas
- Identificación de las Vulnerabilidades
- Controles
- Determinar la Probabilidad de ocurrencia
- Análisis de Impacto
- Determinación del Riesgo
- Recomendación de Controles
- Documentar los Resultados

Los bancos se enfrentan al riesgo de que los sistemas que eligen no estén bien diseñados o ejecutados.

Por ejemplo, un banco se expone al riesgo de una interrupción o retraso de sus sistemas cuando el sistema de banca electrónica o dinero electrónico que escoge es incompatible con las exigencias de sus usuarios.

Un proceso de gestión de riesgo se puede resumir en los siguientes tres elementos básicos de evaluación de riesgos, control de riesgos y seguimiento de riesgos lo que ayudará a los bancos y a los supervisores en el logro de estos objetivos. Los bancos pueden

emplear un proceso de este tipo al comprometerse con nuevas actividades de banca electrónica y dinero electrónico y al evaluar los compromisos ya existentes.

Como los bancos deben tener medidas, ya sea de control y mitigación de riesgo operativo esto va a estar directamente relacionado al impacto en el capital, siendo la inversiones de infraestructura de TI una parte importante de este, creando protección financiera y proveyendo de confianza a los inversionistas.

Mitigar los Riesgos

La metodología a implementar debe considerar opciones de mitigación de los riesgos:

- **Prevención**: Implementación de Controles, Tecnológicos, administrativos y operacionales
- **Transferencia de los riesgos**: seguros
- **Eludir**: Cambiando la forma de hacer las cosas
- **Aceptar**: Vivir con el riesgo

11.- PLAN DE CONTINUIDAD Y PLANES DE CONTINGENCIA, SU RELACION CON LA DISPONIBILIDAD

En la actualidad una serie de amenazas se ciernen en torno a las organizaciones, estas se encuentran expuestas a diferentes contingencias tanto internas como externas que atentan con la operatividad del día a día y podrían ocasionar grandes pérdidas. Ejemplos de estas amenazas son variados y van desde el simple virus hasta la catástrofe natural de las cuales podemos mencionar; cortes de electricidad, fenómenos meteorológicos, huelgas laborales, situaciones de orden político terrorismo, incendios, terremotos, entre otras. La continuidad del negocio es fundamental y por lo cual las empresas necesitan garantizar su operación por encima de cualquier contingencia y para eso la información crítica del negocio es indispensable.

El ambiente de negocios en que se desenvuelven las organizaciones hoy en día es cada vez más competitivo, por lo que es fundamental que puedan proporcionar niveles de servicios efectivos todo el tiempo. Deben desarrollar la habilidad de continuar proporcionando un predeterminado y acordado nivel de servicio para soportar los requerimientos mínimos del negocio luego de una interrupción o un desastre. La idea primordial es contar con un conjunto de procedimientos de acción que les permita estar preparadas para afrontar desastres informáticos, minimizando los efectos que estos tienen sobre el desempeño del negocio, aumentando las posibilidades de supervivencia de la empresa.

Es imprescindible que las organizaciones puedan preparase para enfrentar de la mejor manera posible una desgracia, para esto deben entender que no son inmunes a ningún siniestro y enfocar su atención en como estos acontecimientos afectan a su negocio, en cuanto tiempo su negocio volverá a funcionar, como los afectaría y que harían para mitigar o solventar esa situación. Una herramienta de ayuda en este sentido es el **"Plan de Continuidad de negocios" y "Plan de Contingencia"**

11.1.- Plan de Continuidad de Negocio

Continuidad de Negocio

Para continuar con el desarrollo de este tema es necesario saber que la Continuidad de Negocio engloba todo lo relacionado con los esfuerzos de las empresas de operar armónicamente en cualquier circunstancia. Lo anterior incluye otras dos categorías que son; recuperación de desastres y alta disponibilidad de sistemas.

La Recuperación de desastres, significa superar las contingencias que se puedan producir, independientemente de su origen. Un plan de recuperación tiene por objetivo proporcionar a la empresa los medios alternos para realizar sus funciones normales, cuando los medios habituales no están disponibles debido a una contingencia. Abarca por tanto mucho más que los sistemas informáticos, se necesitan también otros elementos como archivos, puestos de trabajo, teléfonos, faxes y muchos otros elementos.

La alta disponibilidad puede cubrir, dentro de un plan de recuperación los de Sistemas de Información Electrónica, así como también, los paros de sistemas que no son causados por contingencias, sino por la propia dinámica de los sistemas, que se suelen llamar "paros planificados". Entre ellos contamos los causados por copias de seguridad, mantenimientos o cambios de versión de sistemas operativos o del software aplicativo.

Plan de Continuidad de Negocios,

El Plan de Continuidad de Negocios es una herramienta que permite prevenir o evitar los posibles escenarios originados por una situación de crisis, minimizando las consecuencias económicas, de reputación o de responsabilidad civil. Además señala las acciones a adoptar en caso que los riesgos se materialicen. Ayuda a reducir los costos asociados a la interrupción al evitar penalizaciones contractuales por incumplimiento de contratos como proveedor de productos o servicios. Asimismo, permite determinar de antemano qué información es crítica y cómo debe salvaguardarse. Recuperando los Procesos Críticos del Negocio, en el menor tiempo posible, de acuerdo al análisis de riesgo y los recursos destinados por la compañía.

11.1.1.- OBJETIVOS Y BENEFICIOS PRINCIPALES:

Los objetivos principales del Plan de Continuidad los podemos resumir en:

- Garantizar la pronta recuperación de los servicios (críticos) tras un desastre.
- Establecer políticas y procedimientos que eviten, en la medida de lo posible, las perniciosas consecuencias de un desastre o causa de fuerza mayor.

Entre los beneficios que otorga la implementación de un Plan de Continuidad de Negocios encontramos el ahorro de tiempo y dinero para afrontar los desastres, interrupciones y contingencia, además de la imagen y revalorización de la confianza en la empresa por parte de los accionistas, inversores, empleados, proveedores y clientes al mostrarles que se toman medidas diarias para garantizar la continuidad del negocio.

11.1.2.- FASES DE UN PLAN DE CONTINUIDAD

La elaboración de un Plan de continuidad de negocios consta de cinco etapas las cuales se describen a continuación:

- **Gestión e iniciación del proyecto:** Establece un equipo para el proyecto y una estrategia para desarrollar el plan.
- **Análisis de impacto sobre el negocio (AIN):** Identifica los aspectos críticos relacionadas con el máximo tiempo en que un proceso puede estar no disponible.
- **Estrategia de recuperación:** Identifica y selecciona las apropiadas alternativas de recuperación para lograr los tiempos requeridos definidos en el AIN.
- **Diseño del plan y desarrollo:** Se trata en esta fase de documentar las estrategias de recuperación
- **Prueba, Mantenimiento, y entrenamiento:** La idea es esta fase es probar las estrategias de recuperación anteriormente definidas, manteniendo actualizado el plan y dándolo a conocer a todos los empleados.

Estrategia de Recuperación

Una vez que tenemos los resultados del análisis de impactos sobre el negocio, en donde se obtuvo un entendimiento de los procesos de éste, lo usamos como base para realizar la estrategia de recuperación, la cual es una combinación de medidas preventivas y correctivas, cuyo objetivo es de minimizar el impacto ante una posible interrupción o desastre.

Para el desarrollo de la estrategia de recuperación se debe tener en cuenta algunos aspectos tales como: costo, recursos humanos necesarios, tiempo requerido para la implementación y recuperación, la decisión de su desarrollo dependerá de los análisis realizados con anterioridad en la fase del AIN.

En líneas generales podemos mencionar las siguientes opciones de recuperación del servicio:

"Cold Standby" requiere un emplazamiento alternativo en el que podamos reproducir en pocos días nuestro entorno de producción y servicio. Esta opción es la adecuada si los planes de recuperación estiman que la organización puede mantener sus niveles de servicio durante este periodo sin el apoyo de la infraestructura TI.[8]

Para esta opción se utilizan los centros Cold-site. Estos tienen la infraestructura básica (cableado eléctrico, aire acondicionado, piso, etc.) para operar un centro de proceso de datos.

El cold-site está listo para recibir el equipamiento pero no ofrece ningún componente instalado antes de que sea necesario. La activación del centro puede llevar semanas.

"Warm Standby" requiere un emplazamiento alternativo con sistemas activos diseñados para recuperar los servicios críticos en un plazo de entre 24 y 72 horas. Los que se llaman Warm-sites estos son centros que están parcialmente configurados, generalmente con equipo periférico seleccionado, tal como unidades de disco, cinta y controladores, pero sin el ordenador principal. A menudo un warm-site está equipado con una CPU de menor capacidad.[8]

El supuesto que respalda al concepto de warm-site es que, en una situación de emergencia, el ordenador se pueda obtener rápidamente (siempre que sea un modelo de uso común) por lo que, dado que el ordenador es la unidad más cara, tal arreglo es menos costoso que un hot-site.

(8) Apunte Gestión de la continuidad del servicio (ver bibliografía)

Después de la instalación de los componentes necesarios, el centro puede ser considerado listo para el servicio en cuestión de horas; sin embargo, la ubicación e instalación de la CPU y de las otras unidades faltantes puede llevar días o semanas.

"Hot Standby" requiere un emplazamiento alternativo con una replicación continua de datos y con todos los sistemas activos preparados para la inmediata sustitución de la estructura de producción. Ésta es evidentemente la opción mas costosa y debe emplearse sólo en el caso de que la interrupción del servicio TI tuviera inmediatas repercusiones comerciales. [8]

Las principales diferencias entre los tres tipos de centros son el tiempo de activación y el costo.

En el caso de un desastre a largo plazo, es deseable una reducción en los costos operativos. Ello puede lograrse utilizando primero un hot-site por un corto plazo y después un warm-site o un cold-site.

"Instalaciones de procesamiento duplicados", es decir, múltiples centros de desarrollo internos con el fin de distribuir el procesamiento y de esta forma lograr un mejor nivel de disponibilidad.

"Mirror Site" se trata de procesar cada transacción en paralelo con el sitio principal.

"Acuerdos recíprocos con otras organizaciones" Los acuerdos recíprocos son contratos entre una o más organizaciones con equipos o aplicaciones similares. En un acuerdo típico, las partes se comprometen a dar tiempo de proceso cuando surja una emergencia.

Ventajas

- Costo reducido.
- Puede ser la única opción disponible en el caso de que no existan hot-sites disponibles.

Desventajas

- Generalmente no es exigible. Solo se utiliza la capacidad de procesamiento sobrante de la otra parte del acuerdo.
- Las diferencias en la configuración del equipo de la otra parte, normalmente, exige cambios a programas a fin de operar eficazmente.
- Los cambios que no se notifiquen en cuanto a carga de trabajo o configuraciones del equipo hacen inútil el acuerdo.

Entrenamiento y Capacitación del Plan de Continuidad de Negocios

Por último, es importante destacar que todos los empleados de la organización deben conocer de manera detallada los alcances y objetivos del plan de continuidad del negocio. Esto con el objetivo que en el caso de activarse el plan, cada uno de los empleados conozcan las actividades que el debe desarrollar, para con esto el plan sea ejecutado de una forma efectiva y eficiente.

11.2.- PLAN DE CONTINGENCIA

La información es el patrimonio principal de toda organización, por lo que se deben aplicar medidas de seguridad para protegerla y estar preparados para afrontar contingencias y desastres de diversos tipos.

DEFINICIÓN

Un plan de contingencia se puede definir como una estrategia planificada con una serie de procedimientos que faciliten tener una solución alternativa que permita restituir rápidamente los servicios de la organización ante la eventualidad de todo lo que pueda paralizar, ya sea de forma parcial o total.

El Plan de Contingencia de los Sistemas de Información es una herramienta que ayuda a que los procesos críticos de una empresa u organización continúen funcionando a pesar de una posible falla en los sistemas informáticos.

Los riesgos pueden medirse según el grado de impacto en la actividad normal de una empresa, hoy en día es de vital importancia realizar un estudio de los diversos riesgos e impactos que nos pueden afectar en nuestra empresa por su alta incidencia por las implicaciones que tienen en la empresa y probabilidades de ocurrencia.

Objetivo del Plan de Contingencia

Definir las pautas generales para asegurar una adecuada recuperación de la información en caso de ser necesario a través de la metodología definida para recuperar el procesamiento de los recursos críticos.

A través de la metodología definida, garantizar la continuidad de las operaciones de los elementos críticos que componen los sistemas de información.

Según la criticidad de los Servicios afectados, una eventualidad en los Sistemas de Información tendrá diferente impacto en la organización, pudiendo afectar la supervivencia de la empresa, si no se tienen definidas diversas medidas que minimicen impactos de riesgos a los cuales se esta expuestos.

11.2.1.- ANALISIS DE CRITICIDAD

Críticos:

- Sus funciones no pueden ser ejecutadas a menos que sean reemplazadas por recursos idénticos.
- No se pueden utilizar métodos manuales.
- Costo de interrupción es muy alto.

Vitales

- Sus funciones pueden ser ejecutadas manualmente durante un período corto.
- Mayor tolerancia a las interrupciones.
- Costos de interrupción menores.

Sensitivos

- Sus funciones pueden ser ejecutadas manualmente durante un período relativamente largo.
- Mientras se hace manualmente requiere de Staff adicional.
- Costos de interrupción medios.

No Críticos

- Sus funciones pueden ser interrumpidas durante un período relativamente largo, con poco o ningún costo.

11.2.2.- METODOLOGIA

Una forma de abordar los Planes de Contingencia de Sistemas de Información es analizando detalladamente la relación costo/impacto de los recursos que garantizan la continuidad de los servicios, con objeto de ir ajustando las inversiones y los costos involucrados.

Los planes de contingencia sirven para minimizar el impacto que pueda generar un siniestro en los sistemas de información de una compañía, asegurando la continuidad del servicio prestado, una satisfacción del cliente y productividad de alta calidad, a pesar de una catástrofe ocurrida, además de alcanzar una alta disponibilidad de la información para la infraestructura crítica.

Una metodología empleada para el desarrollo y aplicación del Plan de Contingencias de los Sistemas de Información, puede ser desarrollada en las siguientes fases:

- Identificación de Servicios Críticos
- Inventario de Recursos
- Asignación de Criticidad y Tiempo de Recuperación Límite
- Identificación de Riesgos
- Identificación de soluciones
- Diseño de Estrategias de Respaldo
- Definir la Organización de Contingencias
- Documentación de los procedimientos de Respaldo
- Realización de las pruebas

Tipo de Plan de Contingencia

Backup & Restore

Debido a los grandes volúmenes de datos que las empresas modernas crean, transmiten y gestionan cada día, es imprescindible que las organizaciones estén bien equipadas para reanudar sus operaciones rápidamente en caso de desastre o interrupción. No sólo ha aumentado la dependencia de estos datos, también lo ha hecho la cantidad, el tipo y la gravedad de las amenazas a las que se enfrenta cada día (desde virus, software maligno y corrupción accidental o malintencionada de datos errores de aplicación y desastres naturales). Para conseguir una infraestructura segura y fiable, la organización necesita restablecer rápidamente la continuidad de sus operaciones, antes de que el tiempo de inactividad afecte de forma negativa al funcionamiento del negocio o las relaciones con los clientes.

Un Backup permite garantizar la fiabilidad y disponibilidad de los datos críticos de la empresa.

Definición de Backup & Restore

Los Backup son una contramedida que podemos realizar de protección de datos de alto rendimiento, unen la innovadora tecnología de eliminación de datos duplicados, informes potentes de gestión de recursos de almacenamiento, copias de seguridad de disco a disco a cinta (D2D2T) y de bibliotecas de cintas virtuales (VLT), así como medidas de seguridad exhaustivas. Por ello, es uno de los métodos más seguros, fiables y eficaces de proteger la información que reside en los servidores físicos y virtuales. Los backup permiten garantizar la integridad y la disponibilidad del activo de negocio más importante y de mayor valor estratégico, su información.

11.3.- Plan de Contingencia v/s Continuidad de Negocio

El enfoque del plan de contingencia se basa en la minimización del impacto financiero que pueda tener un desastre en la compañía, mientras que el plan de continuidad está orientado a asegurar la continuidad financiera, satisfacción del cliente y productividad a pesar de una catástrofe. Mientras que el plan de contingencia se concentra en la recuperación de eventos únicos que producen una interrupción prolongada del servicio, el plan de continuidad se ejecuta permanentemente a través de la administración de riesgos tanto en la información como en la operación. Los riesgos que se enfrentaban en la planeación anterior eran desastres con baja frecuencia pero muy alto impacto. Hoy los riesgos son casi todos de muy alto impacto por las implicaciones que tienen en la empresa ampliada (socios de negocios) y de muy alta ocurrencia. Ya todas las empresas están expuestas a ataques con virus, problemas de seguridad en la información, calidad del software, almacenamiento de datos inapropiado, arquitecturas tecnológicas complejas y hasta políticas poco efectivas de administración de recursos que pueden abrirle las puertas a una catástrofe con el mismo impacto en el negocio (y hasta mayor) que el impacto causado por una amenaza física como un incendio o un terremoto.

Debe quedar claro que un plan de continuidad no es excluyente de un plan de contingencia, sino más bien que el segundo está dentro del primero. Un plan de continuidad para el negocio debe incluir: un plan de recuperación de desastres, el cual especifica la estrategia de un negocio para implementar procedimientos después de una falla; un plan de reanudación que especifica los medios para mantener los servicios críticos en la ubicación de la crisis; un plan de recuperación que especifica los medios para recuperar las funciones del negocio en una ubicación alterna; y un plan de contingencia que especifica los medios para manejar eventos externos que puedan tener serio impacto en la organización.

El plan de continuidad es costoso y no es para todas las empresas, ni para todos los procesos de una gran empresa. Se requiere un adecuado estudio de riesgos y balancear el

costo de la implementación de un plan de continuidad con el riesgo de no tenerlo. Sigue siendo el primer paso todavía determinar la criticidad de cada proceso dentro de la empresa ampliada. Para los de muy alta criticidad se deberá implementar un plan de continuidad, para otros, bastará con un plan de contingencia.

12.-USO DE INFORMACIÓN COMO HERRAMIENTA DE COMPETITIVIDAD Y DIFERENCIACIÓN, CON RELACION CON DISPONIBILIDAD

Las actividades de las empresas se apoyan cada vez más en los ordenadores, esto genera que su dependencia de las aplicaciones vaya creciendo.

Algunas aplicaciones tecnológicas son tan críticas para la continuidad de las operaciones de las empresas, que sencillamente no toleran ningún tipo de interrupciones. Esto ocurre en aplicaciones del sector bancario, en bolsas de valores, aerolíneas, empresas de transporte, operadores logísticos, agencias de viajes, procesos de fabricación just in time, etc. Este tipo de empresas utiliza la tecnología como medio para obtener ventajas competitivas, ya que necesitan una alta disponibilidad de la información para continuar con sus operaciones y fortalecer su relación con los clientes, por lo que un paro en sus servicios puede causar en pocas horas enormes pérdidas e inclusive poner en peligro la supervivencia de la empresa.

Para obtener una ventaja competitiva una compañía requiere una mejor posición que los rivales para asegurar a los clientes y defenderse contra las fuerzas competitivas. Existiendo muchas fuentes de ventajas competitivas: elaboración del producto con la más alta calidad, proporcionar un servicio superior a los clientes, lograr menores costos que los rivales, tener una mejor ubicación geográfica, diseñar un producto que tenga un mejor rendimiento que las marcas de la competencia.

La disponibilidad de la información puede ayudar a la empresa en la obtención de éstas y otras ventajas competitivas como lo veremos en el siguiente ejemplo.

Industria Automotriz empresa Toyota

Toyota para poder operar con el sistema Just in Time dentro de sus fábricas necesita un sistema de información simple, rápido y fiable que apoye con las comunicaciones continuas que debe mantener con sus proveedores, ya que al ser los trabajadores los que en definitiva deciden la cantidad a producir y no pueden perder el tiempo en descifrar complejos listados de datos ni equivocarse, debido a que esto llevaría a incrementar los stocks, aumentando sus costos de producción.

Mantener una comunicación adecuada es vital para cumplir con los plazos estipulados de entrega, por lo que la disponibilidad que deben tener las líneas de comunicación y la información es esencial.

13.- ENTREVISTA

La entrevista fue realizada a Javier Herrera quien se desempeña como consultor informático. Esta empresa es pequeña, donde el rubro es la Tecnología y su personal (consultores) está muy bien evaluado en el mercado debido a que el equipo de trabajo es la base del éxito de la compañía. El área de TI de la empresa esta compuesta por el Jefe de TI, el mantenedor de las aplicaciones y la persona de soporte técnico.

Desde sus inicios en 1993, ofrece en su ámbito de competencia, productos y servicios acordes con la evolución de las tecnologías de la información, y el aporte de valor que éstas significan para sus clientes; especializándose en productos y servicios de tecnologías de la información Oracle, Microsoft y EMC[2].

Es una empresa Chilena dedicada a la prestación de servicios profesionales, tales como mantención de Base de Datos, Aplicaciones Web, Auditorias Informáticas entre otros, especializados de consultoría, educación y soporte en tecnologías de la información. También es proveedora de productos de software de bases de datos, servidores de aplicaciones, herramientas de desarrollo y de aplicaciones de negocios en arquitectura Internet.

A petición del entrevistado, el nombre de la empresa lo dejaremos en el anonimato.

Al avanzar en la entrevista nos podemos dar cuenta que la empresa no aplica lo que ofrece como servicios a sus clientes en sus procesos internos.

13.1.- PREGUNTAS

1.- ¿Cuáles a su criterio son los procesos críticos de la empresa?

- Asignación de horas de los consultores.
- Registro y cuadratura de horas de los consultores.
- Facturación.

2.- ¿Cuál es el principal problema del área de TI en la organización?

Hay mucha dependencia de una única persona, en este caso el Jefe de TI. Existen procesos operativos que solo él los puede solucionar, como por ejemplo cuando se "caen" los sistemas de contabilidad, facturación y el registro de horas de los consultores.

3.- ¿Podrías definir cuál es la mayor prioridad para el área de TI en la empresa?

- Proveer volúmenes de información.
- Entregar alta capacidad de procesamiento.
- Proveer gran cantidad de recursos a sus usuarios (consultores) Ej: En correo electrónico tener varios gigas, capacidad en servidor de archivos, máquinas virtuales para trabajos de los consultores.

4.- ¿Tienen identificados cuáles son los eventos, amenazas que podrían impactar negativamente las operaciones de la empresa?

- Una amenaza que identificamos fue la vulnerabilidad del correo electrónico, ya que el servicio que presta la empresa a sus clientes depende en gran medida del servicio de este (asignación de jornadas laborales, envío de informes, recepción de nuevos negocios, etc.).

- Otro tema, era que teníamos la información en sistemas de disco sin redundancia, esto quiere decir, teníamos la información en múltiples partes (máquinas) y en sistemas de discos con poca tolerancia a fallas (cortes de luz, fallas del disco físico, etc.)

- El servidor de impresión dependía de una máquina que podía fallar.

5.- ¿Cuáles fueron las soluciones en que incurrió la empresa al punto anterior?

- El tema de la vulnerabilidad del correo electrónico, la empresa opto por externalizar el servicio y migro a Google Apps (el servicio de correo que mantenía la empresa antes era mantenido por ella misma).

- Por otro lado, el tema de la redundancia de información, mejoró comprando una solución de almacenamiento (Storage), donde se consolido la data de múltiples servidores y se agregaron mecanismos como múltiples fuentes de poder, discos despejados.

- Y por ultimo lo que se refiere a la impresora, la solución para esto fue una nueva que recibe conexiones directas desde la red. Esto nos ayudo a no tener estancamiento de trabajos enviados por los empleados.

6.- ¿Cuáles y defina estas políticas para enfrentar estos eventos?

Existe una política, que ante cualquier problema técnico se debe contactar al Jefe de TI.

7.- ¿Cuáles son los riesgos a considerar en la evaluación del área de TI de la empresa, frente a la Disponibilidad?

- Corte del servicio de Internet.
- El site (sala de servidores) es único, no existe site de contingencia.
- Que estén inubicable el Jefe de TI y el mantenedor de las aplicaciones.

8.- ¿Qué controles tienen ante estos riesgos?

- Corte del servicio de Internet: controles proactivos no existen, solo hay reacción rápida con la empresa proveedora de Internet.
- El site (sala de servidores) es único, no existe site de contingencia: no existen.
- Que estén inubicable el Jefe de TI y el mantenedor de las aplicaciones: no existen.

9.- ¿Tienen procedimientos a realizar ante alguna eventualidad o plan de contingencia si ocurrieran algunos de los riesgos?

Hay ciertas labores que realiza el Jefe de TI, y estas pueden ser realizadas por consultores que estén disponibles en la oficina, por ejemplo "rebutar la máquina".

14.- EVALUACION

Una vez realizada la entrevista se nos viene a la mente el siguiente refrán popular "en casa de herrero cuchillo de palo". A pesar de pertenecer al rubro de la Tecnología, debiera estar mas interiorizada en el tema de la disponibilidad, aplicando políticas en este sentido, sin embargo, estas no son realizadas por la empresa.

Hay que tener en cuenta que el tamaño de esta es pequeño, por lo tanto, el costo es mucho más elevado en relación al beneficio que entrega. A pesar de esto, debido al crecimiento que han tenido, a los cambios tecnológicos y necesidades de información de los usuarios, se vieron en la necesidad de implementar tecnologías relacionadas con la disponibilidad.

Según los riesgos identificados por el entrevistado, los planes implementados por la empresa están de acuerdo a sus necesidades de disponibilidad, por lo cual a nuestro juicio no estimamos necesario que en este nivel se adopten otras medidas, sin embargo, si los niveles de disponibilidad crecen se debería evaluar los planes de contingencia que debiera incorporar.

15.- CONCLUSIÓN

Nuestro estilo de vida actual, debido al avance de la tecnología, es mucho más rápido y eso obliga a las empresas a responder a los requerimientos de los usuarios en forma constante, confiable, óptima y con alta disponibilidad.

Además de los sucesos ocurridos a principio de siglo, hizo tomar conciencia a las empresas en adoptar medidas para operar normalmente ante inconvenientes que pudieran interrumpir las operaciones. Estos sucesos influyeron en la incorporación de soluciones para mantener la alta disponibilidad, la que hace frente a una rápida recuperación en caso de que ocurra una falla en el servidor, ante estas las empresas han implementado planes de continuidad y contingencia, para asegurar la disponibilidad y minimizar los impactos que las amenazas puedan provocar si no se encuentran medidas de protección adoptadas.

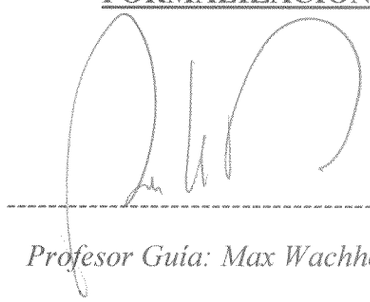
Al utilizar mayor tecnología en las empresas, la dependencia de estas es más alta, ya que la interrupción prolongada genera pérdidas elevadas que no son solo cuantificables, entre las que podemos encontrar pérdida de imagen, de clientes, entre otras. Es por esto que se hace cada vez menos tolerables las fallas que afecten su funcionamiento, maximizando el tiempo disponible de sus sistemas.

De acuerdo a lo expuesto en nuestra investigación podemos concluir que es necesario tomar conciencia de que la disponibilidad para el uso en nuestra vida diaria es importante. Es vital disponer de herramientas que nos faciliten el uso de información, la continua comunicación entre usuarios internos y externos, que permitan un flujo constante sin interrupciones, disponibilidad al 100%.

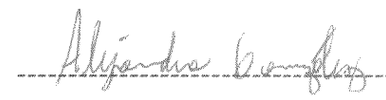
16.- BIBLIOGRAFÍA

- http://www.swgreenhouse.com/Productos/Vision/ContNegocios.html
- Apuntes de Auditoria Computacional, profesor Miguel Ángel Elizondo, Tema: "Procesos de servicios de TI", "Roles relevantes de TI", "ITIL"
- http://www.scribd.com/doc/3572163/Gestion-de-la-Disponibilidad) Downtime
- http://itil.osiatis.es/Curso_A ITIL/Gestion_Servicios_TI/gestion_de_la_disponibilidad/proceso_gestion_de_la_disponibilidad/proceso_gestion_de_la_disponibilidad.php
  Gestión de la disponibilidad
- http://www.scribd.com/doc/3479640/Gestion-de-la-Continuidad-del-Servicio-de-TI
  Gestión de la continuidad
- http://www.monografias.com/trabajos32/auditoria-seguridad-informatica/auditoria-seguridad-informatica2.shtml
  Vulnerabilidades, contramedidas y amenazas
- http://www.mkm-pi.com/mkmpi.php?article450
  SERVICIOS DE TI LA NUEVA ERA DE LA INFORMATICA
- http://www.ca.com/files/ProductBriefs/ca_arcserve_r125_pb_es_167335.pdf
  BACKUP
- Apuntes de Administración de la Disponibilidad, entregados por profesor Max Wachholtz
  http://download.microsoft.com/.../Nivel2AdministraciondeDisponibilidad
- Apunte entregado por profesor Max Wachholtz en seminario N° 56 Tema: Seguridad Informática.
- http://help.sap.com/saphelp_40b/helpdata/es/f4/7d286044af11d182b40000e829fbfe/content.htm
  Cálculo de la Disponibilidad.
- http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/gestion_de_la_continuidad_del_servicio/vision_general_gestion_de_la_continuidad_del_servicio/vision_general_gestion_de_la_continuidad_del_servicio.php
  Continuidad del Negocio.
- http://www.sisteseg.com/sindustrial.html
  Continuidad del Negocio.

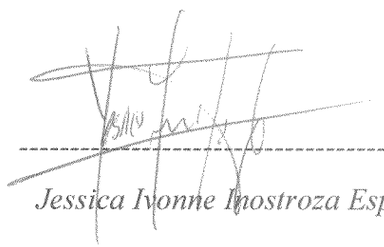
FORMALIZACION



Profesor Guía: Max Wachholtz A.



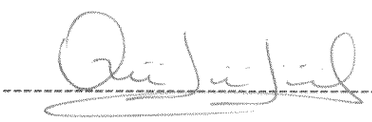
Alejandra Jacqueline González Flores



Jessica Ivonne Inostroza Espinoza

Cheryll Emily Jorquera Pérez

Isabel Margarita Pavez Vásquez



Alejandra Elizabeth Rivas Soto

Santiago, 15 de Julio de 2009