

Contenido

1. INTRODUCCIÓN	4
2. INTRODUCCION A LA RECUPERACION DE DESASTRES	5
2.1. ENTENDIENDO LA RECUPERACIÓN DE DESASTRES	5
NECESIDADES Y BENEFICIOS DE RECUPERACIÓN DE DESASTRES	5
Los efectos de los desastres	5
La recuperación no es accidental	6
La recuperación es requerida por la regulación	7
Los beneficios de la planificación de recuperación de desastres	7
2.2. INICIALIZAR EL ESFUERZO PARA EL PLAN DE RECUPERACION DE DESASTRES	9
COMENZANDO CON LO PRIMERO	9
RECURSOS PARA COMENZAR A PLANIFICAR	11
PLANIFICACIÓN DE OPERACIONES DE EMERGENCIA	12
PREPARACIÓN DE UN PLAN DRP PROVISIONAL	13
CONSTRUYENDO EL PLAN PROVISIONAL	14
3. CONSTRUYENDO PLANES DE RECUPERACION DE DESASTRES	21
3.1. MAPEANDO FUNCIONES DEL NEGOCIO A LA INFRAESTRUCTURA	21
USANDO ARQUITECTURA DE ALTO NIVEL	22
IDENTIFICAR LAS DEPENDENCIAS	24
3.2. PLANIFICACIÓN DE RECUPERACIÓN DE USUARIOS	28
ADMINISTRACIÓN Y RECUPERACIÓN INFORMÁTICA DE USUARIO FINAL	28
ADMINISTRACIÓN Y RECUPERACIÓN DE LAS COMUNICACIONES DE USUARIO FINAL	35
3.3. PLANIFICACIÓN, PROTECCIÓN Y RECUPERACIÓN DE INSTALACIONES	38
PROTEGER LAS INSTALACIONES DE PROCESAMIENTO	38
SELECCIONAR LUGARES DE TRATAMIENTO ALTERNATIVO	41
3.4. PLANIFICACIÓN DE RECUPERACIÓN DEL SISTEMA Y LA RED	44
ADMINISTRACIÓN Y RECUPERACIÓN DE LOS SERVIDORES DE CÓMPUTO	44
ADMINISTRACIÓN Y RECUPERACIÓN DE INFRAESTRUCTURA DE RED	48
LA IMPLEMENTACIÓN DE INTERFACES ESTÁNDAR	49
IMPLEMENTACIÓN DE CLÚSTERES DE SERVIDOR	49

3.5. PLANIFICACIÓN DE RECUPERACIÓN DE DATOS	52
PROTECCIÓN Y RECUPERACIÓN DE LOS DATOS DE LAS APLICACIONES	52
ELECCIÓN DE CÓMO Y DÓNDE DESEA ALMACENAR LOS DATOS	53
PROTECCIÓN Y RECUPERACIÓN APLICACIONES	55
3.6. ESCRIBIENDO EL PLAN DE RECUPERACIÓN DE DESASTRES	56
DETERMINAR EL CONTENIDO DEL PLAN	56
ESTRUCTURACIÓN DEL PLAN	57
3.5. DIEZ HERRAMIENTAS DE PLANIFICACIÓN DE RECUPERACIÓN ANTE DESASTRES	59
LIVING DISASTER RECOVERY PLANNING SYSTEM (LDRPS)	59
BIA PROFESIONAL	59
ANÁLISIS DE RIESGOS COBRA	60
GENERADOR BCP	60
KIT DE DRP PRÁCTICAS PROFESIONALES	60
PLANTILLA PLAN DE RECUPERACIÓN DE DESASTRES	61
KIT DE SLA	61
LBL CONTINGENCIA PRO SOFTWARE	62
GUÍA DE GESTIÓN DE EMERGENCIAS PARA LA EMPRESA Y LA INDUSTRIA	62
CAJA DE HERRAMIENTAS DE DRJ	62
4. CONCLUSIONES	64
5. BIBLIOGRAFÍA	65

PLAN DE RECUPERACION DE DESASTRES (DRP)**1. INTRODUCCIÓN**

Los desastres de muchos tipos atacan organizaciones de todo el mundo en casi de manera diaria. Pero la mayoría de estos desastres nunca son los titulares de las noticias, ya que se producen a nivel local. Nosotros probablemente nos enteramos de los acontecimientos desastrosos que ocurren en o cerca de nuestra comunidad: incendios, inundaciones, deslizamientos de tierra, disturbios civiles, y así sucesivamente, que afectan a las empresas locales, a veces de manera devastadora. Grandes desastres afectan a amplias zonas y resultan en daños generalizados, evacuaciones, y pérdida de la vida, y puede hacer que se sienta congelado a veces, debido a la magnitud de sus efectos.

El presente trabajo trata de la supervivencia de los sistemas de negocios de TI en la organización frente a los desastres a través de la preparación y la respuesta. Somos, en gran medida, incapaces de detener los propios desastres, e incluso si podemos librarnos lo más posible, rara vez podemos escapar de sus efectos por completo. Los desastres, por su propia naturaleza, interrumpen todo a su alcance.

La organización puede planificar para estos desastres y tomar medidas para asegurar la supervivencia de los sistemas críticos de TI. Este trabajo muestra cómo prepararse.

2. INTRODUCCION A LA RECUPERACION DE DESASTRES

2.1. ENTENDIENDO LA RECUPERACIÓN DE DESASTRES

La planificación de recuperación de desastres (DRP) se refiere a la preparación y respuesta cuando ocurre un desastre. El objetivo de la planificación DRP es la supervivencia de una organización.

NECESIDADES Y BENEFICIOS DE RECUPERACIÓN DE DESASTRES

Son cosas que pasan. Cosas malas.

Los desastres de todo tipo pasan, y es posible salir de su camino y escapar de sus consecuencias muy difícil. Tener la suerte de evitar el impacto directo de un desastre, esquivando sus efectos secundarios, es más difícil todavía.

Estos son algunos de los desastres que pueden atacar a una organización:

- Los incendios
- Inundaciones
- Tornados
- Los huracanes
- El viento y las tormentas de hielo
- Las tormentas severas
- Los incendios forestales
- Los deslizamientos de tierra
- Avalanchas
- Los tsunamis
- Terremotos
- Volcanes
- Los incidentes de seguridad
- Los fallos del equipo
- Fallas eléctricas
- Fracasos de utilidad
- Incendio provocado
- Las pandemias
- Sabotaje
- Las huelgas y paros laborales
- La escasez
- Los disturbios civiles
- Terrorismo
- Guerra

Cada uno de los escenarios de la lista anterior tiene efectos primarios y secundarios únicos que necesitamos tener en cuenta al desarrollar un plan de recuperación de desastres.

Los efectos de los desastres

Los acontecimientos que se enumeran en la sección anterior tienen el potencial de infligir daños en edificios, equipos y sistemas de TI. Afectan a las personas, también, matando, hiriendo y dislocándolos, sin mencionar que les impide presentarse a trabajar. Los desastres pueden tener los siguientes efectos en las organizaciones:

1. **Los daños directos:** Muchos de estos eventos puede dañar directamente los edificios, equipos y sistemas de TI, quedando edificios inhabitables y sistemas inutilizables.
2. **Inaccesibilidad:** A menudo, un evento daña a un edificio hasta el punto de que es peligroso entrar. Las autoridades civiles pueden prohibir que el personal entre en un edificio, incluso para recuperar artículos o equipos.
3. **Corte de Energía:** Incluso en los incidentes que no causan ningún daño directo, eléctrico, la energía eléctrica, agua y gas natural son a menudo interrumpidos en amplias zonas por horas o días. Sin los servicios públicos, los edificios son a menudo inhabitables y los sistemas no pueden funcionar.
4. **Interrupción de transporte:** Los incidentes generalizados a menudo tienen un profundo efecto sobre el transporte regional, incluyendo carreteras principales, carreteras, puentes, ferrocarriles y aeropuertos. Las interrupciones en los sistemas de transporte puede impedir que los trabajadores vayan al trabajo (o ir a casa), puede quitar la recepción de los suministros, y detener el envío de los productos.
5. **Interrupción de comunicación:** La mayoría de las organizaciones dependen de comunicaciones de voz y de datos para las necesidades operativas diarias. Los desastres ocasionan interrupciones generalizadas en las comunicaciones, ya sea por daños directos a la infraestructura o los picos repentinos relacionados con el desastre. En muchas organizaciones, que no tienen forma de comunicación, especialmente comunicaciones de datos - es tan devastador como el cierre de sus sistemas informáticos.
6. **Evacuaciones:** Muchos tipos de desastres representan una amenaza directa a la gente, lo que resulta en evacuaciones obligatorias de ciertas áreas o regiones enteras.
7. **Ausentismo laboral:** Cuando se produce un desastre, los trabajadores a menudo no pueden o no se presentarán a trabajar por muchas razones. Los trabajadores con familias a menudo necesitan cuidar a sus familias si el desastre les afecta. Sólo después de que atiendan a sus familias los trabajadores consideran presentarse a trabajar. Además, el transporte y cortes de servicios públicos pueden impedir viajar al trabajo. Los trabajadores tampoco pueden saber si la organización espera que se reporten al trabajo si los daños de un desastre cierran los locales de trabajo.

Estos efectos pueden devastar negocios haciéndolos cesar sus operaciones por horas, días o más tiempo. En la mayoría de casos, las empresas simplemente no pueden sobrevivir después de experimentar una interrupción tal. Las empresas proveedoras de

bienes o servicios a clientes que, en su mayor parte, sólo quieren esos bienes y servicios; si los clientes no pueden obtener esos bienes o servicios de una empresa, simplemente van a ir a otro que si les puede proporcionar los productos. Muchas empresas no se recuperan de un éxodo de clientes.

La recuperación no es accidental

Desde una perspectiva de DRP, el mundo se divide en dos tipos de negocios: los que tienen DRP y las que no lo hacen. Si ocurre un desastre en las empresas de cada categoría, ¿Cuáles van a sobrevivir?

Cuando ocurre un desastre, las empresas sin planes DRP tienen una extremadamente difícil tarea por delante. Si el negocio tiene algún proceso crítico altamente sensible al tiempo, ese negocio está prácticamente, destinado al fracaso. Si un desastre golpea un negocio sin un plan de DRP, esa empresa tiene muy pocas posibilidades de recuperación. Y es, seguramente, demasiado tarde para comenzar a planificar.

Las empresas que sí tienen planes DRP todavía pueden tener un momento difícil cuando ocurre un desastre. Es posible que tengamos que poner un gran esfuerzo para recuperar las funciones críticas del negocio. Pero si tenemos un plan DRP, tenemos una oportunidad de luchar por la supervivencia.

La recuperación es requerida por la regulación

El desarrollo de los planes de recuperación de desastres solían ser simplemente una buena idea. Estos planes son aún una buena idea, pero también están empezando a aparecer en las normas y reglamentos, incluyendo:

- **PCI DSS (Payment Card Industry Data Security Standard):** Aunque no es realmente la legislación del gobierno, se requiere para casi todas las empresas de comercio y de servicios financieros. PCI es un gran ejemplo de lo que llamamos la legislación privada: leyes hechas por corporaciones en lugar de los gobiernos. Todos los grandes bancos y compañías de tarjetas de crédito imponen PCI.
- **ISO 27001:** Esta norma internacional para la gestión de la seguridad está ganando considerable reconocimiento. Muchas grandes organizaciones exigen a sus proveedores de servicios de TI cumplir la ISO 27001.
- **BS 25999:** La norma internacional emergente para la gestión de la continuidad del negocio.
- **NFPA 1620:** El estándar de la Asociación Nacional de Protección contra Incendios para la planificación antes del

desastre. Es una práctica recomendada que se ocupa de la protección, la construcción y las características operativas de las ocupaciones específicas para desarrollar planes anteriores a los incidentes que socorristas pueden utilizar para gestionar los incendios y otras emergencias mediante el uso de los recursos disponibles.

Con el tiempo, más leyes de seguridad de datos están seguros de incluir la planificación de recuperación de desastres.

Los beneficios de la planificación de recuperación de desastres

Además de la preparación evidente para sobrevivir a un desastre, las organizaciones pueden disfrutar de otros beneficios de la planificación DRP:

- **La mejora de los procesos de negocio:** Debido a los procesos de negocio se someten a un análisis y escrutinio, los analistas casi no pueden dejar de encontrar áreas de mejora.
- **La tecnología mejorada:** A menudo, es necesario mejorar los sistemas de TI para apoyar los objetivos de recuperación que desarrollamos en el plan de recuperación de desastres. El conocimiento que usted paga para recuperar también conduce a menudo a hacer los sistemas de TI más coherentes entre sí y, por lo tanto, más fácil de administrar y predecir.
- **Menos interrupciones:** Como resultado de la mejora de la tecnología, los sistemas de TI tienden a ser más estables que en el pasado. Además, cuando se realizan cambios en la arquitectura del sistema para satisfacer los objetivos de recuperación, eventos que solían causar apagones no lo hacen más.
- **Servicios de mayor calidad:** Debido a la mejora de procesos y tecnologías, que mejoran los servicios, tanto internamente como a los clientes y socios de la cadena de suministro.
- **Ventajas competitivas:** Tener un buen plan DRP da una empresa exigir derechos que pueden eclipsar a competidores. El precio no es necesariamente el único punto en el que las empresas compiten por el negocio. Un plan de DRP permite a una empresa con la reivindicación también una mayor disponibilidad y fiabilidad de los servicios.

Un negocio a menudo no espera estos beneficios, a menos que sepa anticiparse a través de su desarrollo de planes de recuperación de desastres.

2.2. INICIALIZAR EL ESFUERZO PARA EL PLAN DE RECUPERACION DE DESASTRES

Poner un completo plan de recuperación de desastres (DRP) en nuestra organización puede tomar uno o dos años, desde el inicio, para el análisis del impacto de negocios, para planificar el desarrollo y pruebas. Un proyecto DRP adecuado, debe envolver sus brazos alrededor de todo el negocio (o, en todo caso, en torno a esas partes del negocio que usted elija para colocar dentro del alcance del proyecto, porque son lo suficientemente importantes como para justificar la planificación DRP); realizar un análisis profundo de los procesos de negocio; desentrañar y analizar dependencias entre procesos, sistemas de información, bienes y proveedores; y comenzar construyendo el plan ellos mismos.

Un proyecto DRP es un esfuerzo considerable el cual debe comenzar y terminar. Podemos tomar algunos enfoques diferentes para empezar. Se podría pensar de estos enfoques como las diferencias en estilos, o como formas de abordar las brechas o los riesgos operativos:

- **Llevar a cabo un proyecto completo DRP.** Podemos sólo saltar en el gran proyecto de DRP, empezando por el Análisis de Negocios Impacto (BIA), el análisis crítico, análisis de riesgos y planes de recuperación específicos para los sistemas de TI.
- **Comenzar con un proyecto a corto plazo.** Por otra parte, es posible que decida construir un plan de operaciones de emergencia primero, en caso de que ocurra un desastre antes de completar el DRP. La creación de un plan de operaciones de emergencia es básicamente, una estructura de comando y control establecido y un plan de comunicación sin ningún procedimiento de recuperación reales, pueden ayudar a identificar y estructuras de arriba hacia abajo de gestión de documentos y comunicaciones que deben llevarse a cabo durante un desastre.
- **Desarrollar un plan provisional.** Es posible construir un DRP interino que dirige los pasos específicos que se puede tomar para obtener los sistemas de TI que dan soporte a los procesos de negocio críticos en funcionamiento lo antes posible. Un DRP provisional no es un plan completo, y no es un sustituto para uno, pero sí le proporcionan cierta protección en caso de un desastre antes de que termine el DRP completo.

A continuación, se describen los recursos críticos que se necesita para la planificación de un DRP y cómo llevar a cabo la planificación de las operaciones de emergencia y planificación de un DRP interino.

COMENZANDO CON LO PRIMERO

Antes de iniciar un esfuerzo de planificación DRP, tiene que imaginar los efectos que un desastre podría tener en su organización. DRP es sobre la prevención y respuesta a los desastres, y para planificar correctamente, necesitamos saber sobre que debemos planificar.

Cómo un desastre puede afectar a la organización

Pensemos acerca de los desastres que han ocurrido en esta región del mundo. Considere los efectos inmediatos que el desastre tuvo: Tal vez el desastre dañó instalaciones de comunicaciones; interrumpió los servicios públicos, como la electricidad o el agua, por horas o días; o dañó sistemas de transporte, como carreteras, ferrocarriles y aeropuertos.

Ahora, tengamos en cuenta los efectos secundarios de la catástrofe. Cuando un desastre interrumpe las principales instalaciones de infraestructura, como las comunicaciones, el transporte y la energía, la capacidad de su negocio y su funcionamiento se ve afectado en gran medida. Los trabajadores no pueden transportarse y presentarse a trabajar. Los clientes no pueden viajar a las instalaciones de la empresa o visitar aquellas empresas en línea.

Si los efectos de un desastre son relativamente de corta duración (es decir, sólo unas horas o unos pocos días), la mayoría de las empresas se pueden recuperar. La organización puede satisfacer la demanda reprimida de servicios cuando se reanuden sus procesos de negocio más críticos, por lo general los procesos directamente relacionados con la generación de ingresos o de servicio al cliente.

Si los efectos de un desastre son más persistentes, los clientes pueden desviar temporalmente su demanda de bienes y servicios a otros proveedores (si otros proveedores están disponibles). La naturaleza de los bienes o servicios que una organización presta, ayuda a determinar si esa organización puede recuperarse de un desastre que dura más de unos pocos días.

Comprender el papel de la prevención

No se puede prevenir desastres naturales o provocados por el hombre. Sin embargo, puede controlar un poco el impacto que un desastre tiene en las operaciones de su organización mediante la reducción de los efectos del desastre en el negocio.

En la planificación de recuperación de desastres, prevención significa la promulgación de medidas de anticipación que reduzcan o eliminen los efectos que un desastre puede tener en los procesos críticos de negocio. He aquí algunos ejemplos:

- **Alimentación de emergencia:** Una organización puede ser capaz de mitigar los efectos de un desastre mediante la inversión en equipos de generación de energía eléctrica de emergencia que pueden producir electricidad, incluso cuando los servicios públicos no están disponibles para varios días o más.

- **Varias rutas de comunicación:** Si usted reconoce que los desastres suelen causar interrupciones de comunicación, usted puede ser capaz de mitigar este riesgo mediante la inversión en vías de comunicaciones secundarias y terciarias que pueden seguir funcionando, incluso si las instalaciones principales están dañados.
- **Ordenadores de copia de seguridad en otra ciudad:** Un negocio donde los servicios de los clientes se da a través de Internet, pueden ser capaces de proporcionar esos servicios desde prácticamente cualquier lugar, si esas capacidades se han diseñado a partir de los inicios.

Aunque ninguna de las medidas en la lista anterior previene desastres, esas medidas pueden ayudar a una organización para que siga funcionando después de que un desastre se lleve a cabo. Todas estas medidas requieren de una planificación previa e inversión. El tiempo para equipar a un trasatlántico con chalecos salvavidas es antes de que salga de puerto, no después de que el barco comienza a hundirse.

Comprender el papel de la planificación

Las medidas que se puede tomar para disminuir los efectos de los desastres son la esencia de la planificación de recuperación de desastres. La planificación de escenarios con antelación, y la preparación para ellos a través de la inversión en equipo y capacitación, constituyen la mayor parte de la planificación de DRP.

La parte de planificación de la planificación DRP implica averiguar lo que debe hacer el personal cuando ocurre un desastre. Cuando ocurren los terremotos, tsunamis, huracanes, deslizamientos de tierra, o huelga laboral, ¿Qué es lo que el personal necesita hacer para mantener los sistemas críticos funcionando? Estos y muchos otros escenarios requieren una planificación anticipada para que el personal de operaciones de emergencia sepan cómo mantener esos sistemas en marcha.

La planificación anticipada es la clave para la supervivencia en caso de desastre.

RECURSOS PARA COMENZAR A PLANIFICAR

Para obtener el proyecto de recuperación de desastres en marcha, necesita recursos de muchas de las diferentes áreas del negocio. El proyecto requiere de personas con una amplia variedad de habilidades, así como una gran cantidad de información, y de conseguir esa información, es necesario involucrar a más personas.

Inicio de un proyecto DRP no es una tarea fácil. La planificación de la recuperación de desastres es complicado y multidisciplinario. Es

probable que sea uno de los proyectos más grandes que la mayoría de las organizaciones se comprometen, y que reúne a muchas personas que normalmente no se asocian entre sí.

Por estas y otras razones, necesita muchos recursos importantes antes de empezar un proyecto DRP:

- **Patrocinio Ejecutivo:** Un alto directivo o ejecutivo que esté dispuesto a decir: ". La planificación de recuperación de desastres es tan importante que tenemos que completarlo antes de esta fecha" En otras palabras, necesitamos encontrar a alguien que esté dispuesto a poner su dinero en lo que dice.
- **Presupuesto:** En las primeras etapas de un proyecto DRP, necesita dinero para un jefe de proyecto, expertos en tecnología, expertos en procesos o ayuda suplementaria para los departamentos, ya que desvían recursos lejos de su negocio habitual al proyecto DRP. En las etapas posteriores del proyecto, de gastar dinero en mejoras de la tecnología que usted necesita para apoyar los objetivos de recuperación.
- **El director del proyecto:** Se necesita un fuerte jefe de proyecto para un proyecto multidisciplinar que puede involucrar a docenas de personas o más, como la planificación de recuperación de desastres. Usted puede tener un gerente de proyecto a tiempo parcial o a tiempo completo, en función del número de personas y las actividades involucradas.
- **Expertos en la materia:** Se necesitan expertos en los procesos de negocio que la organización tiene en juego, en particular los procesos que ganan ingresos o servicios a los clientes. También necesita expertos en tecnología que entienden las aplicaciones de TI e infraestructuras que dan soporte a dichos procesos.
- **Las personas con habilidades de escritura:** Fases posteriores de los proyectos DRP requieren que las personas puedan escribir los procesos y procedimientos de manera que cualquiera puede entender. Nunca se sabe quién puede terminar en un equipo de respuesta a desastres.

Un proyecto típico de DRP puede tomar entre tres meses (para la organización más pequeña) a más de un año en completarse. Con qué rapidez se obtiene un plan de DRP depende de qué tan alto sea la prioridad con la que necesite hacerla y la cantidad adicional de dinero que tiene disponible para la ayuda externa.

Si no tenemos un buen control sobre la cantidad de recursos que podemos necesitar en el proyecto, aquí hay un par de sugerencias:

- **Contratar a un consultor.** Traer un consultor experimentado DRP, sólo por un compromiso a corto plazo (no más de unos

pocos días), para echar un vistazo alrededor y darte algunas estimaciones en miniatura en las dimensiones del proyecto.

- **Desarrollar un plan de DRP provisional.** Usted debe desarrollar un plan de DRP interino de todos modos, pero al escribir este plan, usted puede conseguir la información adicional sobre el número de procesos críticos, sistemas, proveedores, y así sucesivamente en su negocio. Esa información puede ayudar a estimar el tamaño y el alcance del plan de DRP real.

PLANIFICACIÓN DE OPERACIONES DE EMERGENCIA

Después de un desastre, el equipo de respuesta a desastres comienza a realizar sus diversas tareas relacionadas con la evaluación, reinicio, y la recuperación de los sistemas críticos de TI que dan soporte a los procesos críticos de negocio. La respuesta a desastres implica más que sólo aquellas personas que están en recuperación de sistemas, sin embargo. El resto del personal de respuesta a desastres tiene que realizar una variedad de actividades, incluyendo la comunicación con los clientes, gestión de la empresa, proveedores y socios. Como la respuesta al desastre se desarrolla, un montón de gente está trabajando, la comunicación y la toma de decisiones. El control de todas estas actividades requiere considerable la gestión, el liderazgo y la planificación.

Planificación de las operaciones de emergencia es la parte de la planificación de recuperación de desastres asociados con la instalación y el funcionamiento de las operaciones de emergencia durante e inmediatamente después de un desastre.

A menudo se realizan operaciones de emergencia de planificación en las primeras etapas de la planificación de recuperación de desastres. El propósito principal de la planificación de operaciones de emergencia es asegurar que la gestión de la empresa pueda seguir gestionando las operaciones comerciales día-a-día, incluyendo los esfuerzos de respuesta a desastres, durante e inmediatamente después de un desastre.

Un plan de operaciones de emergencia puede incluir:

- **Listas de contactos de emergencia:** El personal clave necesita saber cómo ponerse en contacto entre sí cuando ocurre un desastre.
- **Procedimiento de declaración de desastre:** El personal clave debe saber cómo reconocer cuando un evento ha interrumpido las actividades clave del negocio suficientes para iniciar la respuesta a desastres.
- **Comunicaciones de emergencia:** procedimientos de comunicaciones, información de contacto para el personal y

recursos adicionales, y tal vez con un guion de comunicaciones a los clientes o accionistas.

El plan de operaciones de emergencia también puede incluir el establecimiento de un **Centro de Operaciones de Emergencia (COE)**. Las organizaciones más grandes a menudo configuran un comando y centro de control de emergencia, tales como el centro neurálgico de sus operaciones de emergencia durante un desastre.

PREPARACIÓN DE UN PLAN DRP PROVISIONAL

La mayoría de las organizaciones pueden reconocer de inmediato los riesgos asociados con la ausencia de un plan de recuperación de desastres. Si se sabe que no se puede tener un plan de DRP completo en su lugar y probarlo durante más de un año, es posible que se desee tener algo mientras se complete el plan de DRP completo.

A menudo, un plan de DRP interino puede llenar este vacío. Se puede crear este plan de forma rápida y con el mínimo esfuerzo. No es, por supuesto, tan completo como un plan de DRP completo.

Estas son las características generales de un plan provisional:

- Está construido rápidamente, generalmente en menos de 15 a 20 horas-hombre.
- Está construido con una cantidad relativamente baja de esfuerzo.
- Proporciona al negocio acciones con algunas capacidades limitadas si un desastre ocurre antes de completar el plan de DRP completo.
- No es ningún sustituto para el plan completo DRP que la organización está (o debería ser) trabajando.

¿Por qué se debe construir un plan provisional? Bueno, estadísticamente hablando, los desastres ocurren con poca frecuencia - pero ocurren. Ayuda a mantener su negocio a flote - pero no es un reemplazo para un plan de DRP real. Cuando se hace un plan de DRP interino, está en desarrollo sólo un pequeño plan de DRP.

Selección de personal del equipo de plan de DRP interino

Los miembros de la alta dirección o ejecutivo que patrocinan el esfuerzo completo DRP deben seleccionar dos o tres gerentes con experiencia y conocimientos para construir el plan de DRP provisional. Estos administradores deben tener conocimiento pragmático y práctica de las operaciones y procesos de negocio actualmente en vigor.

Se debe reunir a los planificadores DRP provisionales una oficina o una sala de conferencias, y proporcionarles espacio pizarra, un par de ordenadores portátiles, y sobre todo un día de comida.

CONSTRUYENDO EL PLAN PROVISIONAL

Las siguientes secciones describen los pasos que los planificadores DRP provisionales necesitan hacer para obtener el plan de DRP provisional construido. Los pasos son los siguientes:

1. Construir el Equipo de Respuesta de Emergencia (ERT).

Los planificadores DRP provisionales primero identificar un equipo de individuos dentro de la organización que pueden ser llamados a la acción, a cualquier hora del día o de la noche, cuando ocurre un desastre. Los planificadores DRP provisionales eligen los miembros del Equipo de entre la población mayor general.

Se debe seleccionar al menos un miembro del personal suplente por cada miembro en el Equipo de Respuesta a Emergencias. Tratar a estos miembros del equipo alternos como miembros de pleno derecho del equipo, ya que se podría tener que llamar a la acción cuando se produce un desastre.

2. Definir el procedimiento para la declaración de un desastre.

Declaración de un desastre no es el simple reconocimiento de que ha ocurrido un evento hecho por el hombre o naturales destructivos. Por ejemplo, un tornado rasgado por la ciudad, un ataque terrorista, o una fuerte tormenta no es igual a un desastre.

Estos eventos pueden estar relacionados con un desastre, pero no son el desastre por sí mismos. Un desastre ocurre cuando un evento natural o hecho por el hombre causa una interrupción significativa, o completamente paradas, las operaciones comerciales.

Determinar el **Máximo Tiempo Aceptable de Interrupción (MAOT)** antes de un desastre. El MAOT puede ser un período que va desde unas pocas horas hasta varios días o más. El MAOT es el período más largo de tiempo entre el inicio de un desastre y la reanudación de un proceso de negocio crítico. La ERT debe evaluar el desastre y determinar si los procesos críticos de su negocio es probable que exceda el MAOT. Si la ERT (Emergency Response Team) cree que también le supera el MAOT, la ERT debe declarar un desastre. Saber cuándo declarar un desastre no es realmente difícil, pero no es obvio, tampoco.

Cuando un evento hecho por el hombre o natural ocurre, que puede interrumpir o poner en peligro las operaciones de negocio, los

miembros de la ERT deben comunicarse entre sí, realizar una evaluación rápida (por ejemplo, determinar si el edificio está dañado, energía eléctrica todavía está en marcha, los empleados estarán capaz de presentarse a trabajar, y así sucesivamente), y hacer un juicio sobre si la empresa debe iniciar el plan de DRP provisional.

3. Invocar el plan de DRP.

Después de que la ERT decide que la MAOT (Máximo Tiempo Aceptable de interrupción) se ha excedido de los procesos críticos, invoca el plan DRP provisional.

Esto es lo que hay que hacer para conseguir su plan en marcha y funcionando DRP:

1. Nombrar a uno de los miembros de la ERT para hacer anotaciones en un cuaderno de bitácora.

Asegúrese de que el miembro toma nota de lo siguientes:

- Descripción general del evento que se ha producido
- Los daños a las instalaciones, activos, sistemas y servicios de comunicaciones
- El personal disponibles y personal de desaparecidos, heridos o fallecidos

2. Organizar una reunión de emergencia inicial.

El equipo tiene que hacer lo siguiente:

- Designar un líder ERT.
- Asignar otras funciones, como la evaluación de daños y comunicaciones.
- Establecer un Centro de Operaciones de Emergencia (COE).

3. Tomar decisiones.

La ERT tiene que determinar si hay el personal suficiente para continuar o deben mudarse a otro sitio, por ejemplo.

4. Iniciar los planes de recuperación.

La ERT tiene que comenzar a realizar los planes de recuperación que el Plan Interino de DRP esboza. Dependiendo del tipo de negocio y la naturaleza de la catástrofe, la ERT puede funcionar de forma continua o por turnos.

4. Mantener comunicaciones durante un desastre.

En muchos escenarios de desastre, las redes de comunicación están dañados y/o los picos de utilización crean congestión.

La probabilidad de que las comunicaciones se congestionan, hace que se tomen algunas contingencias de comunicación:

Tener al menos dos números de teléfono diferentes para cada miembro de la ERT.

- Asegurarse que sus miembros ERT están en varias redes de teléfono diferentes para que un corte de luz en cualquier red no afectará a las comunicaciones a todos los miembros de la ERT.
- Evitar depender de un único proveedor de comunicaciones inalámbricas.
- Evitar colocar el sistema de la organización de teléfono (PBX), correo de voz, correo electrónico y capacidades de conferencia en la ruta crítica. (En otras palabras, tratar de evitar los cuellos de botella de comunicación provocados por el desastre.)
- Usar e-mail no propio de la compañía como una alternativa a la empresa de correo electrónico, en caso de que los servidores de la empresa de correo electrónico no estén disponibles.
- Utilice la mensajería instantánea (IM) como medio complementario de comunicación.
- Utilice el teléfono celular mensajes de texto como un medio suplementario para la transmisión de las actualizaciones de estado.

Algunas de estas contingencias toman un poco de tiempo para crear. Durante el desarrollo del plan de DRP provisional, el equipo debe acordar que las contingencias de comunicación son apropiadas para su organización.

5. Identificar planes básicos de recuperación.

El enfoque es un poco más metódico que las de las secciones anteriores. Se debe seguir estos pasos:

1. **Identifique todas las funciones empresariales de la organización.** Comience en un alto nivel haciendo una lista de las funciones básicas.
2. **Elaborar una lista de los procesos de negocio que conforman las funciones de la empresa a identificar.**
3. **Se debe colocar los procesos más críticos en la parte superior de la lista.**

Una lista de alto nivel de una organización típica podría ser algo como esto:

- Marketing
- Venta
- Soporte Técnico
- Operaciones
- Recepción y envío

- Legal
- Comodidades
- Tecnología de la Información (TI)
- Ingeniería
- Recursos Humanos (RRHH)

Utilice una copia del organigrama de la empresa (si la tiene) para ayudar a identificar todas las principales funciones de la organización

Después de crear la lista de los procesos de negocio, se deben seguir estos pasos:

1. Identificar qué procesos se necesita reiniciar tan pronto como sea posible después de que ocurra un desastre.
2. Para cada proceso, identificar qué tan pronto necesita reiniciar el proceso después de un desastre.
3. Para cada proceso, identificar cuáles son los recursos que necesita para reiniciar el proceso.

No se debe desarrollar una excesivamente ambiciosa lista de procesos para comenzar inmediatamente después de un desastre, que probablemente no será capaz de conseguir realmente en funcionamiento debido a la falta de personal y otros recursos.

6. Desarrollar alternativas de procesamiento.

Los planificadores DRP provisionales necesitan identificar lugares cercanos donde las operaciones críticas de negocio pueden reanudar en el caso de un desastre muy localizado, como un incendio, en el que lejos de edificios, incluso a corta distancia no se verán afectados.

En un desastre regional, como una inundación o un huracán, es necesario identificar los lugares a mayor distancia de la ubicación principal de negocios.

Al considerar cualquier ubicación alternativa, el equipo tiene que prepararse para la posibilidad de poner en marcha cualquier activo o sistema, necesarios, en la ubicación alternativa para que pueda continuar sus operaciones de negocio.

Tener en cuenta estos factores cuando se está en busca de lugares alternativos:

- ¿Puede albergar a los activos, sistemas y personal necesario para continuar procesos críticos de negocio?
- ¿Pueden los clientes y socios de la cadena de suministro de ajustar sus rutas y horarios para utilizar la ubicación alternativa?

Los planificadores DRP provisionales deben tener en cuenta estos factores cuando consideren posibles alternativas de procesamiento:

- La reducción de los niveles de servicios o la producción temporalmente
- Sustituyendo componentes
- El uso de personal temporal
- Compartiendo locales con otras empresas
- El uso de procesos más manuales y depender menos de los sistemas de información
- Utilizando proveedores alternativos y proveedores de servicios

7. Promulgar medidas preventivas.

La pérdida de la información y los activos clave puede ser devastador si ocurre un desastre. El plan DRP interino tiene que identificar la información crítica, registros y activos, y llegar a las medidas de prevención que se pueden implementar de forma rápida y fácilmente con el fin de reducir la probabilidad y el impacto de la pérdida de esos registros y activos.

La siguiente lista contiene sugerencias sobre las medidas preventivas que pueden ser apropiadas para la organización:

Medidas preventivas de TI, tales como

- **Confirme las copias de seguridad de trabajo.** Asegurarse de que las copias de seguridad son en realidad copias de seguridad de datos críticos.
- **Guarde las cintas de copia de seguridad fuera del sitio.** Desarrollar un plan de almacenamiento de medios de copia de seguridad que incluye el almacenamiento fuera del sitio.
- **Practique una estantería segura.** Asegúrese de que los sistemas de bastidores están bien sujetos, de modo que un evento como un terremoto no causará daños.

Mantenimiento de Registros medidas preventivas, tales como:

- **Centralizar el almacenamiento de registros.** Un primer paso lógico para proteger los registros vitales es para sacarlos de los cajones del escritorio de los trabajadores y en una ubicación central.
- **Escanear documentos en papel en los servidores de archivos.** Considere la posibilidad de promulgar un proyecto de electrónica para escanear registros difíciles de reemplazar en papel, tales como archivos de personal y contratos.
- **Registros en papel de fotocopias.** Tienen registros vitales fotocopados y almacenar las copias en un lugar seguro fuera de sitio, lo suficientemente lejos que un desastre regional no daña tanto los originales y las copias.
- **Utilice archivadores resistentes al fuego.** Considere el uso de gabinetes de archivo resistentes al fuego para los registros vitales.

Medidas de prevención de las instalaciones, tales como

- **Utilice gabinetes resistentes al fuego.** Considere actualizar los gabinetes de almacenaje para los activos críticos con el fin de proteger esos bienes de fuego.
- **Inspeccione detección de incendios y sistemas de extinción.** Asegúrese de que los extintores, detectores de humo, sistemas de riego, y otras medidas de detección y

extinción de incendios están al día y funcionando correctamente.

- **Configurar la ayuda de emergencia y planes de evacuación.** Establecer y realizar pruebas periódicas de las medidas de seguridad personal, tales como artículos de primeros auxilios, luces de emergencia y planes de evacuación.

8. En el documento del plan de DRP provisional

Después de desarrollar el plan de DRP provisional, debe claramente documentarlo. La estructura del plan de DRP interino podría incluir alguna o todas de las siguientes características:

- **Antecedentes:** ¿Quién promovió y patrocinó el desarrollo del plan de DRP provisional?, ¿Quién en realidad lo escribió?, y ¿Quiénes trabajaron como los planificadores DRP provisionales?
- **Equipo de Respuesta a Emergencias (ERT):** Los miembros de la ERT y qué departamentos que representan. Incluir información de contacto completa.
- **Procedimiento de Declaración de Desastres:** describe cómo su empresa declara un desastre. Este procedimiento debe incluir la MAOT (Máximo Permitido Interrupción Tiempo), así como una justificación para el valor MAOT.
- **Procedimientos de comunicaciones:** Describe cómo la ERT y otro personal de negocios harán para comunicarse, tanto entre sí y con el mundo exterior.
- **Procedimientos del plan de recuperación:** Estos procedimientos son la carne del plan de DRP provisional. Describen los procedimientos de recuperación, ubicaciones alternativas, y otra información de contingencia para cada proceso de negocio que ha incluido en el plan de DRP provisional.
- **Medidas preventivas:** Se debe documentar las medidas preventivas en forma de puntos de acción para que las personas y departamentos lleven a cabo estas medidas.

Almacenamiento y distribución

Cuando se completa la documentación del plan de DRP provisional, como mínimo, tener estas copias en su lugar:

- **Copia impresa:** Cada miembro de la ERT debe tener por lo menos dos copias impresas del plan: uno para mantener en el trabajo y otro en casa.
- **Copia impresa fuera de las instalaciones:** Tener una copia del plan de DRP provisional disponible en un lugar fuera de las

instalaciones, lo suficientemente lejos que no va a estar en riesgo de un desastre regional.

- **Copia Electrónica:** Cada miembro de la ERT también debe tener copias electrónicas del plan DRP provisional. Un miembro de la ERT puede encontrar una copia en una memoria USB útil en caso de que él o ella no puede conseguir su ordenador portátil que funciona, pero puede encontrar a alguien que tiene un ordenador portátil que funciona.
- **Online:** Coloque el plan de DRP provisional en un lugar seguro en línea, accesible por todos los miembros de la ERT.

9. Los miembros de tren ERT.

Todos los miembros de la ERT, y sus suplentes, tienen que pasar por una sesión de entrenamiento formal, en el que se informan todos los elementos básicos del plan de DRP provisional, incluyendo:

Lo que el plan es y no es: miembros de la ERT tienen que saber que el plan de DRP provisional no es el plan a largo plazo DRP, es sólo una medida provisional hasta que se pueda plenamente desarrollar e implementar el plan de DRP a largo plazo.

Declaración de desastre: Probablemente la parte más difícil de un plan de DRP está en recibir miembros de la ERT para declarar realmente un desastre. Tienen que estar familiarizado con el procedimiento y los criterios utilizados para determinar si deben invocar un desastre.

Centro de Operaciones de Emergencia (COE): Los miembros de la ERT necesitan saber cómo configurar y gestionar las operaciones de emergencia en el COE. Cada miembro de la ERT tiene que entender que él o ella puede ser el líder del COE, dependiendo de quién está disponible y cómo una situación de desastre se desarrolla.

La promulgación de las operaciones de recuperación: Cada miembro de la ERT tiene que estar familiarizado con las operaciones de recuperación en el plan de DRP provisional.

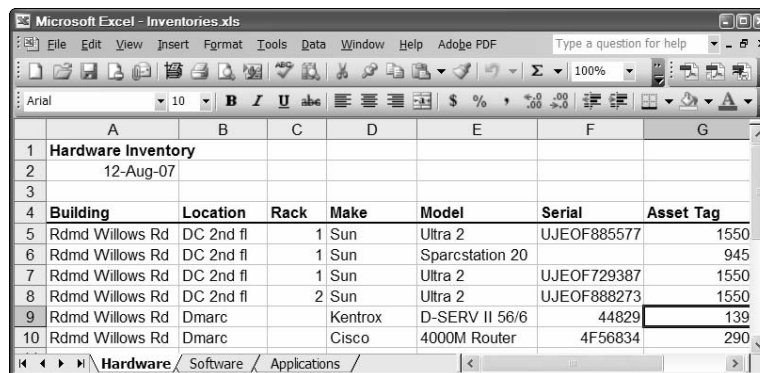
3. CONSTRUYENDO PLANES DE RECUPERACION DE DESASTRES

3.1.MAPEANDO FUNCIONES DEL NEGOCIO A LA INFRAESTRUCTURA

Se debe conocer los principios y procedimientos relacionados con esta asignación de planes de recuperación ante desastres porque son aplicaciones de negocio basadas en procesos. Alinear determinados planes de recuperación ante desastres para los procesos de la empresa. Sistemas de TI no hacen el negocio, los procesos de negocio. Es necesario comprender perfectamente que los sistemas de información dan soporte los procesos de negocio.

COMO ENCONTRAR Y USAR INVENTARIOS

- **Inventario de activos de hardware:** Las partes y piezas de su infraestructura. Todos sus servidores, routers, firewalls y otros componentes físicos. Es necesario conocer su estado o condición, de cada uno y clasificar adecuadamente - por ejemplo, como activos o inactivos, producción o prueba. También obtener la marca, el modelo, número de serie, y la

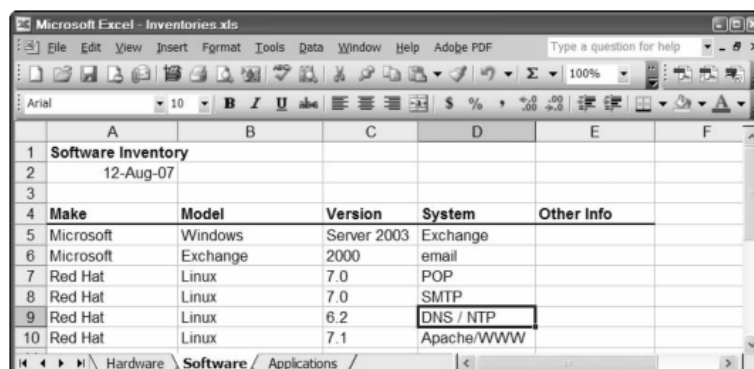


	A	B	C	D	E	F	G
1	Hardware Inventory						
2	12-Aug-07						
3							
4	Building	Location	Rack	Make	Model	Serial	Asset Tag
5	Rdmd Willows Rd	DC 2nd fl	1	Sun	Ultra 2	UJE0F885577	1550
6	Rdmd Willows Rd	DC 2nd fl	1	Sun	Sparcstation 20		945
7	Rdmd Willows Rd	DC 2nd fl	1	Sun	Ultra 2	UJE0F729387	1550
8	Rdmd Willows Rd	DC 2nd fl	2	Sun	Ultra 2	UJE0F888273	1550
9	Rdmd Willows Rd	Dmarc		Kentrox	D-SERV II 56/6	44829	139
10	Rdmd Willows Rd	Dmarc		Cisco	4000M Router	4F56834	290

ubicación (habitación, rack, lo que sea), como se muestra en la imagen.

No olvidarse de los componentes de red, cables, fibra, y así sucesivamente.

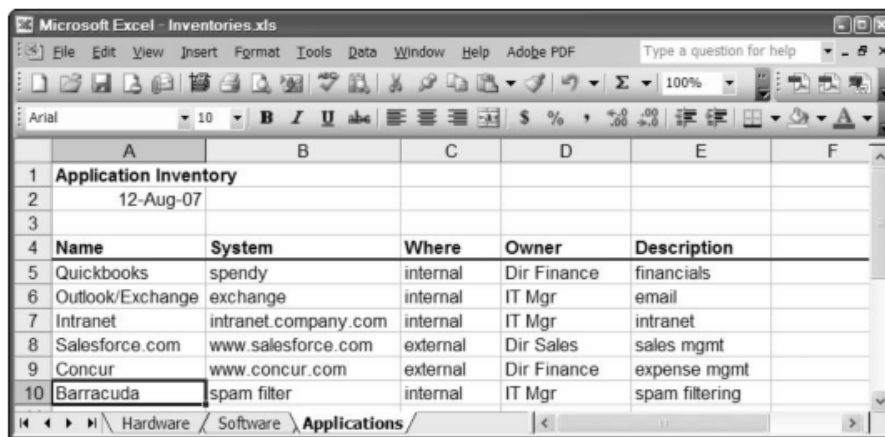
- **Inventario de software:** Saber desde donde se están ejecutando programas. Al pasar por los servidores, tenga en cuenta los componentes importantes que se están ejecutando en cada uno. Indicar la versión, nivel de parche, que servidor se está ejecutando y otros puntos de datos que tienen sentido



	A	B	C	D	E	F
1	Software Inventory					
2	12-Aug-07					
3						
4	Make	Model	Version	System	Other Info	
5	Microsoft	Windows	Server 2003	Exchange		
6	Microsoft	Exchange	2000	email		
7	Red Hat	Linux	7.0	POP		
8	Red Hat	Linux	7.0	SMTP		
9	Red Hat	Linux	6.2	DNS / NTP		
10	Red Hat	Linux	7.1	Apache/WWW		

(como las principales opciones de configuración, ubicación de medios, y así sucesivamente).

- **Las aplicaciones de negocios:** Hablar con los jefes de departamento (o sus delegados) para averiguar qué aplicaciones internas y externas de sus departamentos utilizan. Pregunta cómo acceder y conectarse a estas aplicaciones. Con esta información, se puede comenzar a trazar las aplicaciones



	A	B	C	D	E	F
1	Application Inventory					
2	12-Aug-07					
3						
4	Name	System	Where	Owner	Description	
5	Quickbooks	spendy	internal	Dir Finance	financials	
6	Outlook/Exchange	exchange	internal	IT Mgr	email	
7	Intranet	intranet.company.com	internal	IT Mgr	intranet	
8	Salesforce.com	www.salesforce.com	external	Dir Sales	sales mgmt	
9	Concur	www.concur.com	external	Dir Finance	expense mgmt	
10	Barracuda	spam filter	internal	IT Mgr	spam filtering	

empresariales a hardware y software activos.

USANDO ARQUITECTURA DE ALTO NIVEL

Uno de los pequeños secretos sucios en muchas organizaciones es la falta de arquitectura de alto nivel - los diagramas de cajas y flechas que lógicamente representan sistemas y datos en una organización o entre varias organizaciones. Estos diagramas, que a menudo van acompañados de listas de componentes y/o especificaciones, muestran la relación entre los componentes y capas de un entorno de aplicación.

Diagramas de flujo y de almacenamiento de datos

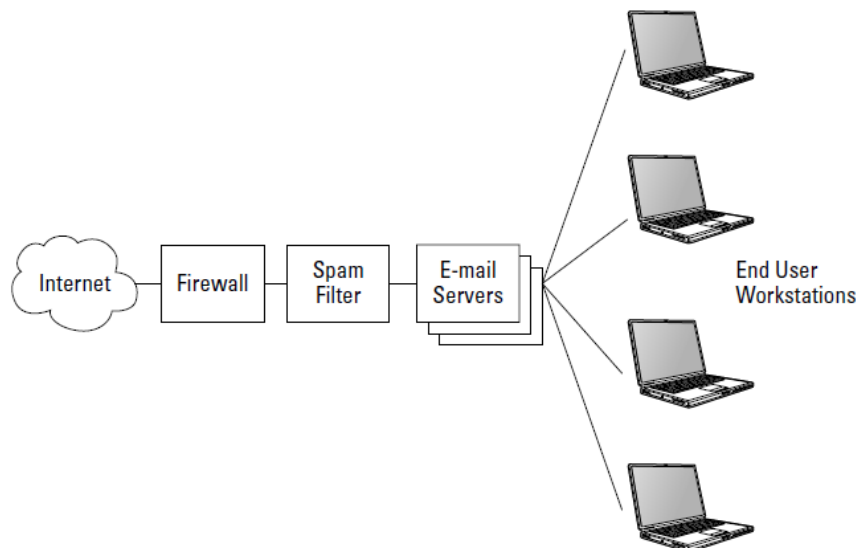
Diagramas de flujo de datos y de almacenamiento de datos que dan representaciones centradas en datos decididamente del flujo de información dentro de las aplicaciones y entre aplicaciones. En casi todos los casos, las aplicaciones de recibir, almacenar, enviar, y reportar información. Obtener una visión centrada en los datos de una aplicación puede ayudar a usted, el planificador de DRP, entender mejor cómo funciona la aplicación y cómo apoya los procesos de negocio, así como que le proporciona. Los sistemas que contienen información y cómo la información se mueven entre sistemas. Si quieres desarrollar planes para la recuperación de negocio vital y crítico procesos, que tienen que saber que los sistemas de apoyo a

estos procesos y cómo esos sistemas y procesos están interconectados. Sin este conocimiento, no se puede desarrollar planes de DRP que ayudan a recuperar los sistemas que soportan estos procesos - y si no se admiten esos procesos, que permanecen ociosos, poniendo la supervivencia del negocio en riesgo. A partir de la gran imagen a menudo le proporciona una ruta de acceso a la identificación de detalles. En otras palabras, después de ver el panorama completo, puede seleccionar las partes del cuadro grande y explorar los detalles acerca de cómo las aplicaciones específicas de trabajar y son compatibles.

Primer ejemplo: Entorno de E-mail

Esta sección habla de un ejemplo sencillo de flujo de datos en el correo electrónico de la aplicación Outlook, que utilizan muchas empresas.

La Figura de abajo muestra el flujo de información a través de únicos de componentes principales. Por ejemplo, el correo electrónico que fluye entre el servidor de correo y el Internet va a través del filtro de firewall y el spam que aparecen en el diagrama, pero se puede ver en la mayoría de los dispositivos de red que en el camino no aparecen en el diagrama, incluyendo uno o más routers, conmutadores y dispositivos de seguridad. Pero para el propósito de e-mail, los otros



dispositivos de red son extrañas - son sólo la fontanería.

Diagramas y esquemas de infraestructura.

Diagramas de Infraestructura, a menudo conocidos como esquemas, son de abajo hacia arriba. Diagramas de infraestructura son los esquemas (o diagramas) que muestran cada pieza y parte en un entorno.

Entrevista a expertos en la materia

Comenzar a poner junto el esquema general de la infraestructura entrevistando la red y los ingenieros de sistemas, y obtener cada tipo de información con el fin de averiguar cómo se armó el entorno. En todos menos en los entornos más simples, es probable que se encuentre uno o dos anomalías, tales como:

- **Conflictos:** Ted dice algo es poner juntos de esta manera, pero Bill dice que es hecho de otra manera. Lo que realmente importa es la verdad: ¿Cómo funciona realmente? Si te encuentras con un conflicto de este tipo, alguien tiene que ayudar a los expertos decidir necesitas encontrar un experto.
- **Brechas:** Usted puede encontrar una parte del entorno de red o sistemas que nadie conoce. Tal vez la persona que lo construyó no es de alrededor de cualquier más tiempo, él o ella no escribió ninguna documentación al respecto, y nadie más ha molestado en averiguarlo.

Uso de Redes y Herramientas de Gestión de Sistemas

Alguien en el grupo de TI puede tener herramientas, tales como la detección de redes o herramientas de mapeo, que proporcionan alguna información de la arquitectura de red que se puede utilizar como punto de partida. Estos son algunos ejemplos de los tipos de análisis herramientas de mapeo que dará una idea de la arquitectura de la red:

Herramientas de Alta Gama:

- **HP OpenView: Caro**
Herramienta de nivel empresarial. Si su organización ya lo tiene, una de las personas que lo usan deben ser capaces de conseguir que algunos mapas de la red.
- **IBM NetView:**
Una herramienta de gestión de red con todas las funciones de alta gama.
- **Sun Solstice Enterprise Manager:**
Una para entornos de alta gama.
- **LANsurveyor:**
Una herramienta de mapas y diagramas de red en tiempo real.
- **netViz:** Una herramienta de visualización de la red.

Herramientas menos costosas / gratis: Estas herramientas proporcionan alguna funcionalidad básica para diagramar las redes:

- **Network Magic:**
Una estación base de herramienta que incluye diagramas y otras funciones.
- **Cheops:**
Herramienta gratuita para la asignación y supervisión de una red.
- **FreeMap:**
Esta herramienta gratuita se ejecuta desde una ubicación central, de forma que la red debe ser accesible a través de la Internet.

IDENTIFICAR LAS DEPENDENCIAS

- **Entrevistas:** Identificación de expertos en la materia y hablar con ellos sobre los sistemas, las redes y las aplicaciones. En concreto, preguntarse qué interno (en el sistema), interno (de la organización), y dependencias externas existen entre dispositivos, sistemas y aplicaciones.
- **Configuraciones:** Puede usted o alguien con privilegios administrativos necesitar examinar las configuraciones de los sistemas, dispositivos y aplicaciones, e identificar servicios externos, sistemas, dispositivos, y así sucesivamente.
- **Herramientas y aplicaciones de gestión:** Es posible que su organización ya está utilizando herramientas y aplicaciones para configurar y administrar sistemas y dispositivos. Por ejemplo, usted podría tener una base de datos de gestión de configuración (CMDB) y aplicación complementaria que se utiliza para administrar dispositivos, sistemas y/o aplicaciones de la organización.

Interdependencias de Sistemas

- Dependencias de Sistemas.
- Dependencias de Comunicaciones.
- Dependencias de Servicios de Redes.
- Dependencias de Gestión de Servicios.
- Dependencias de Seguridad.
- Dependencias de Aplicaciones.

Dependencias del sistema

- **Configuración de hardware:** Los fundamentos - la cantidad de memoria, espacio en disco, otros componentes, y también CMOS / BIOS y otra a nivel de hardware configuraciones de cada sistema contiene.
- **Opciones de arranque:** ¿Es necesario que cada servidor o cualquier configuración de arranque no están predeterminados opciones para que funcione correctamente? ¿Puede arrancar el servidor desde una imagen en una SAN (Storage Area Network) u otro almacenamiento en disco externo?

Dependencias de Comunicaciones

- **Configuración de la red:** Algunos de los ajustes que pueden importar incluyen la configuración del servidor DHCP, servidores DNS, la máscara de subred, puertas de enlace, entradas de la tabla de enrutamiento, y así sucesivamente.
- **Host-a-host Communication:** Por ejemplo, es IPsec o GRE túnel, o SSH, establecido entre los hosts?
- **Fibre Channel SAN:** La configuración de las comunicaciones a una Red de área de almacenamiento (SAN) puede ser crítico en algunos sistemas.

Dependencias de Servicios de Redes

- **Gestión de la identidad:** las cuestiones de gestión de identidad si el sistema autentica a los usuarios mediante el uso de un servicio basado en la red. El sistema debe ser configurado para conectarse correctamente al servicio correcto de la manera correcta.
- **Autenticación de dos factores:** Aunque la autenticación es técnicamente una parte de gestión de identidad, vale la pena mencionar en su propia bala porque por lo general tienen una infraestructura separada involucrada.
- **E-mail:** ¿Qué organización no tenerlo? Las aplicaciones críticas a menudo dependerán de e-mail para comunicar el estado de los usuarios e incluso a veces para transferir datos entre aplicaciones.
- **Servicios Web:** interfaces de aplicaciones a base de SOAP (Simple Object Access Protocol, y también Service-Oriented Architecture Protocol) y otras tecnologías.

Dependencias de Gestión de Servicios

- **Agentes para la gestión de parches:** Sistemas de gestión de parches, requiere un agente en cada sistema con el fin de detectar adecuadamente la presencia de parches de software.
- **Agentes para la Gestión de la Capacidad:** Cuando la memoria y discos duros del sistema se encuentren bajos, se envía alertas o mensajes a una gestión consola.
- **Agentes para la gestión de alertas:** Cuando el sistema experimenta un error (tales como fallas en el servicio o de hardware), se envía capturas a una consola de administración

Dependencias de Seguridad.

- **Firewall:** crítica en algunos entornos, una gran idea en otros. Protege las aplicaciones de tráfico de red no deseado, incluyendo el tipo de tráfico que pueden hacer que una aplicación (o servicio) uso incorrecto o no.
- **Anti-virus:** Es posible que su aplicación no requiere un programa anti-virus, sino simplemente tratar de convencer a los demás de que es innecesario.
- **IDS/IPS (Intrusion Detection System/Intrusion Prevention System):** a bordo de IDS, que generalmente se ejecuta como una especie de servicio, o el suplemento en la pila de protocolos TCP/IP. Se pone a la lista en el tráfico de red y alertas sobre anomalías.
- **Gestión de Integridad:** Herramientas como Tripwire puede estar presente y esencial para la seguridad y la gestión de la calidad.
- **Infraestructura de clave pública (PKI):** La aplicación puede depender de servicios externos las claves de cifrado que puede ser en un servidor de claves o un aparato

Dependencias de Aplicaciones.

- **Fuentes de Datos:** Una aplicación puede requerir un continuo (o lotes) de las transacciones de otras aplicaciones con el fin de funcionar correctamente (o simplemente evitar resultados nulos).
- **Interfaces:** a menudo, las aplicaciones comunicarse entre sí en tiempo real con el fin de funcionar correctamente.

Las dependencias externas

- **E-mail:** La omnipresente plataforma de mensajería para el transporte no sólo mensajes, sino también datos entre las entidades.
- **Las comunicaciones de voz:** Ah sí, las personas deben ser capaces de comunicarse entre sí a través de voz. No siempre vinculadas directamente a las aplicaciones, pero a menudo vinculados directamente a los procesos.
- **Fax:** como las comunicaciones de voz, las comunicaciones por fax puede ser esencial o incluso crítico para la recuperación de los procesos de negocio.
- **Servicio de nombres de dominio (DNS):** Es absolutamente necesario para cualquier comunicación de red. Traduce los nombres de dominio DNS (como www.avaya.com) las direcciones IP que sistemas que utilizan para comunicarse entre sí.
- **World Wide Web:** a veces es necesario por las aplicaciones, a menudo por la gente, y a veces en la ruta crítica de los procesos vitales de su negocio.

- **Identidad federada:** Algunos entornos utilizan identidad federada para gestión de perfiles de usuario. Es necesario entender la arquitectura de datos y flujos de datos si su organización utiliza identidad federada.
- **PKI:** Sus aplicaciones o infraestructura de apoyo podría depender de una clave externa proveedor de servicios de cifrado, descifrado o verificación de los datos.
- **Traductores En Línea:** Algunas organizaciones que tengan componentes en muchos idiomas utilizan traductores de idiomas en línea externa para comprender sus mensajes entrantes o salientes para traducir.
- **Los proveedores de servicios externos:** Las funciones que utilizan las aplicaciones de los proveedores de servicios externos, como Salesforce.com y Winweb, podrían estar en la ruta crítica de las aplicaciones internas y servicios.

3.2. PLANIFICACIÓN DE RECUPERACIÓN DE USUARIOS

Las personas son una parte esencial de todos los procesos de negocio críticos. Incluso los procesos de negocio pronto romperán el mito, sin intervención humana, orientación e intervención.

Recuperar los usuarios supone recuperar los puestos de trabajo y su capacidad para comunicarse con las personas de dentro y fuera de su organización. Usted tiene que analizar muchos de los detalles para comprender el papel de los usuarios finales de las estaciones de trabajo y necesidades de comunicaciones en los procesos de negocio críticos.

ADMINISTRACIÓN Y RECUPERACIÓN INFORMÁTICA DE USUARIO FINAL

Las personas desempeñan un papel fundamental en el funcionamiento de los procesos de negocio. Cada vez más, la gente es parte de procesos de negocio implica el uso de equipos de sobremesa o portátiles. La Informática de usuario final varía ampliamente, dependiendo de las tareas que cada empleado realiza durante su jornada laboral. Algunos ejemplos incluyen:

- Cómo utilizar el correo electrónico para enviar y recibir las notificaciones de las aplicaciones y otros usuarios.
- Acceso a Internet de la empresa.
- Las aplicaciones basadas en Web para acceder a aplicaciones externos.
- El acceso a las aplicaciones cliente/servidor.
- Acceso y trabajar con documentos en los servidores de archivos.
- Acceder a documentos dentro de la estación de trabajo.

Estaciones como Terminales Web

Desde el punto de vista de Recuperación de Desastres, el más fácil de recuperar función en las estaciones de trabajo del usuario final como terminales, sobre todo si las funciones del terminal utilice los componentes nativos, tales como software de navegador Web. Pero incluso en este caso simple, existen varios factores de consideración.

Plug-ins de Aplicaciones

Sólo por el hecho de que usted tenga acceso a uno o más de sus aplicaciones críticas a través de la Web los navegadores no significan que su planificación para la recuperación de desastres va a ser gratis. Cuando usted está de mapas de todas las piezas móviles y piezas de un extremo a otro entorno de la aplicación, es necesario identificar todas Web browser plug-ins que las aplicaciones Web para funcionar correctamente.

Algunos ejemplos de aplicaciones Web incluyen, pero no son limitadas a, las siguientes:

- **Adobe Acrobat:** Para leer los archivos PDF.
- **Apple Quicktime:** reproducir clips de vídeo y audio.
- **Adobe Flash:** Para mostrar las páginas Web de contenido Flash.
- **Shockwave:** Para mostrar las páginas Web de contenido Shockwave.
- **Windows Media Player y otros reproductores multimedia:** Para reproducir los vídeos y clips de audio.
- **Los visores de documentos:** Para ver los documentos, hojas de cálculo, presentaciones, proyectos, dibujos técnicos, etc.
- **Máquina virtual de Java (JVM):** Para ejecutar applets de Java.
- **Complementos personalizados:** Desarrollado por la organización o por un tercero.

Administrar aplicaciones web Híbridas

Algunas aplicaciones basadas en la Web y tienen código que trae en contenido y funciones de un montón de aplicaciones diferentes al mismo tiempo. Las aplicaciones web híbridas utilizan APIs (Interfaces de programación de aplicaciones - Las formas de obtención de la información dentro de otro programa) de diversos sitios de la Web, en la que se mezclan código de estas diferentes fuentes, con el objetivo de crear el resultado visto en la ventana del navegador. Aquí están algunos ejemplos de combinaciones interesantes visualmente:

Acceso a Estación Central de Información

Una razonable organización promueve (si no es necesario) que los documentos, hojas de cálculo y otros archivos se almacenan de forma centralizada en servidores, en lugar de centrarse exclusivamente en las estaciones de trabajo del usuario.

Las estaciones de trabajo que funcionan como terminales para acceso al Internet, los clientes de aplicaciones distribuidas, independiente y plataformas informáticas también necesitan acceso a información centralizada, a menudo en forma similar y que requieren algunas características comunes y los servicios para hacerlo.

Los tipos de servidor requieren incluir estaciones de trabajo de acceso a:

- Servidores de archivos y de impresión.
- Servidores Web.
- Servidores de aplicaciones.

1. Acceder a los servidores de archivos e impresión

Los principales temas relacionados con servidor de archivos y de impresión acceso:

- **Mapping:** Sí a través de Windows drive mapping, accesos directos y enlaces, Samba, o NFS (Network File System), las estaciones de trabajo de los usuarios finales requieren información de configuración para que pueda encontrar el servidor.
- **Autenticación:** Los usuarios deben autenticarse para la red, o directamente a los servidores, a fin de acceder a los archivos e impresoras.
- **Controles de acceso:** Servidores de archivos y de impresión utilice controles de acceso que determinan qué usuarios pueden tener acceso a directorios, archivos e impresoras.
- **Servicio de Directorio:** Las aplicaciones deben tener servicio de nombres de dominio (DNS) o del Servicio de nombres Internet de Windows (WINS) para las estaciones de trabajo de los usuarios pueden localizar los sistemas de la red corporativa, por ejemplo, servidores de aplicaciones, servidores de archivos y servidores de impresión, así como los sistemas de Internet.

0. Acceder a Servidores Web

- **Autenticación:** a menudo los usuarios necesitan estar autenticada para redes y/o aplicaciones con el fin de acceder al contenido en los servidores Web.
- **Controles de acceso:** servidores Web que utilizan controles de acceso para determinar qué usuarios y grupos tienen permiso para acceder a la información específica en el servidor Web.
- **Servicio de Directorio:** Estaciones necesidad servicio de nombres de dominio (DNS) para que ellos puedan encontrar servidores Web en la red.

0. Acceso a servidores de aplicaciones

- **Autenticación:** Las aplicaciones deben saber quién está solicitando acceso. Por lo general, el componente del cliente recopila las credenciales de usuario y los pasa a la aplicación, lo que, a continuación, debe consultar una base de datos interna o una autenticación basada en la red de servicio para validar el usuario.
- **Servicio de Directorio:** Estaciones necesidad servicio de nombres de dominio (DNS) para usuario final estaciones de trabajo puede encontrar servidores y otros recursos de la red.

0. Notas de Recuperación de acceso a estación central de información

- Configurar DNS y/o WINS para las estaciones de trabajo del usuario final puede encontrar estos servidores en la red.
- Incluye servicio de autenticación de red para que los usuarios puedan identificar a los servidores y a otros recursos.

- Que todo el conjunto de permisos de control de acceso de servidores sea fácilmente recuperable y transferibles a los servidores de reemplazo para los mismos controles de acceso que protegen la información en un entorno de recuperación.
- Regularmente copias de seguridad de los servidores, o replicar los datos en servidores remotos, para que pueda recuperar los datos en caso de desastre.
- Establecer una red a la que se ha repuesto diferentes dirección de IP (Protocolo de Internet) y numeración diferente con arquitectura lógica y física para que pueda transferir todo el conjunto de la estación de interacción con el servidor si es necesario.
- Cuenta con un gran ancho de banda las interacciones entre los servidores y estaciones de trabajo para optimización. En un entorno de recuperación, los servidores y estaciones de trabajo pueden estar separados por distancias considerables y/o redes lentas.

Las estaciones de trabajo como Aplicación Cliente.

La informática ha revolucionado a principios de la década de 1990 gracias a la liberación de recursos valiosos en computadoras centrales y el movimiento de la interfaz de usuario lógica fuera de las estaciones de trabajo de los usuarios finales que había relativamente amplio poder de computación. Muchas organizaciones pusieron en marcha las aplicaciones cliente/servidor, y muchas de estas aplicaciones están todavía en uso hoy en día.

A menudo, software cliente/servidor tiene varios componentes de cliente, incluyendo:

- **Software de Base:** Software instalado en los servidores de aplicaciones.
- **Aplicaciones en el lado del cliente lógica de negocios:** Software instalado en las estaciones de trabajo.
- **Datos de Configuración:** Opciones que determinan cómo base de software y software de cliente para comunicarse con los demás.
- **Parches:** correcciones y actualizaciones realizadas en el software base y software de cliente desde instalación inicial.

1. Software Cliente/servidor

Algunas de las preguntas y cuestiones sobre cliente/servidor software de base:

- **Instalación:** ¿Puede hacer que el software de base sea parte de la imagen de la estación?, ¿Puede instalar automáticamente, a través de la red? , Para instalar el software, ¿Es una necesidad introducir un código de licencia o los datos de configuración?
- **Disponibilidad:** ¿Es la versión que está usando todavía disponible para el público en general?
- **Liberación/medios de instalación:** ¿tiene versión portátil o medios de instalación para el software?
- **Compatibilidad con las últimas versiones de sistemas operativos:** ¿el software básico trabaja con las versiones más recientes de Windows y otros sistemas operativos?

0. Cliente de Lógica de Negocios

Las aplicaciones de cliente/servidor tienen algunos códigos de aplicación que se ejecuta en el servidor y algunos en el cliente. En el lado del cliente, el software está instalado y actualizado de alguna manera. Puede utilizar algunos de los siguientes mecanismos para obtener software de cliente en la estación de trabajo:

- Escrito (y, opcionalmente, compilado) por un desarrollador e instalados a través de un mecanismo de actualización dentro del entorno cliente/servidor.

- Escrito por un desarrollador y la instalación de un mecanismo de actualización, tales como Microsoft SMS (Systems Management Server).
- Escrito por un desarrollador e instalar manualmente por el personal de TI, ya sea en persona o a través de una Internet (o intranet) conexión.

0. Lógica de Negocios del Lado del Cliente

En el lado del cliente, el software está instalado y actualizado de alguna manera. Se puede utilizar algunos de los siguientes mecanismos para obtener software de cliente en la estación de trabajo:

- Escrito (y, opcionalmente, compilado) por un desarrollador e instalados a través de un mecanismo de actualización dentro del entorno cliente/servidor
- Escrito por un desarrollador e instalado por separado en un mecanismo de actualización, tales como Microsoft SMS (Systems Management Server).
- Escrito por un desarrollador e instalado manualmente por el personal de TI, ya sea en persona o a través de conexión de Internet (o intranet).

0. Configuración de los Datos del Lado del Cliente

- Nombre del servidor.
- Número de puerto que se debe usar cuando se comunica con el servidor.
- Configuración de la autenticación.
- Parámetros de comportamiento, tales como opiniones iniciales.
- Usabilidad, como colores y fuentes.

Algunos de estos valores son esenciales para la función básica de la aplicación, pero otros son más para comodidad del usuario y sus preferencias. Todos los valores de configuración de la lista anterior, excepto para la usabilidad, puede determinar las funciones de la aplicación.

0. Parches del Lado Cliente

Considere los siguientes parches de software cliente:

- ¿El entorno cliente/servidor usan parches en el nivel de la aplicación?
- ¿Se puede usar una vista de gestión para determinar los clientes que tienen que parches instalados?
- ¿Está bien documentado el registro histórico de los parches?

Las respuestas a las preguntas de la lista anterior nos indican cómo realizar las actualizaciones de software por parte del cliente, así como determinar qué parches son en las estaciones de trabajo cliente.

Recuperación de las estaciones de trabajo como clientes de aplicación

La siguiente lista le dará alguna preparación específica y las acciones de recuperación que se pueden tomar para obtener las estaciones de trabajo de los usuarios finales que tienen software de cliente/servidor en el aire:

- **En la mayor medida de lo razonablemente posible, utilizar configuraciones estándar para las estaciones cliente/servidor.** Configuraciones estándar también ayudan a reducir los costes de soporte. Asegúrese de que las configuraciones estándar incluyen todos los componentes necesarios, a partir de base de software en el código de la aplicación y de la configuración del sistema operativo y lo que se requiere para la compatibilidad con el software.
- **Utilizar tecnología de creación de imágenes y herramientas que pueden ayudarle a crear rápidamente de las estaciones cliente/servidor.** Prueba tus imágenes en una gran variedad de estaciones: En una situación de desastre, es posible que se tenga que construir estaciones de trabajo en las plataformas de hardware que no trabajan de forma rutinaria.
- **Considerar un entorno de cliente ligero, con software de cliente/servidor instalado en servidores, lo que reduce a las estaciones terminales inteligentes.** Tecnología Thin-client como, por ejemplo, Citrix, permite a la organización a centralizar software de cliente instalación, configuración y mantenimiento.
- **Copia de seguridad de imágenes de los sistemas para estaciones de trabajo.** Se pueden recuperar los sistemas de imagen en un desastre, se pueden utilizar para construir nuevas estaciones cliente/servidor, según sea necesario.

Estaciones de Trabajos como Equipos Locales

Muchos de los trabajadores de la empresa que utilizan sus estaciones de trabajo para crear y administrar documentos, hojas de cálculo, presentaciones, dibujos técnicos y planes de proyecto. Estaciones de trabajo pueden tener herramientas de software adicionales para el desarrollo y prueba de aplicaciones, análisis de datos y la elaboración de modelos, modelado gráfico, análisis estadístico, y quién sabe qué más.

A menudo, los usuarios almacenan los datos (los archivos o bases de datos que se crean y utilizan) localmente en la estación de trabajo, especialmente cuando la estación de trabajo es un ordenador portátil. Tiene que decidir si utilizar estos programas es verdaderamente fundamental para procesos de negocio específicos o si las estaciones de trabajo de los usuarios finales son más accesibles a estos procesos.

La gestión y recuperación de las estaciones de trabajo como equipos locales tienen tres aspectos importantes:

- **Programas:** Los programas de aplicación que se utiliza para crear y gestionar los documentos y datos.
- **Datos:** Los datos que los usuarios crean y trabajar con ellos en sus estaciones de trabajo.
- **Procedimiento:** Documentos sobre el uso de los programas locales, en términos de su apoyo a los procesos de negocio críticos.

Sistemas Operativos de Estaciones de Trabajo

Los Sistemas operativos de estaciones de trabajo. Ya sea de Windows, Linux, Mac OS o cualquier otra cosa, es el corazón de las estaciones de trabajo del usuario final, no importa si son usados como terminales Web inteligente, la computación distribuida los clientes, las plataformas informáticas, o todas las anteriores.

Esta lista incluye los aspectos principales del sistema operativo de la estación que requieren atención para fines de recuperación:

- Plataforma de hardware.
- La versión del sistema operativo.
- La configuración y los niveles de parches.
- La conectividad de red.
- La autenticación.
- La autenticación se restablece durante un desastre.
- Seguridad.

Conectividad de red para sistemas operativos de estación

Es necesario comprender los métodos de conectividad de la red en uso en la organización, independientemente de la función de la estación. Los navegadores Web y las aplicaciones deben ser capaces de comunicarse con sistemas dentro de la empresa y, posiblemente, en el mundo exterior.

- **Control de acceso a la Red:** ¿sus aplicaciones objetivas limitan el acceso a direcciones de IP específicas o rangos de IP? Si es así, es posible que tenga que volver a configurar para su recuperación todavía puede conectar las estaciones, incluso si están conectadas a nuevas, redes temporales.
- **Acceso remoto/Red Privada Virtual (VPN):** Son las aplicaciones y servidores de acceso remoto a través de cualquier acceso o servicio VPN? Si no, puede haber muy pocas opciones de recuperación debido a que puede ser necesario ubicar temporalmente los usuarios lejos de recuperar el entorno del servidor.
- **Acceso a múltiples servidores:** ¿Sus aplicaciones requieren acceso simultáneo a varios servidores de aplicaciones?

Autenticación para sistemas operativos de estación

- **ID de usuario y la contraseña:** bastante fácil, en la mayoría de los casos. **Biometría:** Generalmente requiere hardware extra, como escáneres de huellas digitales. Si los empleados iniciar sesión en las aplicaciones que requieren autenticación biométrica.
- **Smart card:** De manera similar a los datos biométricos, tarjetas inteligentes de autenticación requieren hardware, la mayoría de los puestos no tienen. **Contraseña de una sola vez:** a menudo, las contraseñas de un solo uso en forma de fichas y dispositivos similares. Aunque puede que los usuarios todavía tienen sus fichas en una situación de desastre, el token de infraestructura de autenticación no puede todavía estar en funcionamiento.
- **Una sola identidad y el inicio de sesión único:** Algunas aplicaciones basadas en Web dependen de servicios centralizados para administrar la autenticación.

Autenticación se restablece durante un desastre:

- **Contraseña Vía Email:** A menudo, las aplicaciones pueden enviar por correo la contraseña existente, una nueva contraseña temporal, o una nueva contraseña permanente a un usuario que ha perdido su contraseña. Por esta asistencia contraseña el trabajo, el usuario tiene que tener acceso al correo electrónico.
- **Las contraseñas a través de live support:** En muchos casos, los usuarios pueden llamar a un servicio de asistencia técnica para obtener sus contraseñas. Por supuesto, es necesario tener un personal helpdesk disponible en una situación de desastre para que este enfoque funcione.

Seguridad del sistema operativo de la estación

- **Configuración de seguridad:** Las configuraciones de seguridad en cada capa de la pila estación - deben tener contraseñas de BIOS (hardware las claves necesarias para iniciar el equipo) para autenticación de la aplicación, y en muchos lugares, permiten la recuperación si se configura correctamente.
- **Claves Encriptadas:** Puede utilizar el cifrado en muchos lugares, incluyendo cifrado de archivos, cifrado de mensajes de correo electrónico, sesiones (comunicaciones) cifrado, encriptación de datos, tales como las tarjetas de crédito y contraseñas, y el cifrado de discos duros de la estación entera. Cuando se trabaja para recuperar las capacidades de procesamiento, que a menudo es necesario para recuperar las claves de cifrado original para facilitar la continuidad de los procesos.

- **Certificados digitales:** Se debe utilizar certificados (que son muy semejantes a las claves de cifrado) para el cifrado, firmas digitales y autenticación. Y como las claves de cifrado, con frecuencia no se puede simplemente crear un nuevo certificado mejorado para acceder a los datos almacenados en los certificados antiguos.

ADMINISTRACIÓN Y RECUPERACIÓN DE LAS COMUNICACIONES DE USUARIO FINAL

Las comunicaciones de voz.

- Simple teléfono de marcado directo.
- Empresa telefónica PBX basado (centralitas, anteriormente conocido como Centrex - una manera elegante de decir de un sistema telefónico), en la que la compañía telefónica local administra las extensiones de discado directo para una empresa.
- PBX analógicas o digitales conectados a analógica o digital las extensiones
- IP-PBX basado conectado a digital o teléfonos basados en IP, o se conecta mediante marcación softphones a través de redes de cable o inalámbricas.

E-mail

Aspectos de los mensajes de correo electrónico de los proyectos de RECUPERACIÓN ANTE DESASTRES que necesitan abordar incluyen:

- Correo de Clientes.
- Servidores de correo electrónico.
- Las puertas de enlace de correo electrónico para el mundo exterior.
- Pasarelas de correo electrónico e interfaces a aplicaciones internas.
- Seguridad de correo electrónico

El Correo de Clientes. En la mayoría de las arquitecturas, los usuarios que envían y reciben mensajes de correo electrónico utilizando software de cliente que se ha instalado en las estaciones de trabajo. Este software proporciona la interfaz de usuario con el que los usuarios leen, crean y envían mensajes de correo electrónico, y a menudo también almacenan de forma local los mensajes de correo electrónico. Algunas cuestiones a tener en cuenta acerca de los correos electrónicos de clientes incluyen:

- Configuración
- Almacenamiento de Correo electrónico Local.
- Lista de Direcciones
- Filtros y regla de reenvío.

Servidor de Correo

Servidores de correo electrónico reciben, almacenan y envían los mensajes de correo electrónico a y desde otros servidores de correo electrónico y los usuarios. Las grandes organizaciones tienen varios servidores de correo electrónico, con una porción de la mano de obra asignada a cada servidor. Uno de estos servidores de correo electrónico también pueden enviar y recibir correo de entidades externas y de la Internet, o servidores independientes puede ser dedicado a este fin.

Las puertas de enlace de correo electrónico y conexión a Internet

Además de transmitir mensajes de correo electrónico entre usuarios dentro de una organización, los usuarios también pueden enviar un correo electrónico a los destinatarios que se encuentran fuera de la organización. Y el correo electrónico de fuentes externas llega para su entrega a los destinatarios locales.

Hay varias cuestiones a considerar en relación con los servidores de correo electrónico:

- **Configuración.** Las configuraciones de puertas de enlace y otros sistemas que procesan e-mail permitir hacer su trabajo correctamente.
- **Almacenamiento Local.** A menudo, estas puertas almacenan los mensajes, por lo general, aunque no siempre temporalmente, mientras que aquellos mensajes esperan a ser transmitidas a sus destinos finales.

Recuperación de correo electrónico.

- Saber cómo fluye el correo electrónico en, alrededor, y fuera de la organización, incluidos servidores, clientes, puertas, y así sucesivamente. Documentar todos los hechos de su organización en el registro de nombres de dominio en la Internet, que incluyen registros MX que determinan dónde correo electrónico entrante de Internet debe ser entregada. La introducción de los cambios de su negocio el dominio los servidores deben estar preparados para cuando un desastre puede tomar un tiempo considerable.
- Todos los usos de rastreo e-mail a través de los procesos de negocio determinan las direcciones de correo electrónico, listas de distribución, las reglas de filtrado, y otras características que los mensajes de correo electrónico para llegar a sus destinos.

Máquinas de fax.

Muchas organizaciones todavía dependen en gran medida de facsímil (fax) para transmitir documentos comerciales, como contratos, recibos, facturas, etcétera. A pesar de que muchas organizaciones están haciendo la transición con el mundo de la imagen digital, las máquinas de fax son sin embargo esencial para muchos procesos clave de su negocio.

- **Directorios:** Personas que necesitan enviar faxes se necesita saber los números de teléfono destino. Capturar la imagen de su negocio de números de fax en proceso de documentación, si estos números no se han incluido.
- **Los números de fax:** Algunas organizaciones utilizan una amplia publicidad o números de fax. En caso de ocurrir un desastre, es posible que la organización necesite los faxes entrantes se deben enrutar a otra máquina de fax o servidor de fax.

Mensajería instantánea o IM

Es frecuentemente considerado como un ad hoc, contracultura, metro o herramienta de comunicación de las organizaciones. Sin embargo, muchas organizaciones utilizan MENSAJERÍA INSTANTÁNEA, y aunque no esté en la ruta crítica de los procesos de negocio, es muy útil para las comunicaciones informales, tales como:

- Hola, la llamada de conferencia ha comenzado.
- ¿Usted desea unirse con nosotros?
- ¿Dónde está?
- Mi programa de correo electrónico acaba de colapsar.
- ¿Cuál es el número de reunión en línea de hoy?

Aunque IM no podrían estar en la ruta crítica, que podría hacer uso del mismo durante un desastre puede ayudar a mantener los equipos. Considere estos consejos para recuperar mensajería instantánea:

- Publicar los miembros del equipo de respuesta de emergencia las direcciones de mensajería instantánea en listas de contactos de emergencia.
- No depende de un único proveedor IM, en caso que el proveedor está involucrado en el mismo desastre.
- Si su organización utiliza un servidor de mensajería instantánea centralizada, considere la posibilidad de establecer un servicio externo como una copia de seguridad.
- Si la organización utiliza servicios de mensajería instantánea sólo afuera, internalizar y hacer que esté disponible en situaciones de desastre.

3.3. PLANIFICACIÓN, PROTECCIÓN Y RECUPERACIÓN DE INSTALACIONES

PROTEGER LAS INSTALACIONES DE PROCESAMIENTO

El Procesamiento de la Información en las instalaciones son altas concentraciones de computadoras y equipo de apoyo en los procesos de negocio críticos. En una sola sala, prácticamente todo el equipo de una organización de los procesos críticos generalmente se apilan en racks de equipos especiales colocados uno al lado del otro, con masas de cables de alimentación y cables de red. Una sala de reducidas dimensiones, es decir 20 pies por 20 pies, puede ser crítico, 50,000 pies cuadrados de espacio de oficina con 250 trabajadores que utilizan los sistemas de información contenida en esa pequeña sala.

Los tipos de mecanismos para proteger el equipo incluye:

- Control de acceso físico.
- Energía Eléctrica.
- Detección y supresión de incendios.
- Riesgos de los Productos Químicos.
- Agua/inundaciones detección.

Controlar el acceso físico.

El alto valor de los sistemas de información - y el valor de los activos de los mismos, así como su apoyo a los ingresos de los procesos de negocio, con lo que la información de hoy necesita instalaciones de procesamiento similar a Fort Knox. Centros de datos son a menudo una organización de mayor concentración de la riqueza de producción de activos. Por lo tanto, el acceso a estos lugares se debe hacer de forma controlada, de modo que sólo el personal autorizado con una válida razón de negocio se les permita entrar y salir.

Controles de acceso físico previene los desastres provocados por el hombre de sabotaje y otros daños provocados o accidentales. Centros de datos a menudo emplean a varios controles de acceso físico que trabajen juntos para detectar y prevenir entrada no deseada por parte de personal no autorizado. Los controles más comunes son:

- Vigilancia de vídeo.
- Tarjeta-llave para Controles de entrada.
- Controles de entrada biométrica.
- Guardias de seguridad.
- Armarios de seguridad.
- El equipo las jaulas.

Carga de energía eléctrica

La electricidad es un elemento fundamental de los sistemas de información y equipos de apoyo. Los servidores y el equipo de la red se malogran cuando cualquiera de las comunes y no tan comunes anomalías eléctricas, incluyendo las caídas de tensión, subidas de

tensión, picos, transitorios, bajadas de tensión, ruido y fracasos totales.

Electricidad sucia, y también frecuentes cortes en el suministro eléctrico y apagones, no sólo causa paradas no programadas, sino que también pueden tener un efecto significativo en la esperanza de vida de los equipos.

Algunos Equipos para proteger la información:

- **Los controladores de potencia remoto:** Estos smart, con conexión a la red de tiras que de apagar y a cada bujía. Son muy útiles para controlar de forma remota en equipos de centros de datos (centros que están vacantes).
- **Fuente de alimentación ininterrumpida (SAI):** Es posible que no necesite uno grande, pero lo necesita. No sólo almacenar varios minutos de electricidad en baterías, sino que también (por lo general) filtrar toda la corriente sucia.
- **Los acondicionadores de línea:** un posible complemento a UPS, acondicionadores de línea suave de los golpes y las caídas de potencia de entrada.
- **Diversas fuentes de alimentación:** Para instalaciones críticas, considere la posibilidad de hacer que el servicio público que en dos alimentaciones separadas de potencia que ingresan al edificio desde extremos opuestos, se alimenten de diferentes subestaciones.

Detección y Supresión de Fuego

Detección precoz de incendios es fundamental en el tratamiento de la información. Si se puede identificar un incendio en sus primeras etapas, puede hacer frente a lo que antes se produce graves daños.

Detección de Incendios y Humo

Donde hay humo, hay fuego. El viejo refrán no está muy lejos de la verdad. Detección de incendios eficaz comienza con detectores de humo. Cuando el fuego se encuentra en sus etapas iniciales, puede emitir humo en cantidades muy pequeñas.

Las opciones de detección de incendios y humo son:

- **Barrera fotoeléctrica:** El humo se dispersa en el aire. Detectores fotoeléctricos de humo trabajo de detectar esta dispersión.
- **Ionización:** En una pequeña cámara de ionización, humo altera el proceso de ionización y activa la alarma.
- **Muestras de aire:** Una red de tuberías para muestras de aire en toda la planta absorbe el aire en forma centralizada y altamente sensible con cámara de muestreo. Para el diseño, esta configuración puede detectar fuego antes que otros tipos de detectores, ya que puede obtener un mayor muestreo de

calidad del aire con un solo dispositivo de muestreo realmente bueno en lugar de muchos menos costoso.

- **Temperatura:** Cuando el fuego se vuelve más activo, se calienta el aire a su alrededor. La Temperatura o la tasa de aumento de los sensores detectan los cambios de temperatura.

Las alarmas de incendio y evacuación

Porque la vida humana y la seguridad son las principales preocupaciones en cualquier situación de desastre, las alarmas de incendio deben ser adecuadamente diseñado y mantenido para que el personal sepa cuando se produce un incendio y cómo evacuar rápidamente las instalaciones. También es necesario y de señales de salida, por supuesto, están para ayudar a la gente a encontrar la manera de salir de un edificio cuando las alarmas han saltado.

Supresión de incendios

Cuando el fuego se ha iniciado en el centro de datos de la información, es necesario extinguir el fuego tan pronto como sea posible, antes de que dañen los equipos costosos.

Los extintores de incendios, sistemas de rociadores, supresión de incendio, son algunos de los equipos a usar y tenerlos listos.

Riesgos de los Productos Químicos.

Muchas organizaciones trabajan con materiales y productos químicos peligrosos como parte de su negocio. En los Estados Unidos, la Administración de Salud y Seguridad Ocupacional (OSHA) y la Agencia de Protección Ambiental (EPA) tienen normas estrictas en cuanto a la adquisición, almacenamiento y uso de un gran número de sustancias peligrosas, así como planes específicos de contingencia para tratar los derrames y escapes accidentales de estas sustancias.

En muchos casos, estos derrames y liberaciones pueden desencadenar desastres. Las evacuaciones obligatorias son suficientes para desencadenar un desastre: si todo el mundo tiene que dejar una instalación, ¿cómo puede la empresa continuar sus operaciones?

Mantener Frio el Ambiente.

El Procesamiento de la Información funciona muy bien con una franja muy reducida de temperatura y humedad. Estas restricciones de medio ambiente se convierten en un desafío cuando el equipo consume mucha electricidad y lanza tanto calor. Deshacerse del calor a la misma velocidad a la que se produce no es una tarea fácil. Y con la cantidad de calor que los nuevos equipos vierten por pie cuadrado de espacio, y el equipo de refrigeración debe ofrecer mucho más que lo anterior.

La esperanza de vida del procesamiento de la información desciende bruscamente (a veces por más de 90 por ciento) con la alta

temperatura. El Control de temperatura es esencial, un procesamiento de la información debe tener redundancia en su sistema HVAC "Heating, Ventilation, Air Conditioning" (calefacción, ventilación y aire acondicionado) y por consiguiente no pone el centro de datos en riesgo.

Mantener Seco el Ambiente: Agua/inundaciones detección y prevención.

Sistemas de Información y el agua no se mezclan muy bien. Por esta razón, el agua de sistemas de supresión de incendios (como primera línea de defensa) ha caído en favor de la resolución, porque descarga de agua puede dañar gravemente equipos informáticos.

Puede hacer algunas cosas para asegurarse de que el agua no se convierta en un problema. Es posible que no tenga que preocuparse por algunas de estas medidas, en función de las condiciones locales:

- **Peligro de inundación Local:** Encontrar un hidrólogo que puede proporcionar una evaluación realista de la inundación potencial para la instalación. Tomar los resultados de un arquitecto que puede recomendar mitigar las características de su sitio que puede garantizar que cualquier inundación de aguas es dirigida hacia el centro.
- **La encuesta:** Buscar riesgos dentro de su instalación que puede representar un peligro de agua. Verificar que los drenajes del techo y otras características están funcionando correctamente.
- **Los procedimientos de emergencia:** Si el edificio es propenso a cualquier tipo de acumulación de agua, es posible que se necesite realizar procedimientos de emergencia y los suministros a la mano, como sacos de arena, bombas, u otros medios para mantener el agua fuera o eliminar el agua si se le da.

SELECCIONAR LUGARES DE TRATAMIENTO ALTERNATIVO

A pesar de los medios razonables para impedir que se produzca un desastre o minimizar el impacto de la catástrofe, algunos de los eventos son tan intensas que no tendrá más remedio que abandonar de manera temporal o permanente una instalación de procesamiento de datos y reanudar las operaciones en otros lugares. Naturales Extremos y los desastres provocados por el hombre, y en su lugar, usted sabe qué tipos son más probabilidades de provocar una verdadera catástrofe para su organización.

Tiene varias alternativas para reubicar sus sistemas si su centro de datos termina inundado:

- **Sitios Fríos:** instalaciones de transformación sin computadoras instaladas.
- **Sitios Tibios:** instalaciones de procesamiento de las computadoras que requieren la instalación y la configuración.

- **Sitios Calientes:** instalaciones de elaboración con los equipos que están listos para llevar a cabo procesos de negocio.
- **Otros lugares de negocios:** Otras instalaciones que posee la organización.
- **Sitios móviles:** instalaciones de procesamiento en remolques.
- **Servicios Contratados:** instalaciones de transformación por otras organizaciones.
- **Facilidades recíprocas:** acuerdo de ayuda mutua.

Otros Lugares de Negocio

Algunas empresas ya tienen más de una instalación de tratamiento o tengan la capacidad de implementar una segunda planta en uno de sus locales. La capacidad de crear su propio sitio de procesamiento alternativo puede costar menos el servicio fuera de las oficinas o salas.

Algunos puntos a considerar cuando se piensa en otros lugares de negocios alternativos como lugares de tratamiento incluyen:

- **Ubicación de los riesgos:** ¿Está el lugar libre de riesgos relacionados con la situación de los aeropuertos, ferrocarriles, materiales peligrosos, inundaciones, tormentas, deslizamientos y otros factores?
- **Medio ambiente:** ¿El sitio tiene suficiente VENTILACIÓN Y AIRE ACONDICIONADO y capacidad de alimentación, o se puede agregar?
- **Seguridad física:** ¿La otra ubicación de la empresa tiene suficientes controles de seguridad física, tales como cercas, video vigilancia, sistema de llave, etc.?
- **Proximidad al centro principal de procesamiento:** ¿El sitio está bastante lejos de la actual planta de procesamiento de información no se considera en la misma zona de riesgo? La distancia mínima pueden oscilar entre 100 a 500 millas, dependiendo de la naturaleza de los riesgos, tales como terremotos, volcanes, huracanes, tsunamis, y así sucesivamente.
- **Transporte:** ¿Es el sitio alternativo lo suficientemente cerca de los principales sistemas de transporte, tales como aeropuertos, ferrocarriles, puertos, autopistas, debe hacer que los sistemas sean accesibles en caso de una emergencia?
- **Servicios de Apoyo:** ¿Son servicios de apoyo lo suficientemente cerca del sitio alternativo? Ejemplos de los servicios de apoyo que puede ser necesario tomar en consideración incluyen el envío, la policía y los bomberos, alojamiento y restaurantes, servicios públicos, construcción y reparación, y la conectividad de la red.
- **Las leyes y los códigos:** ¿Son los códigos de construcción y leyes relativas a la seguridad y otros asuntos para el centro de procesamiento alternativo, adecuado para sus necesidades?

Páginas web para móviles

Organizaciones como APC, Sun Microsystems y SunGard han desarrollado centros de datos móviles de emergencia que puedan proporcionar a la ubicación de negocios. Estas compañías ofrecen las siguientes características:

APC InfraStruXure Express:

- **Sun Microsystems Project Blackbox:** Centro de datos en un contenedor de mercancías que pueden ser enviados en cualquier parte del mundo por el camión, el barco, tren o aire. Equipado con una alimentación y refrigeración, y configurable selección de servidores y equipos de red.
- **SunGard:** Mobile data center en un semi-remolque plataforma que incluye un generador, comunicaciones de voz y datos acceso, terminales e impresoras, bastidores de equipos, áreas de trabajo, cocina, baños, iluminación, y la seguridad física. SunGard Higher Education tiene varias de estas unidades disponibles para el envío dentro de las 48 horas.
- **Ubicación de las Instalaciones.** Centros de datos comerciales, también conocido como staff instalaciones o sólo coloso, son un gran negocio en casi todas las áreas metropolitanas en el mundo. Los grandes jugadores, tales como AT&T, con decenas de instalaciones en todo el mundo; muchas empresas regionales y locales han construido grandes centros de datos, así.
- **Seguridad física:** Guardias de seguridad, llave de tarjeta en las entradas, video vigilancia, cercas, y quizás otras medidas, tales como edificios duros, perros de guardia, de las barreras, y así sucesivamente.
- **Red/conexión a Internet:** Proporciona conectividad a Internet, sólo se tiene que conectar el router, firewall, switches, y así sucesivamente.

Instalaciones Recíprocas

Colocación de las instalaciones, una de las pocas opciones disponibles para instalaciones de procesamiento alternativo es el servicio recíproco. Instalación de reciprocidad es un acuerdo legal entre ambas partes, en la que cada uno se compromete a hacer una parte de su instalación a disposición de la otra parte en el caso de que la otra parte experimentan un desastre que le obliga a abandonar su propio centro de datos.

Simple y sencillamente en español, el acuerdo es: "YO le permito usar una parte de mi centro de datos si se produce un desastre, y permítanme usar una parte de su centro de datos si tengo un desastre." En la época de computadoras mainframe, el acuerdo recíproco no sólo se aplica al espacio físico, sino al uso que se hace de la organización de la computadora central(s).

Las dos organizaciones que tienen el mismo tipo de computadoras para que programas de aplicación en una también se ejecute en el otro. Las organizaciones necesitan para llevar a cabo una prueba inicial para comprobar la viabilidad de largo plazo acuerdo recíproco y tal vez las pruebas regulares para asegurarse de que los sistemas siguen siendo compatible.

En el entorno de hoy en día, un acuerdo de reciprocidad puede incluir o no el uso de los demás sistemas de la organización, puede cubrir sólo el espacio y energía de los sistemas en el otro centro de datos de la organización. Sin embargo, un acuerdo recíproco puede costar mucho menos que la alternativa, de colocación de instalación.

3.4. PLANIFICACIÓN DE RECUPERACIÓN DEL SISTEMA Y LA RED

Aunque la planificación de recuperación de desastres tiene que ver con la recuperación de las funciones críticas de negocio, los datos y las aplicaciones asociadas, la recuperación de aplicaciones no puede existir ni opera sin el apoyo de los sistemas de los que residen y las redes que permiten la comunicación con todo lo demás en su ecosistema de aplicaciones.

ADMINISTRACIÓN Y RECUPERACIÓN DE LOS SERVIDORES DE CÓMPUTO

La resistencia de los sistemas es la clave de recuperación en caso de desastre. La organización debe contar con sistemas que estén listos cuando usted los necesita, en el caso de que un desastre dañe sus servidores primarios o hace que no estén disponibles para su uso. Esta configuración y necesidad específica podría significar:

- Servidores calientes ya que comparten la carga de trabajo actual.
- Servidores de reserva en caliente listo para asumir el control a corto plazo.
- Servidores de reserva caliente lista para hacerse cargo con un poco de preparación.
- Servidores de reserva frías listas para la instalación de aplicaciones y datos.
- Servidores comprados cuando el desastre ocurre, instalar la aplicación y los datos en ellos cuando llegan.

Determinando la disponibilidad de los sistemas

Un plan de arriba hacia abajo DRP define los procesos de negocio más críticos, y por lo tanto identifica las aplicaciones y bases de datos asociadas con esos procesos como críticos. Estas aplicaciones críticas y bases de datos, a su vez, identifican a los servidores críticos y la infraestructura de apoyo.

Al determinar los objetivos de tiempo de recuperación (RTO - es decir, la rapidez con que los servidores de reemplazo deben estar en funcionamiento), se puede calcular la cantidad de tiempo que tiene para conseguir nuevos servidores listos para ejecutar esas aplicaciones críticas. Un RTO determina la rapidez que necesita para recuperar sus sistemas en un desastre.

Arquitectura y configuración del servidor

Configuración de hardware: Descubre todo sobre el hardware en el servidor, incluyendo:

- Marca, modelo, número de serie

- Versiones de firmware (BIOS / CMOS)
- Número y tipo de CPUs
- Cantidad y tipo de memoria
- El número, tipo y configuración de hardware de adaptadores de red
- El número, tipo y configuración de hardware de las interfaces de almacenamiento (por ejemplo, los adaptadores SCSI)
- Exactamente cómo el hardware se monta (orden de tarjetas adaptadoras, tarjetas de memoria, etc.)
- Los dispositivos periféricos conectados (tipo, modelo, versión, etc.)

Sistema operativo: Figura todo sobre el sistema operativo (OS) que se está ejecutando en el servidor, incluyendo:

- Versión, la fecha, y el nivel de parches para el sistema operativo que esté utilizando.
- Los parches instalados (y las versiones de esos parches e incluso el orden de instalación, si se puede saber)
- Los componentes instalados y sus versiones
- Configuración de arranque
- Ajustes de recuperación

Configuración de recursos: memoria virtual, la configuración de la utilización del disco, utilización de la memoria, y cómo el sistema operativo hace que los recursos disponibles para las aplicaciones y procesos del sistema. En el mundo UNIX, estos son los parámetros del núcleo; en Windows, éstos se configuran en su mayoría en el Registro y en algunas funciones de la interfaz de usuario administrativo.

Los servicios de red y de la red de configuración: Todos los ajustes habituales, incluyendo la máscara de subred, puerta de enlace, servidor DNS, servidor de directorios y servidor de tiempo, así como los ajustes de sintonización, como el número de conexiones abiertas y amortiguar la asignación.

Configuración de seguridad: Una gran cantidad de estos ajustes lidiar con el registro de eventos, la auditoría del sistema, la configuración de control de acceso a nivel de sistema, descarga y la instalación y configuración de la cuenta de usuario.

Componentes de nivel de sistema: Los componentes adicionales instalados a nivel del sistema, incluyendo:

- Firewall
- La detección de intrusiones y prevención
- Anti-virus y otros anti-malware
- Agentes de gestión del sistema

Gestión de acceso: Toda la gama de acceso a nivel de sistema que incluye:

- Configuración del ID de usuario, ID de usuario y contraseña
- Configuraciones relacionadas con los recursos de gestión de usuarios centralizados, como LDAP o Active Directory
- Los recursos compartidos, es decir, directorios y otros recursos que pueden acceder los usuarios a través de la red

- **Gestión del cambio:** El proceso de negocio de que se trate con el adecuado desarrollo, el análisis y la aprobación de los cambios realizados en un entorno de producción, en todas las capas. El objetivo de la gestión del cambio es exponer a riesgos potenciales y otras cuestiones que puedan poner en riesgo los cambios propuestos antes de que ocurran. El manejo adecuado cambio le da una mayor disponibilidad del sistema y un menor número de interrupciones no programadas.
- **Gestión de la configuración:** El proceso de grabación de todos los cambios realizados a todos los componentes (en todas las capas) en un entorno. El repositorio central se conoce como la base de datos de gestión de configuración (CMDB), que almacena todos los detalles de los sistemas bajo su gestión.

Consideraciones en la computación de servidores distribuidos

Muchos entornos utilizan una arquitectura de aplicación compleja que incluye componentes que residen en muchos servidores, y no todos los servidores están necesariamente situados en la misma ubicación.

Con empresas conectadas a Internet y la integración de aplicaciones que se alimentaron por la interoperabilidad de negocio y posibles gracias a las tecnologías más recientes, como la Arquitectura Orientada a Servicios (SOA), la planificación de recuperación de desastres asume un nivel mucho más alto de complejidad.

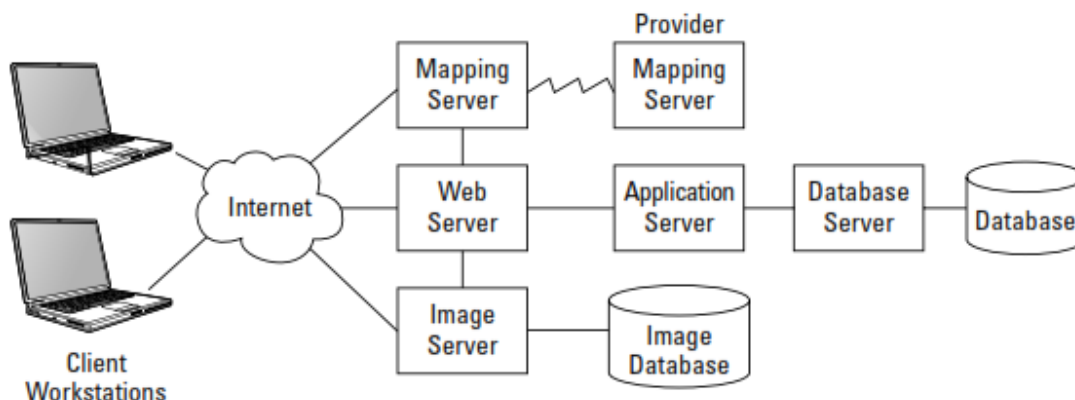
Es posible que se encuentren estos temas relacionados con la arquitectura de la aplicación durante el análisis y planificación del DRP:

- **Interfaces:** Si se dispone de interfaces personalizadas entre los componentes de su entorno distribuido, que va a tomar más de esfuerzo (por parte de los desarrolladores de sistemas o integradores) para mejorar la capacidad de recuperación en el medio ambiente en general. Involucrar al personal de la arquitectura de aplicaciones y los instamos a desarrollar planes estratégicos que incluyen movimiento de interfaces estándar, tales como la arquitectura orientada a servicios (SOA).
- **Latencia:** En un entorno altamente distribuido, los sistemas que se comunican a través de grandes distancias y/o más de red de área amplia de conexiones lentas (WAN) pueden experimentar latencia (retrasos en la transmisión de los datos de sistema a sistema). El comportamiento de la aplicación puede cambiar de manera inesperada en un escenario de desastre si la latencia entre componentes aumentos (o

disminuciones) por una cantidad significativa. Partes de un entorno distribuido pueden no ser capaces de tolerar la latencia, y otras partes que incluir latencia significativa pueden comportarse de manera diferente si la latencia disminuye.

- **Consideraciones sobre la red:** Un entorno de aplicación distribuida que abarca conectividad WAN necesita tomar en cuenta el diseño de redes. Las aplicaciones distribuidas que fueron diseñados para, e implementados en las redes de área local rápidas pueden sufrir una degradación del rendimiento en una red de área amplia. El efecto acumulativo de varios saltos largos a través de una WAN puede ralentizar el tiempo de respuesta e incluso causar tiempos de espera de la red.
- **Puntos de falla:** sistemas distribuidos tienen más puntos de falla (literalmente, el número de componentes de hardware y software necesarios para apoyar el medio ambiente) que los sistemas centralizados, y un desastre es más probable que ocurra cuando los puntos de falla son geográficamente diverso, en lugar de en una sola / ubicación central.
- **Recuperación distribuida:** Un desastre que se produce en una ubicación de un entorno distribuido puede indicar una operación de recuperación que implica personal en muchos lugares.
- **Componentes de terceros:** Si un proveedor de servicios de terceros que aloja un elemento vital para su aplicación experimenta un desastre, la lista de prioridades de ese proveedor de servicios puede ser diferente a la suya.
- **Prioridad:** En un entorno distribuido, un desastre que desactiva un componente puede tener complicaciones adicionales de recuperación. El fallo de un componente en una ubicación remota puede ser su alta prioridad, pero una prioridad más baja que otros componentes para la organización de la ubicación remota.

Consideraciones de arquitectura de aplicaciones



- **Introducir la autenticación centralizada:** los arquitectos de aplicaciones e integradores deben considerar seriamente un cambio hacia los servicios de autenticación basados en la red en lugar de confiar en la autenticación dentro de la aplicación.
 - o **Credenciales de conexión estándar:** Los usuarios tienen menos (tan sólo uno) identificadores de usuario y contraseñas que necesitan para recordar.
 - o **Gestión de autenticación simplificada:** Usted necesita menos personal para gestionar la emisión y revocación de los derechos de acceso.
 - o **Contraseñas menos olvidadas:** Dado que los trabajadores tienen menos contraseñas que necesitan para recordar (tan sólo uno), no van a olvidar sus contraseñas tan a menudo, así que usted puede pasar menos tiempo de restablecer contraseñas. Ejemplos de servicios de autenticación y de identidad centralizados incluyen LDAP, Microsoft Active Directory, Oblix, y de IBM Tivoli Identity Manager.
- **Las interfaces estandarizadas:** arquitectos de aplicaciones deben poner SOA (Arquitectura Orientada a Servicios), Servicios Web, ETL (Extract, Transform, Load) y XML (Extensible Markup Language) en sus planes de trabajo como medio para la integración altamente ágil entre las aplicaciones, tanto dentro de la empresa.

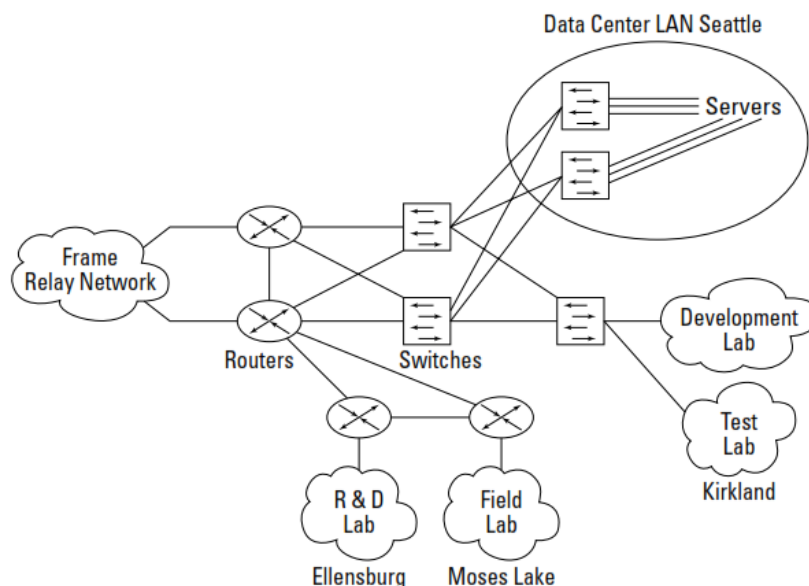
La consolidación de servidores

El concepto es simple: en lugar de dedicar aplicaciones a servidores individuales, que pueden resultar en servidores infrautilizados, instala varias aplicaciones en servidores para utilizar de manera más eficiente el hardware del servidor, reduciendo así los costos.

La consolidación de servidores es una decisión inteligente para llevar a cabo, siempre y cuando te acuerdas de que la consolidación de servidores es algo para llevar a cabo durante el tiempo de paz (operaciones normales), no en un escenario de desastre.

ADMINISTRACIÓN Y RECUPERACIÓN DE INFRAESTRUCTURA DE RED

Las redes son mucho más que sólo los dispositivos que se mueven sobre el tráfico de red. Las redes realizan funciones a menudo invisibles que permiten las comunicaciones dentro y entre empresas.



LA IMPLEMENTACIÓN DE INTERFACES ESTÁNDAR

A menudo se pueden extender más fácilmente y cambiar una arquitectura de aplicaciones que se basa en estándares abiertos que uno que se construye con interfaces personalizadas.

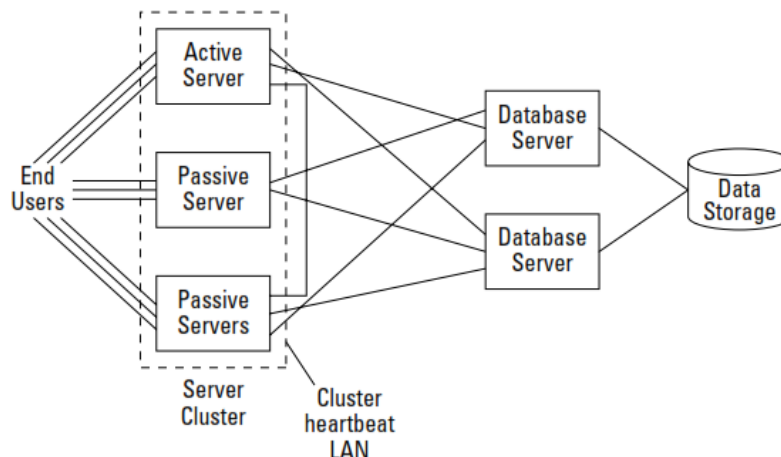
Los estándares abiertos son los estándares de programación y de las comunicaciones en que las aplicaciones y los sistemas están contruidos. He aquí algunos ejemplos de estándares abiertos:

- **TCP / IP:** El protocolo de red de Internet. Decenas de estándares abiertos caen dentro de TCP / IP, incluyendo SMTP (Simple Mail Transfer Protocol) que hace que el trabajo de e-mail, DNS (dominio de servicio de nombres) que se utiliza para traducir nombres a direcciones IP, NTP (Network Time Protocol) que sincroniza los relojes del sistema , HTTP (hyperText Transfer Protocol) que web navegadores utilizan para solicitar datos de los servidores Web y SNMP (Simple Network Management Protocol) que se utiliza para administrar los dispositivos y sistemas de red.
- **World Wide Web:** Abarca los protocolos y normas que apoyan la Web.
- **GSM:** El estándar de comunicación de telefonía celular se utiliza en la mayor parte del mundo.

IMPLEMENTACIÓN DE CLÚSTERES DE SERVIDOR

Un clúster de servidores es una colección estrechamente acoplado de dos o más servidores que están configurados para alojar uno o más aplicaciones.

En otras palabras, un clúster es un conjunto de equipos que aparecen como un solo equipo para los usuarios finales.



Los clústeres de servidores, mejoran la disponibilidad de las aplicaciones, reduciendo los efectos de:

- **Error de hardware:** Los fallos en componentes como la CPU, RAM, autobús, o el resultado de una unidad de inicio, interrupción imprevista inmediata para aplicaciones críticas que se ejecutan en el sistema.
- **El fracaso del software:** Un fallo en el software puede resultar en un bloqueo del servidor o accidente.
- **Falla en la red:** Usted pareja un racimo sistema bien diseñado con una arquitectura de red que tiene redundancias similares. Si se produce un fallo en la red, otros componentes de la red deben estar disponibles, por lo que al menos algunos de los servidores en el clúster todavía deben ser accesibles desde los sistemas cliente.
- **Mantenimiento:** Con dos o más sistemas de un clúster, puede realizar mucho más fácilmente las actividades de mantenimiento regulares en servidores individuales.
- **Problemas de rendimiento:** Se puede configurar un clúster para permitir más de un servidor de la agrupación para servir aplicaciones.

Arquitectura Clúster y almacenamiento

La arquitectura de servidores en clúster, sistemas de almacenamiento, y las propias aplicaciones están estrechamente unida. Aplicaciones alojadas en un clúster de servidores deben estar

diseñados para interactuar correctamente con la arquitectura física de los sistemas de almacenamiento y cómo funcionan clúster conmutaciones por error. La integridad de las aplicaciones es vital para la salud de la aplicación, sobre todo cuando los servidores y arquitectura de clúster se pueden cambiar en tiempo real.

Elije una tecnología de cada uno de los siguientes grupos de armar una arquitectura completa en clúster:

Arquitectura Clúster:

- Activo / activo
- Activo / pasivo

Arquitectura de almacenamiento:

- **SAN (Storage Area Network):** Seleccione si desea almacenamiento unido a través de SCSI, Fibra bucle arbitrado, o una red de fibra.
- **NAS (Network Attached Storage):** Se conecta a sistemas de almacenamiento la red y acceder a ellas con NFS (Network File System) o SMB (Server Message Block) protocolos de red.

La replicación de datos:

- **Espejo:** La base de datos, sistemas operativos de servidor o sistema de almacenamiento de capas puede realizar el espejo, en que los cambios a los datos en un dispositivo de almacenamiento sistema se copian en un sistema de almacenamiento remoto en tiempo real.
- **Réplica:** La copia de las transacciones de un sistema a otra.

Arquitectura de la red:

Balanceadores de carga: Para arbitrar el acceso entre varios servidores activos.

Turnos de DNS: Para el balanceo de carga a través de un activo/activo clúster geo localizado.

Cambios de enrutamiento dinámico: Para la conmutación por error a nivel de red para que clientes de aplicaciones están dirigidas a los servidores activos, donde están los servidores.

3.5. PLANIFICACIÓN DE RECUPERACIÓN DE DATOS

PROTECCIÓN Y RECUPERACIÓN DE LOS DATOS DE LAS APLICACIONES

Se sabe que los activos más valiosos de TI son tus bases de datos, protegerlos es sólo una cuestión de incorporar algunas copia de seguridad o esquema de replicación a fin de hacerlas más fácilmente disponible si ocurre un desastre.

En la mayoría de las organizaciones, aunque almacenan muchos de los datos en el centro de las bases de datos, también almacenan algunos de los datos en otro lugar. Y, probablemente, sólo unos pocos puesto que la gente está familiarizada con los detalles de los datos que existen en el remanso lugares en la red.

Localización de todos sus datos requiere un poco de trabajo detectivesco. Es necesario un proceso centrado en vista que descubre todos los entresijos de sus datos (donde vienen los datos ni a dónde va) por lo que no te pierdas ningún detalle.

Recuperación de funciones críticas del negocio significa algo más que la recuperación de las bases de datos. También se requiere la recuperación de las capacidades para mover los datos entrar y salir de las aplicaciones que admiten las funciones de negocio.

Antes de explorar las diversas opciones para proteger los datos contra pérdidas (y haciéndolo disponible poco después de un desastre), es necesario comprender algunos básicos principios de protección de datos de estilo DRP:

- **La velocidad aumenta los costos.** En otras palabras, cuanto más rápido se desea que sus datos estén disponibles después de un desastre, más le costará.
- **La distancia aumenta los costos.** Cuanto más lejos se almacenan los datos que se necesita recuperar rápidamente, más se le va a costar. Principalmente, este costo se refiere a conexiones privadas, WAN de alta velocidad entre dos o más de sus instalaciones.
- **El tamaño aumenta los costos.** Cuantos más datos que desea poner a disposición poco después de un desastre, más le costará. Este coste se refiere a la cantidad de almacenamiento que debe adquirir para lograr la redundancia de almacenamiento que requiere.
- **La complejidad aumenta los costos.** Un plan de protección y recuperación de datos que contiene varias soluciones diferentes para partes de los gastos de organización más que un simple plan.

El equipo del proyecto debate estas posibles estrategias:

- **La recuperación de dos niveles:** Pueden proteger y recuperar la mayor parte del tiempo-crítico los datos mediante el uso de un mecanismo de replicación de datos y recuperar el resto de los datos, que es menos sensible al tiempo, a partir de cintas de copia de seguridad.
- **Recuperación de un solo nivel:** Se puede usar la replicación de datos para proteger y recuperar todos los datos de la organización. Aunque este enfoque tiene más en costos iniciales para proteger a todos los datos, la estrategia es simple y fácil de implementar los miembros del equipo en favor de este enfoque argumentan que su sencillez supera el adicional costes. Probablemente se encuentra que esta forma más fácil y fiable durante una recuperación.

ELECCIÓN DE CÓMO Y DÓNDE DESEA ALMACENAR LOS DATOS

El proceso de planificación DRP comienza con el Análisis de Impacto al Negocio (BIA), que incluye una evaluación de riesgos y la determinación del tiempo de recuperación Objetivos (RTO) y Punto de Recuperación Objetivo (RPO). Estos pasos ayudan a identificar qué procesos de negocio son los más importantes en una organización y la rapidez que necesita para recuperarlos.

El Análisis de Impacto al Negocio y los esfuerzos del detective de datos, una vez terminado, debe proporcionar dos hechos importantes:

- ✓ Qué datos son importantes
- ✓ Fueron los datos importantes se encuentra ahora

La protección de datos a través de las copias de seguridad

Recientemente, la copia de seguridad de datos en discos duros extraíbles, como las que fácilmente conectar a arreglos RAID (altamente sistemas de almacenamiento en disco recipientes), se ha convertido popular. Desde un punto de vista la función empresarial, medios de copia de seguridad, tales como cintas y los discos, son más o menos lo mismo: Son los medios que se utilizan para almacenar y conservar copias de los datos electrónicos. Copia de seguridad se define más por la función - hacer copias de seguridad de la información - que por el tipo de material utilizado.

La copia de seguridad cumple varios propósitos:

- **Archivado a largo plazo:** Reglamento a menudo requieren el almacenamiento a largo plazo de ciertos registros

empresariales.

- **La recuperación de datos:** El error humano ocurre a menudo - un error del programa puede pasar inadvertidamente o alguien puede borrar los archivos accidentalmente.
- **La recuperación de desastres:** Si un evento desastroso golpea a un centro de datos en la que su organización almacena información de negocios importante, puede recuperar fácilmente los datos de las cintas de copia de seguridad en reemplazo o sistemas alternativos.

Pros y contras de la realización de Backups

Pros	Contras
Medios económicos	Acceso lento / secuencial
Buena estabilidad	Media es algo frágil (se aplica principalmente a la cinta)
Los medios tienen una larga vida útil	
Media es fácilmente transportable, se presta fácilmente para el almacenamiento fuera del sitio	

La protección de los datos a través del almacenamiento elástico

Estas son algunas de las maneras en que se puede hacer un sistema de almacenamiento más elástico:

- **RAID:** Matriz redundante de unidades independientes (o discos), también conocido como Matriz redundante de unidades de bajo costo (o discos). Puede elegir entre muchas funciones RAID y configuraciones. Pero todo el almacenamiento basado en RAID tienen la capacidad para que el sistema de almacenamiento para mantener el funcionamiento, incluso si una de las unidades de disco duro falla. Los sistemas RAID también le permiten sustituir una unidad defectuosa sin necesidad de apagar el sistema RAID (llamado intercambio en caliente).
- **Fuentes de alimentación redundantes:** Muchos sistemas de almacenamiento tienen varias fuentes de alimentación, los que permiten el funcionamiento continuo de los sistemas de almacenamiento, incluso si una de las fuentes de alimentación falla. Estos sistemas de almacenamiento permiten también el

reemplazo en caliente (hot swap) o de fuentes de alimentación, asegurar disponibilidad continua.

- **Las conexiones con servidores redundantes:** Muchos sistemas de almacenamiento tienen múltiples controladores y las conexiones físicas para servidores, garantizando así el funcionamiento continuo, incluso si una de las conexiones falla.
- **La Virtualización:** puede utilizar grandes sistemas de almacenamiento central para crear volúmenes de disco virtual que cumplen con las necesidades de almacenamiento servidores de aplicaciones.

Protección de datos a través de la replicación y duplicación

La Duplicación y replicación por lo general, se refieren a la capacidad de escribir nuevos datos en más de un sistema de almacenamiento al mismo tiempo. Replicación y duplicación difieren un poco en los detalles.

Los datos se copian a otro sistema de almacenamiento que un servidor puede utilizar inmediatamente, casi en tiempo real.

Se puede tener acceso a los datos sin la necesidad de una cinta magnética del tipo de restauración.

Protección de datos mediante almacenamiento electrónico

Una opción muy popular disponible para realizar copias de seguridad de los datos se conoce como almacenamiento electrónico, conocido a veces como copia de seguridad remota e-vaulting. Almacenamiento electrónico es el proceso de envío de datos por correo electrónico a una ubicación fuera del sitio a través de una conexión de red.

Puede utilizar almacenamiento electrónico para un montón de cosas, dependiendo de a quien se le pregunte. Algunas de las posibilidades son:

- El uso de software de copia de seguridad en sus sistemas para enviar los datos de copia de seguridad a las computadoras dirigido por un proveedor de servicios de copia de seguridad.
- Replicar las transacciones de bases de datos que se envían fuera de sitio.
- Copia de datos a un sistema de espera situado a distancia que puede asumir funciones de procesamiento primario durante un desastre.

Protección de datos al tiempo en modo DRP

Mientras que en el modo de recuperación de desastres, en caso de un desastre cuando las aplicaciones de negocio críticas están

funcionando en ubicaciones alternativas, también es necesario que todos de estas protecciones cuenten con lo siguiente:

- Copia de seguridad de los servidores de DRP.
- Proteger los medios de copia de seguridad, por lo general a través del almacenamiento fuera del sitio.
- Proteja los datos transmitidos.
- Guarde los datos críticos en sistemas de almacenamiento flexibles.

En el modo de desastre, información y procesos de negocio son tan crítico como son en tiempos de las operaciones normales. En consecuencia, los sistemas y procesos que se utilizan durante un desastre deben proporcionar el mismo nivel de protección que los sistemas y procesos primarios.

PROTECCIÓN Y RECUPERACIÓN APLICACIONES

Desde el punto de vista de un experto, aplicaciones es sólo otra forma de datos empresariales. Aunque esta afirmación es sobre todo verdad, debe tener en cuenta muchas cuestiones al recuperar aplicaciones que no tienen que preocuparse por los datos. Debe tener en cuenta estos datos de las aplicaciones:

- Versión
- Parches y correcciones
- Configuración
- Usuarios y roles
- Interfaces
- Personalizaciones
- Vinculación con versiones del sistema operativo y base de datos
- Los sistemas cliente
- Consideraciones sobre la red
- Gestión del cambio
- Gestión de la configuración

3.6. ESCRIBIENDO EL PLAN DE RECUPERACIÓN DE DESASTRES

DETERMINAR EL CONTENIDO DEL PLAN

Los planes DRP deben contener varios elementos clave que se pueden utilizar para poner en marcha sistemas y procesos críticos después de la ocurrencia de un desastre. La mayoría de las organizaciones debe incluir los siguientes elementos en su plan de recuperación ante desastres:

- ✓ Un procedimiento de declaración de desastre
- ✓ Listas de contactos de emergencia y árboles

- ✓ Selección de liderazgo de emergencia (el equipo de liderazgo predeterminada así como el procedimiento para armar rápidamente un equipo)
- ✓ Procedimientos de evaluación de daños
- ✓ La recuperación del sistema y los procedimientos de reinicio
- ✓ Procedimientos para la transición a las operaciones normales
- ✓ La selección del equipo de recuperación (el equipo de recuperación pre-seleccionado, así como el proceso para encontrar otras personas que pueden ayudar cuando ocurre un desastre en realidad)

Procedimiento de declaración de desastre

Muchos planificadores DRP se obsesionan sobre cómo declarar un desastre. Aquí están algunas ideas de cómo declarar un desastre:

Declaración de consenso: Para designar un equipo básico de los tomadores de decisiones, probablemente los mandos medios o superiores, como el equipo de liderazgo DRP. Cuando un desastre ocurre, los miembros del equipo central en contacto entre sí y tal vez convocar una conferencia telefónica, si pueden.

Declaración por criterios: Designar los miembros principales del equipo como el DRP equipo de liderazgo. Cuando se produce un evento, una o más de ellos lee una lista definitiva, que podría ser una serie de Sí o No. Si acierta las respuestas, o un número mínimo de respuestas, son Sí, el equipo declara un desastre, lo que desencadena el plan de DRP.

Listas de contactos de emergencia

Después de declarar un desastre, el siguiente paso lógico en un plan integral es que comenzará a notificar al personal que se encargan de realizar DRP plantean actividades, como las comunicaciones, la evaluación y recuperación. el DRP miembros del equipo central del plan que participan en la declaración de desastre, obviamente, saber en primer lugar cuando la organización declara un desastre, y las notificaciones salir de allí a personal de respuesta a desastres adicional, gestión, personal que se comunican con proveedores y clientes, y así sucesivamente.

Procedimientos de evaluación de daños

El objetivo de la evaluación de daños es identificar el estado de los sistemas de TI y servicios de apoyo que están involucrados en un desastre y decidir si los sistemas y medios de apoyo están dañados o discapacitados en la medida en se necesita sistemas de TI en otra ubicación a seguir apoyando a funciones críticas del negocio.

La evaluación de daños es tanto un arte como una ciencia. Del mismo modo, no ahondar para determinar si una evacuación garantiza desastre o si el personal puede quedarse atrás para ayudar con la evaluación y posible recuperación o se reinicia. Estos asuntos son importante, para estar seguro, pero están más allá del alcance de este libro.

La recuperación del sistema y los procedimientos de reinicio

Es probable que necesita para hacer sus procedimientos de recuperación del sistema y reinicie bastante complejo y largo. Tienen que incluir cada detalle implicado en conseguir sistemas en funcionamiento de varios estados, incluyendo el metal desnudo (servidores con ningún sistema operativo o aplicación de software instalado en ellos).

Es necesario tomar muchos factores adicionales en cuenta cuando se desarrolla sus procedimientos de recuperación del sistema:

Comunicaciones: A lo largo de la operación de recuperación, equipos de recuperación necesitan estar en constante comunicación con el equipo central DRP, así como clientes, proveedores, socios y otras entidades.

Las áreas de trabajo: Establecer un área donde los trabajadores de TI críticos pueden trabajar durante y después de la operación de recuperación.

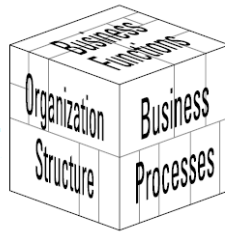
Experiencia: Realice los procedimientos de recuperación lo suficientemente general como para que la gente que están familiarizados con las tareas de administración de sistemas, pero no necesariamente sus sistemas, pueden recuperar sus sistemas sin tener que hacer conjeturas o suposiciones.

ESTRUCTURACIÓN DEL PLAN

Estructura de nivel de empresa

Las organizaciones de varias unidades haciendo grandes planes de DRP tienen que buscar la manera de escribir los planes de los procesos críticos y las aplicaciones que abarcan los departamentos o

unidades de negocio. Planes de RECUPERACIÓN ANTE DESASTRES debe alinearse con las aplicaciones, o si debería alinear con las unidades de negocio.



Estas son algunas consideraciones que pueden ayudar a entender cómo acercarse este problema panorama general:

- Geografía
- La estructura de la organización
- Función de negocio

Estructura de nivel de documento

Como cualquier proyecto oficial en el que aparece información importante de la empresa en los documentos, se debe considerar la posibilidad de crear una estructura dentro de los distintos documentos DRP. Sí, estoy hablando plantillas de documentos. Las plantillas pueden incluir los siguientes:

- **Documento Estándar y nombres de archivo:** Hacer que los nombres de los diferentes documentos (lo que aparece en la página del título), así como los nombres de archivo de documentos (el nombre del documento en una computadora), coherente.
- **Los encabezados y pies estándar:** incluyen el nombre del documento en la parte superior de cada página (encabezado) y como información confidencial de la empresa, número de página , fecha y número de versión en la parte inferior de cada página (pie de página).
- **Título de la página:** Crear una página de título que incluye todos los metadatos del documento, como el título, la versión, la fecha, y así sucesivamente.
- **Tabla de contenido:** una tabla de contenido ayuda al lector encontrar rápidamente las distintas secciones del documento. Documentos de mayor tamaño pueden también necesita un índice lista de figuras, y la lista de tablas.
- **Derechos de autor y otra jerga legal:** Ayuda a proteger intelectual de la organización

- propiedad.
- **Historial de modificación:** le ayuda a mantener un registro de los cambios realizados desde una versión a la siguiente, así como que los han realizado y cuándo.
- **Versión del documento**
- **Encabezados y párrafos estándar:** Un aspecto constante hace que el DRP documenta más fácil de leer y trabajar.

3.5. DIEZ HERRAMIENTAS DE PLANIFICACIÓN DE RECUPERACIÓN ANTE DESASTRES

LIVING DISASTER RECOVERY PLANNING SYSTEM (LDRPS)

Es un mercado maduro y muy respetado DRP. Es un producto de planificación de Strohl Systems. Puede elegir entre cinco versiones para adaptarse a cualquier tamaño de organización. Se puede también conseguir DRP. Como un software alojado como servicio (SaaS) solución en la que Strohl Systems dispone la aplicación en su centro de datos, de modo que no necesita instalar y mantener el software en sus propias instalaciones.

Algunas de las características disponibles en LDRPS:

- Mejores prácticas basadas en navegadores
- Plan integrado de informes estándar
- Dependencia mapas
- Informes personalizables
- Listas de llamadas de arrastrar y soltar
- Gestión de recursos Ubicación
- Planes finales de ejemplo pantallas personalizables
- Importación programada y la publicación del plan

BIA PROFESIONAL

LA BIA Profesional, es un producto de software de Strohl Systems, que le guiará a través del proceso de desarrollo de un análisis de impacto en el negocio (BIA) el estudio, organizar los datos de la encuesta, y presentar los resultados finales. Pinta un panorama detallado de las vulnerabilidades financieras y operacionales, relacionados con el desastre y efectos y de las posibles estrategias de recuperación.

Una característica denominada BIA Professional con servidor Web permite a la organización de encuestas en línea en el que selecciona los expertos en la materia de la organización recibirán un enlace por correo electrónico que se puede hacer clic para realizar la encuesta en línea. Este método de la encuesta permite recoger datos acerca de los procesos de negocio críticos.

LA BIA Professional contiene varias características:

- **Auditoría y aprobación de los estudios:** Apoyo a gerencia de la empresa revisión y aprobación de la BIA encuestas antes de su liberación.
- **Actividad mapa:** le guiará por los pasos para crear un BIA encuesta.
- **Pregunta de ramificación:** Permite que el diseñador de la encuesta para crear una encuesta en la que pedirá a los usuarios sólo las preguntas pertinentes.

- **Informes:** creación de informe simplificado que incluye un Asistente para informes. Puede crear informes en Microsoft Excel, Crystal Reports o formatos PDF.

ANÁLISIS DE RIESGOS COBRA

Consulta, objetivo y Bi-funcional Análisis de Riesgo (COBRA) es un conjunto de análisis de riesgos y seguridad herramientas de revisión que C&A Systems Security.

El conjunto de herramientas consiste en un proceso predeterminado:

- **Cuestionario:** La COBRA herramienta tiene una gran base de datos de las preguntas contenidas en módulos que se pueden seleccionar en una base de conocimientos. Cada módulo aborda un área de riesgo, incluido el control de acceso, seguridad física, desarrollo de software, y así sucesivamente. También puede crear y agregar preguntas manualmente.
- **Estudio riesgo:** El riesgo agrimensor herramienta gestiona la cumplimentación del cuestionario. Los usuarios pueden completar los cuestionarios todos a la vez, o puede volver a él posteriormente.
- **Informes:** El generador de informes genera resultados de los cuestionarios.

GENERADOR BCP

Generador BCP es una popular herramienta basados en plantillas que se pueden utilizar para crear planes de continuidad de negocio.- Pero Generador BCP hace planes que se parezca mucho a los procedimientos de recuperación ante desastres.

Se puede utilizar BCP Generador de la siguiente manera:

- **Plantilla de relleno:** Si estás familiarizado con los procesos y desea obtener resultados más rápidos, puedes ir directamente a las plantillas y empezar a llenar de detalles.
- **Guía interactiva:** Generador BCP le guía, paso a paso, a través de todo el proceso de creación de un plan de continuidad de negocios, Análisis de impacto en el negocio de plan de mantenimiento y todo lo que hay en el medio.

KIT DE DRP PRÁCTICAS PROFESIONALES

El Instituto de la recuperación de desastres (DRP) ha desarrollado una guía de prácticas profesionales. Las secciones de la guía son:

Área Temática 1 - Inicio del Proyecto y Gestión

Área Temática 2 - Evaluación y Control de Riesgos

Área Temática 3 - Análisis de Impacto al Negocio

Área Temática 4 - Desarrollo de Estrategias de Continuidad del Negocio

Área Temática 5 - Respuesta de Emergencia y Operaciones

Área Temática 6 - Desarrollo y Planes de Continuidad de Negocio de

ejecución

Área Temática 7 - Programas de sensibilización y formación

Área Temática 8 - El mantenimiento de los Planes de Continuidad de Negocio

Área Temática 9 - Relaciones Públicas y de coordinación de crisis

Área Temática 10 - Coordinación con Agencias Externas

PLANTILLA PLAN DE RECUPERACIÓN DE DESASTRES

Si desea obtener una verdadera vía rápida, el Plan de RECUPERACIÓN ANTE DESASTRES esta plantilla es un conjunto completo de la planificación de RECUPERACIÓN ANTE DESASTRES documentos plantilla que rellenar. El contenido se divide en las siguientes secciones:

- **Descripción:** plan de recuperación ante desastres misión, alcance, la autorización, la responsabilidad y los principales supuestos.
- **Análisis de impacto en los negocios:** Incluye alcance, objetivos, plazos críticos, y las declaraciones de impacto
- **Estrategia de Copia de seguridad:** incluye sistemas de centros de datos, servidores de archivos, los datos de los sitios externos, estaciones de trabajo, y PDAs
- **Recuperación ante desastres:** Se incluye la recuperación selección de equipo y las responsabilidades para la evaluación de daños, el salvamento, los procedimientos de recuperación
- **Procedimientos de emergencia:** procedimientos de evaluación, el salvamento y recuperación
- **Plan DRP recuperación ante desastres:** Ciclo, incluyendo mantenimiento del plan, capacitación, el ensayo y la distribución

KIT DE SLA

Necesita Acuerdos de nivel de servicio (SLA) para definir prestación de servicios en las organizaciones de TI. Los Acuerdos de nivel de servicio son acuerdos oficiales de servicios entre los proveedores y los clientes que definen la cantidad y la calidad de los servicios prestados a los clientes.

Las operaciones de recuperación de desastres es, probablemente, el servicio vital que realiza una empresa. Si su organización tiene procesos complejos y las interdependencias, es posible que desee definir formalmente las operaciones de recuperación en el contexto de los Acuerdos de Nivel de Servicio

Las secciones de la SLA son:

- Introducción
- Alcance Del Trabajo
- Rendimiento, De Seguimiento, Y De Informes
- Gestión De Problemas
- Compensación
- Deberes Y Responsabilidades Del Cliente
- Garantías Y Remedios
- Seguridad
- Derechos De Propiedad Intelectual E Información Confidencial
- Cumplimiento Legal Y Resolución De Disputas
- Terminación
- General
- Firmas
- Horarios

LBL CONTINGENCIA PRO SOFTWARE

Este navegador basado en Web herramienta de software automatiza todo el plan de continuidad empresarial proceso de desarrollo y proporciona un método eficaz para mantener el plan. El software es un sistema basado en el conocimiento que certificados expertos planificación de la continuidad de negocio.

La base de conocimiento de este producto de software contiene las mejores prácticas de planificación de la continuidad de la actividad, así como de cientos de herramientas electrónicas, guías, plantillas, y muestras. Estos sistemas están totalmente integradas en la Suite de Microsoft Office, por lo que debe ser capaz de utilizarlos fácilmente y de forma intuitiva. El software se basa en una metodología probada que ha ayudado a recuperar las organizaciones de los eventos de desastre.

GUÍA DE GESTIÓN DE EMERGENCIAS PARA LA EMPRESA Y LA INDUSTRIA

La guía contiene las siguientes secciones:

- Paso 1: Establecer un equipo de planificación.
- Paso 2: Analizar las capacidades y peligros.
- Paso 3: Desarrollar el plan.
- Paso 4: Implementar el plan.

Consideraciones de gestión de emergencias.

- Hazard específica información. Incluye incendios, materiales peligrosos, inundaciones, huracanes, tornados, tormentas severas, terremotos, y la tecnología emergencias.

CAJA DE HERRAMIENTAS DE DRJ

Esta página es la recuperación ante desastres del propio Diario lista de herramientas y recursos. Los cambios en la web de vez en cuando nueva herramienta y recursos disponibles.

El sitio contiene las siguientes secciones:

- **Las solicitudes de muestras de Propuesta (RFP):** Varios RFP muestra para la planificación software y servicios de DRP. RFP son documentos que se envían a los proveedores como una forma de solicitar formalmente una propuesta de productos o servicios.
- **Ejemplos de planes de DRP:** Puede descargar varios planes de muestreo, ver cómo alguien puso un plan en conjunto pueden ayudar a despertar sus propias ideas.
- **Reglamentos actuales:** Información sobre reglamentos que pueden influir esfuerzo de planificación de recuperación de desastres de una organización.
- **White Papers:** Varios documentos sobre diversos temas, incluido el terrorismo, seguros, análisis de impacto de negocios, asuntos legales, y el impacto de los desastres en el valor del accionista.
- **Recursos en la Red:** Los enlaces a otros sitios que contienen valiosa información. DRP

4. CONCLUSIONES

Con este trabajo los integrantes del grupo logramos obtener conocimientos necesarios sobre los temas tratados.

Cuando hablamos de desastres, las personas tienen la idea equivocada de que solamente son incendios, terremotos, erupciones volcánicas, etc., pero no se dan cuenta que la pérdida de datos, que constituyen el elemento más importante del Sistema de Información, puede ocurrir por problemas menos dramáticos más comunes que si no son considerados, constituyen una amenaza más probable.

Comprendimos que en una entidad hay demasiadas personas con las que se deben tener en cuenta a la hora de que se nos presente algún problema y lo debemos solucionar.

El Plan de Recuperación ante Desastres debe centrar su atención y análisis en la prevención de pérdida de información y describir el procedimiento para recuperarla. Es importante describir con claridad los procesos que se seguirán sin dejar nada a la memoria de la persona que realiza o programa los respaldos ya que el momento que suceda el desastre o la pérdida de información puede ocurrir mucho tiempo después de que se ha realizado el Plan de Recuperación de Desastres.

5. BIBLIOGRAFÍA

- PLANIFICACION DE RECUPERACIÓN DE DESASTRES DE TI - Peter Gregory - Wiley Publishing, Inc.
- ISO/IEC 22301:2012 Seguridad Social - Sistemas de Gestión de Continuidad - Requisitos.
- ISO/IEC 27001:2013 Gestión de Seguridad de los Sistemas de Información.
- ISO/IEC 27002:2013 Gestión de la Información de Seguridad - Código de buenas prácticas.
- ISO/IEC 22399:2007 Guía para la preparación de incidentes y gestión de la continuidad operativa.
- ISO/IEC 24762:2008 Directrices para los servicios de recuperación de desastres de tecnología de información y comunicaciones.