**Estrategias de recuperación viables para enfrentar contingencias**

**Establecimiento de un marco de trabajo para la seguridad y el control**

Aún con las mejores herramientas de seguridad, sus sistemas de información no serán confiables y seguros a menos que sepa cómo y en dónde implementarlos.

Necesitará saber en dónde está su compañía en riesgo y qué controles debe establecer para proteger sus sistemas de información. También tendrá que desarrollar una política de seguridad y planes para mantener su empresa en operación, en caso de que sus sistemas de información no estén funcionando.

**Controles de los sistemas de información**

Los controles de los sistemas de información pueden ser manuales y automatizados; consisten tanto de controles generales como de aplicación. Los controles generales gobiernan el diseño, la seguridad y el uso de los programas de computadora, además de la seguridad de los archivos de datos en general, a lo largo de toda la infraestructura de tecnología de la información de la organización.

En conjunto, los controles generales se asignan a todas las aplicaciones computarizadas y consisten en una combinación de hardware, software y procedimientos manuales que crean un entorno de control en general.

**Los controles generales:** cuentan con controles de software, controles de hardware físicos, controles de operaciones de computadora, controles de seguridad de datos, controles sobre la implementación de procesos de sistemas y controles administrativos. **(Ver tabla de descripción de controles generales)**

**Los controles de aplicación:** son controles específicos únicos para cada aplicación computarizada, como nómina o procesamiento de pedidos. Implican procedimientos tanto automatizados como manuales, los cuales aseguran que la aplicación procese de una forma completa y precisa sólo los datos autorizados. Los controles de aplicación se pueden clasificar como:

* **Los controles de entrada:** verifican la precisión e integridad de los datos cuando éstos entran al sistema. Hay controles de entrada específicos para autorización de la entrada, conversión de datos, edición de datos y manejo de errores.
* **Los controles de procesamiento:** establecen que los datos sean completos y precisos durante la actualización.
* **Los controles de salida:** aseguran que los resultados del procesamiento de computadora sean precisos, completos y se distribuyan de manera apropiada.

**Descripción de los Controles Generales**

|  |  |
| --- | --- |
| **Tipo de control general** | **Descripción** |
| **Controles de software** | Monitorean el uso del software de sistemas y evitan el acceso no autorizado de los programas de software, el software de sistemas y los programas de computadora. |
| **Controles de hardware** | Aseguran que el hardware de computadora sea físicamente seguro y verifican las fallas del equipo.  Las organizaciones que dependen mucho de sus computadoras también deben hacer provisiones para respaldos o una operación continua, de modo que puedan mantener un servicio constante. |
| **Controles de operaciones de TI** | Supervisan el trabajo del departamento de TI para asegurar que los procedimientos programados se apliquen de manera consistente y correcta al almacenamiento y procesamiento de los datos.  Implican controles sobre el establecimiento de trabajos de procesamiento de computadora y procedimientos de respaldo y recuperación para el procesamiento que termina en forma anormal. |
| **Controles de seguridad de datos** | Aseguran que los archivos de datos de negocios valiosos que se encuentren en disco o cinta no estén sujetos a un acceso sin autorización, no se modifiquen ni se destruyan mientras se encuentran en uso o almacenados. |
| **Controles de implementación** | Auditan el proceso de desarrollo de sistemas en varios puntos para asegurar que el proceso se controle y administre de manera apropiada. |
| **Controles administrativos** | Formalizan estándares, reglas, procedimientos y disciplinas de control para asegurar que los controles generales y de aplicación de la organización se ejecuten e implementen en forma apropiada. |

**Evaluación del riesgo**

Antes de que su compañía consigne recursos a los controles de seguridad y sistemas de información, debe saber qué activos requieren protección y el grado de vulnerabilidad de éstos. Una evaluación del riesgo ayuda a responder estas preguntas y a determinar el conjunto más eficiente de controles para proteger activos.

Una evaluación del riesgo determina el nivel de riesgo para la firma si no se controla una actividad o proceso específico de manera apropiada. No todos los riesgos se pueden anticipar o medir, pero la mayoría de las empresas podrán adquirir cierta comprensión de los riesgos a los que se enfrentan.

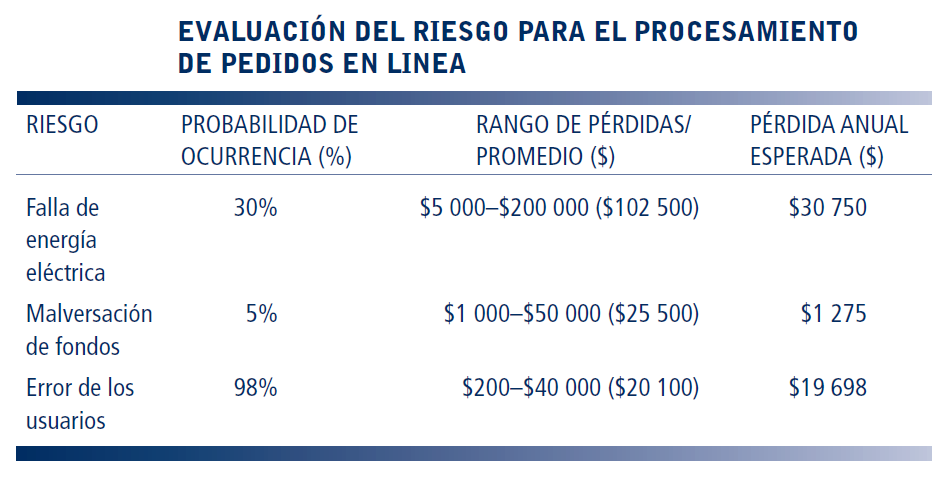
Los gerentes de información que trabajan con especialistas en sistemas de información deberían tratar de determinar el valor de los activos de información, los puntos de vulnerabilidad, la probable frecuencia de un problema y el potencial de daño.

Por ejemplo, si es probable que un evento ocurra no más de una vez al año, con un máximo de una pérdida de $1 000 para la organización, no es conveniente gastar $20 000 en el diseño y mantenimiento de un control para protegerse contra ese evento.

No obstante, si ese mismo evento podría ocurrir por lo menos una vez al día, con una pérdida potencial de más de $300 000 al año, podría ser muy apropiado invertir $100 000 en un control.

Una vez que se hayan evaluado los riesgos, los desarrolladores del sistema se concentrarán en los puntos de control con la mayor vulnerabilidad y potencial de pérdida.

La siguiente tabla muestra un ejemplo de evaluación de riesgos para una de pedidos o compras en línea.



**Planificación De Recuperación De Desastres Y Planificación De La Continuidad De Negocios**

Si opera una empresa, necesita planificar los eventos, como los cortes en el suministro eléctrico, las inundaciones, los terremotos o los ataques terroristas que evitarán que sus sistemas de información y su empresa puedan operar.

La planificación de recuperación de desastres idea planes para restaurar los servicios de cómputo y comunicaciones después de haberse interrumpido. El principal enfoque de los planes de recuperación de desastres es en los aspectos técnicos involucrados en mantener los sistemas en funcionamiento, tales como qué archivos respaldar y el mantenimiento de los sistemas de cómputo de respaldo o los servicios de recuperación de desastres.

**MasterCard** mantiene un centro de cómputo duplicado en Kansas City, Missouri, que sirve como respaldo de emergencia para su centro de cómputo primario en St. Louis. En vez de construir sus propias instalaciones de respaldo, muchas firmas se contactan con compañías de recuperación de desastres, como **Comdisco Disaster Recovery Services** en Rosemont, Illionois, y **SunGard Availability Services**, que tiene sus oficinas generales en Wayne, Pennsylvania. Estas compañías de recuperación de desastres proveen sitios activos con computadoras de repuesto en ubicaciones alrededor del mundo, en donde las firmas suscriptoras pueden ejecutar sus aplicaciones críticas en caso de emergencia.

**Champion Technologies**, que suministra productos químicos para utilizar en operaciones de petróleo y gas, puede cambiar sus sistemas empresariales de Houston a un sitio activo de **SunGard** en Scottsdale, Arizona, en sólo dos horas.

La planificación de continuidad de negocios se enfoca en la forma en que la compañía puede restaurar las operaciones de negocios después de que ocurre un desastre. El plan de continuidad de negocios identifica los procesos de negocios críticos y determina los planes de acción para manejar las funciones de misión crítica en caso de que fallen los sistemas.

Por ejemplo, el **Deutsche Bank**, que provee servicios de banca de inversiones y de administración de activos en 74 países distintos, tiene un plan bien desarrollado de continuidad de negocios que actualiza y refina en forma continua.

Mantiene equipos de tiempo completo en Singapur, Hong Kong, Japón, India y Australia para coordinar planes que tratan con la pérdida de instalaciones, personal o sistemas críticos, de modo que la compañía pueda seguir operando cuando ocurra un evento catastrófico.

El plan de **Deutsche Bank** hace la diferencia entre los procesos que son críticos para la supervivencia de los negocios y aquellos que son críticos para el apoyo en las crisis, y se coordina con la planificación de recuperación de desastres para los centros de cómputo de la compañía.

Los gerentes de negocios y los especialistas en tecnología de la información necesitan trabajar juntos en ambos tipos de planes para determinar qué sistemas y procesos de negocios son más críticos para la compañía. Deben realizar un análisis de impacto comercial para identificar los sistemas más críticos de la firma, además del impacto que tendría una falla de los sistemas en la empresa.

La gerencia debe determinar la máxima cantidad de tiempo que puede sobrevivir la empresa con sus sistemas inactivos y qué partes de la empresa se deben restaurar primero.

**Servicios y herramientas de software basadas en la nube**

El software basado en la nube y los datos que utiliza se alojan en poderosos servidores dentro de centros de datos masivos, y se puede acceder a éste mediante una conexión a Internet y un navegador Web estándar.

En vez de comprar e instalar programas de software, las compañías suscriptoras rentan las mismas funciones de estos servicios, en donde los usuarios pagan ya sea con base en una suscripción, o por cada transacción.

Hoy en día, a los servicios para ofrecer y proveer acceso al software de manera remota como un servicio basado en Web se les conoce como Software como un Servicio (SaaS). Un popular ejemplo es el de Salesforce.com que provee servicios de software bajo demanda para la administración de relaciones con el cliente.

Para poder administrar su relación con un subcontratista (outsourcer) o proveedor de servicio de tecnología, las empresas necesitan un contrato que incluya un Acuerdo de Nivel de Servicio (SLA).

El SLA es un contrato formal entre los clientes y sus proveedores de servicios, en el cual se definen las responsabilidades específicas del proveedor de servicios y el nivel de servicio que espera el cliente.

Por lo general, los SLA especifican la naturaleza y el nivel de servicios proporcionados, criterios para la medición del desempeño, opciones de soporte, provisiones de seguridad y **recuperación de desastres**, propiedad, actualizaciones de hardware y software, soporte al cliente, facturación, condiciones para terminar el acuerdo.

**Actividades en Clase:**

Basados en el análisis informal que se hizo la lección anterior más la información y los ejemplos del presente documento y por supuesto los documentos que ya han entregado hasta el momento, se requiere que los grupos trabajen en lo siguiente:

1. Confeccione una tabla que clasifique y evalúe los riesgos ya encontrados anteriormente, pero esta vez tomando en cuenta:
   1. Probabilidad de ocurrencia (%).
   2. Rango de perdidas promedio ($ Mensual).
   3. Pérdida Anual Esperada ($).
2. Identifique y proponga los controles generales y de aplicación para la empresa de estudio seleccionada por el grupo.
3. Basándose en las dos listas o tablas anteriores propongan al grupo posibles servicios, empresas y productos que puedan apoyar la continuidad del negocio de las empresas que estamos evaluando.