**B.O.B. Corp.**

**ANÁLISIS DE RIESGOS DEL DEPARTAMENTO**

Los Análisis de Riesgos han resultado ser una herramienta útil de los directivos técnicos en la industria para diseñar y operar las instalaciones haciendo énfasis en la seguridad. Para ello se han desarrollado diversas técnicas de carácter cualitativo y cuantitativo de evaluaciones de riesgo.

La flexibilidad que brindan estas técnicas y su poder de adaptabilidad para analizar el riesgo en industrias de diferente naturaleza, unido a los grandes beneficios que su aplicación les ha reportado en todos estos años, ha conducido a extender su aplicación a otros campos como es la Gestión Empresarial.

**Los principales riesgos informáticos de los negocios son los siguientes:**

**Riesgos de Integridad:** Este tipo abarca todos los riesgos asociados con la autorización, completitud y exactitud de la entrada, procesamiento y reportes de las aplicaciones utilizadas en una organización. Estos riesgos aplican en cada aspecto de un sistema de soporte de procesamiento de negocio y están presentes en múltiples lugares, y en múltiples momentos en todas las partes de las aplicaciones; no obstante estos riesgos se manifiestan en los siguientes componentes de un sistema:

**Interfaz del usuario:** Los riesgos en esta área generalmente se relacionan con las restricciones, sobre las individualidades de una organización y su autorización de ejecutar funciones negocio/sistema; teniendo en cuenta sus necesidades de trabajo y una razonable segregación de obligaciones.  Otros riesgos en esta área se relacionan a controles que aseguren la validez y completitud de la información introducida dentro de un sistema.

**Procesamiento**: Los riesgos en esta área generalmente se relacionan con el adecuado balance de los controles detectivos y preventivos que aseguran que el procesamiento de la información ha sido completado.  Esta área de riesgos también abarca los riesgos asociados con la exactitud e integridad de los reportes usados para resumir resultados y tomar decisiones de negocio.

**Procesamiento de errores**: Los riesgos en esta área generalmente se relacionan con los métodos que aseguren que cualquier entrada/proceso de información de errores (Exceptions) sean capturados adecuadamente, corregidos y reprocesados con exactitud completamente.

**Interfaz:** Los riesgos en esta área generalmente se relacionan con controles preventivos y detectivos que aseguran que la información ha sido procesada y transmitida adecuadamente por las aplicaciones.

**Administración de cambios:** Los riesgos en esta área pueden ser generalmente considerados como parte de la infraestructura de riesgos y el impacto de los cambios en las aplicaciones. Estos riesgos están asociados con la administración inadecuadas de procesos de cambios organizaciones que incluyen: Compromisos y entrenamiento de los usuarios a los cambios de los procesos, y la forma de comunicarlos e implementarlos.

**Información:** Los riesgos en esta área pueden ser generalmente considerados como parte de la infraestructura de las aplicaciones.  Estos riesgos están asociados con la administración inadecuada de controles, incluyendo la integridad de la seguridad de la información procesada y la administración efectiva de los sistemas de bases de datos y de estructuras de datos.  La **integridad puede perderse por:** Errores de programación (buena información es procesada por programas mal construidos), procesamiento de errores (transacciones incorrectamente procesadas) o administración y procesamiento de errores (Administración pobre del mantenimiento de sistemas).

**Riesgos de relación:** Los riesgos de relación se refieren al uso oportuno de la información creada por una aplicación.  Estos riesgos se relacionan directamente a la información de toma de decisiones (Información y datos correctos de una persona/proceso/sistema correcto en el tiempo preciso permiten tomar decisiones correctas).

**Riesgos de acceso:**Estos riesgos se enfocan al inapropiado acceso a sistemas, datos e información.  Estos riesgos abarcan: Los riesgos de segregación inapropiada de trabajo, los riesgos asociados con la integridad de la información de sistemas de bases de datos y los riesgos asociados a la confidencialidad de la información.  Los riesgos de acceso pueden ocurrir en los siguientes niveles de la estructura de la seguridad de la información:

**Procesos de negocio:** Las decisiones organizacionales deben separar trabajo incompatible de la organización y proveer el nivel correcto de ejecución de funciones.

**Aplicación:** La aplicación interna de mecanismos de seguridad que provee a los usuarios las funciones necesarias para ejecutar su trabajo.

**Administración de la información:** El mecanismo provee a los usuarios acceso a la información específica del entorno.

**Entorno de procesamiento**: Estos riesgos en esta área están manejados por el acceso inapropiado al entorno de programas e información.

**Redes:** En esta área se refiere al acceso inapropiado al entorno de red y su procesamiento.

**Nivel físico:** Protección física de dispositivos y un apropiado acceso a ellos.

**Riesgos de utilidad:** Estos riesgos se enfocan en tres diferentes niveles de riesgo:

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

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

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

**Riesgos en la infraestructura:** Estos riesgos se refieren a que en las organizaciones no existe una estructura información tecnológica efectiva (hardware, software, redes, personas y procesos) para soportar adecuadamente las necesidades futuras y presentes de los negocios con un costo eficiente.  Estos riesgos están asociados con los procesos de la información tecnológica que definen, desarrollan, mantienen y operan un entorno de procesamiento de información y las aplicaciones asociadas (servicio al cliente, pago de cuentas, etc.). Estos riesgos son generalmente se consideran en el contexto de los siguientes procesos informáticos:

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

Definición de las aplicaciones: Los procesos en esta área aseguran que las aplicaciones satisfagan las necesidades del usuario y soporten el contexto de los procesos de negocio.  Estos procesos abarcan: la determinación de comprar una aplicación ya existente o desarrollar soluciones a cliente.  Estos procesos también aseguran que cualquier cambio a las aplicaciones (compradas o desarrolladas) sigue un proceso definido que confirma que los puntos críticos de proceso/control son consistentes (Todos los cambios son examinados por usuarios antes de la implementación).

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

**Operaciones de red y computacionales:** Los procesos en esta área aseguran que los sistemas de información y entornos de red están operados en un esquema seguro y protegido, y que las responsabilidades de procesamiento de información son ejecutadas por personal operativo definido, medido y monitoreado.  También aseguran que los sistemas son consistentes y están disponibles a los usuarios a un nivel de ejecución satisfactorio.

**Administración de sistemas de bases de datos:** Los procesos en esta área están diseñados para asegurar que las bases de datos usadas para soportar aplicaciones críticas y reportes tengan consistencia de definición, correspondan con los requerimientos y reduzcan el potencial de redundancia.

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

**Riesgos de seguridad general**: Los estándar IEC 950 proporcionan los requisitos de diseño para lograr una seguridad general y que disminuyen el riesgo:

**Riesgos de choque de eléctrico:** Niveles altos de voltaje.

**Riesgos de incendio:** Inflamabilidad de materiales.

**Riesgos de niveles inadecuados de energía eléctrica**.

**Riesgos de radiaciones:** Ondas de ruido, de láser y ultrasónicas.

**Riesgos mecánicos:** Inestabilidad de las piezas eléctricas.

**TECNICAS DE PROCEDIMIENTOS PARA ADMINISTRAR RIESGOS**

**EVITAR RIESGOS:** Un riesgo es evitado cuando en la organización no se acepta. Esta técnica puede ser más negativa que positiva.  Si el evitar riesgos fuera usado excesivamente el negocio sería privado de muchas oportunidades de ganancia (por ejemplo: arriesgarse a hacer una inversión) y probablemente no alcanzaría sus objetivos.

**REDUCCION DE RIESGOS:** Los riegos pueden ser reducidos, por ejemplo, con: programas de seguridad, guardias de seguridad, alarmas y estimación de futuras pérdidas con la asesoría de personas expertas.

**CONSERVACION DE RIESGOS:** Es quizás el más común de los métodos para enfrentar los riesgos, pues muchas veces una acción positiva no es transferirlo o reducir su acción. Cada organización debe decidir cuales riegos se retienen, o se transfieren basándose en su margen de contingencia, una pérdida puede ser un desastre financiero para organización siendo fácilmente sostenido por otra organización.

**COMPARTIR RIESGOS**: Cuando los riesgos son compartidos, la posibilidad de pérdida es transferida del individuo al grupo.

**ANALISIS DE FODA DEL DEPARTAMENTO DE TI**