

Nuevos enfoques al riesgo operativo para instituciones financieras

Por: Raúl V. González Carrión, Gerente Risk Advisory, Deloitte Ecuador.

En vista de la rápida evolución del negocio, cambios en la gestión de procesos, nueva inclusión de tecnología y nuevos escenarios de eventos externos sobre los que se desenvuelven las instituciones financieras, cada vez es más necesario perfeccionar conceptos y procesos relacionados con las buenas prácticas de Continuidad del Negocio, Seguridad de la Información, Gestión de Proyectos, Gestión de la Calidad y Gestión de Ciber-riesgos con el claro objetivo de salvaguardar la información que es el insumo más importante de su giro de negocio.

En la región son varios los países que ya han acogido las mejores prácticas en su marco normativo y para el caso de Ecuador pronto podría ser necesaria su adopción. Por lo anterior, es importante conocerlas y evaluar su mejor implementación. A continuación, un breve resumen de lo que se abarca con estas prácticas y como se podría beneficiar su organización:

Continuidad del Negocio

Ahora llamado resiliencia empresarial, y se define como la capacidad de estar preparados para responder satisfactoriamente a eventos críticos (sean internos y externos) que afecten a cualquier Institución. Una organización debe identificar sus procesos críticos, objetivos, puntos y tiempos de recuperación, proveedores críticos, niveles mínimos de continuidad y relevar todos sus procedimientos de recuperación sea cual fuere el escenario, con el fin de siempre estar preparados. Implementar continuidad del negocio implica tener alineado los procesos de negocio y la tecnología.

Por lo anterior, las instituciones deben identificar escenarios a los cuales se tiene mayor exposición y es ahí donde un adecuado y bien enfocado análisis de riesgos de continuidad permite obtener todas las amenazas y vulnerabilidades para dar los planes de mitigación y protección correctos. Con base a esto, la organización tendrá planes bien estructurados y enfocados para hacer frente a eventos inesperados. Sin embargo, no por dejar de último la capacitación y concientización en estos temas a todos los interesados es vital para el funcionamiento adecuado.

El mayor beneficio de la implementación del modelo: Contar con un modelo integral que abarque planes de recuperación (tecnología, procesos, personas, recursos, entre otros) y permitan a la organización actuar en los máximos tiempos tolerables con el fin de evitar pérdidas financieras o de información, además de evitar paralizar sus operaciones.



Seguridad de la información

Varios ataques han implicado que muchas organizaciones vean afectado la confidencialidad, integridad o disponibilidad de la información. Contar con un sistema de gestión de seguridad de la información alineado al estándar ISO 27001, permitiría identificar procesos/productos/servicios críticos en temas de seguridad, identificar activos claves, evaluar los riesgos asociados con las amenazas y vulnerabilidades para así definir las acciones que permitan salvaguardarlos. Dichas respuestas enmarcadas en: mitigar, aceptar, transferir o evitar dichos riesgos. Una vez implementado el modelo la organización podría hacer frente a los incidentes de seguridad y gestionarlos efectivamente.

Con un adecuado alcance inicial al sistema de gestión de seguridad, permitirá a la Institución avanzar en el trabajo futuro y cubrir mediante controles y procedimientos de activos de información efectivos otros procesos que a posterior podrían ser incluidos en dicho modelo. Por lo anterior, es importante el punto de partida y tener una metodología estructurada para replicar, sin mayor esfuerzo, a los demás procesos.

El mayor beneficio de la implementación del modelo: Lograr que la información sea accesible al personal adecuado, se encuentre disponible cuando el usuario la requiere y sea modificada por el personal autorizado, siempre considerando lo que para la Institución es crítico como negocio con base a sus objetivos estratégicos.



Gestión de Proyectos

El día a día se realiza mediante pequeños y grandes proyectos, lo que marca la diferencia es gestionarlos correctamente a fin de enfocar mejor los esfuerzos, asignando correctamente los recursos.

Es así que tener un valor diferencial para aquellos proyectos con altos niveles de complejidad técnica y funcional, con demanda de grandes esfuerzos a la organización en términos de coordinación y asimilación de sus impactos, requieren de controles rigurosos respecto a:

- La calidad de los productos que generan.
- El cumplimiento de los plazos, cronogramas y presupuestos establecidos.
- La identificación temprana de riesgos y la consecuente ejecución de planes de acción para mitigarlos.
- Manejo efectivo de la comunicación.
- Gestión adecuada de los recursos humanos.

Dentro de una gestión efectiva de proyectos con un aseguramiento independiente se logra este cometido.

El mayor beneficio es: Lograr una gestión adecuada de sus recursos internos, mejorando la asignación de funciones, calidad en los proyectos, gestión de riesgos, plazos establecidos, comunicación de novedades y monitoreo constante con alertas tempranas.



Ciber-riesgos

Estudios indican que 4 de cada 10 organizaciones han sufrido una brecha de seguridad en los últimos 24 meses, dada la alta conectividad, dependencias a sistemas, servicios y proveedores en la nube derivan a que los temas de ciber-riesgos deban mantener un programa de ciberseguridad implementado.

Es importante que la Institución identifique las amenazas asociadas a los temas "Cyber" y determine su grado de exposición considerando los niveles de seguridad en los diferentes componentes tecnológicos, procesos, personas. Debe existir una adecuada capacitación y sensibilización en temas de ciber-seguridad que permitan a la organización de forma preventiva detener posibles ataques, en algunos casos los controles son correctivos, lo que hace más cara la recuperación cuando un ataque se materializa.

El mayor beneficio es: con un programa efectivo implementado se logra seleccionar controles adecuados para dar respuesta a los ciber-riesgos y aplicar las propias directrices en temas de seguridad, socializando a todos los involucrados. Identificando controles claves y clasificando su aplicación para obtener el mayor valor costo-beneficio.



Gestión de la calidad

Implementar una gestión adecuada de los procesos que permita considerar el contexto de la organización, gestión de calidad, enfoque al cliente, planificación de riesgos y oportunidades de mejora, consideración de recursos, esquemas de trazabilidad de mediciones, entre otros aspectos que permitan atender de mejor forma a todos los interesados, entregar productos y servicios con valores agregados y sobre todo el proceso de actualización y mejora continua.

Considerar que una adecuada gestión de calidad involucra a toda la organización identificar las partes interesadas, definir el liderazgo, compromiso y política de gestión con sus roles y responsabilidades, identificar los controles de planificación con sus productos y servicios claves y así poder realizar un seguimiento del desempeño por la dirección con una mejora continua del modelo a implementar.

El mayor beneficio: Trabajar con los factores procesos, personas, clientes para mejorar el enfoque de los servicios optimizando los recursos.

Con una adecuada organización e implementación de los modelos citados las Instituciones lograrán:

- Manejar de forma coordinada sus procesos.
- Administrará eficientemente sus proyectos.
- Controlará los eventos que afecten la continuidad y supervivencia de las operaciones de la institución.
- Salvaguardará su principal activo, la información, y gestionará correctamente los riesgos que se presenten.



Deloitte se refiere a Deloitte Touche Tohmatsu Limited, sociedad privada limitada por garantía en el Reino Unido ("DTTL"), y a su red de firmas miembro, y sus entidades relacionadas. DTTL y cada una de sus firmas miembro son entidades legales únicas e independientes. DTTL (también conocida como "Deloitte Global") no provee servicios a clientes. Conozca en www.deloitte.com/about la descripción detallada de la estructura legal de Deloitte Touche Tohmatsu Limited y sus firmas miembro.

Deloitte presta servicios de auditoría, consultoría, asesoría financiera, gestión de riesgo, impuestos y servicios relacionados a organizaciones públicas y privadas de diversas industrias. Con una red global de firmas miembro en más de 150 países y territorios, Deloitte brinda sus capacidades de clase mundial y servicio de alta calidad a los clientes, aportando la experiencia que necesitan para hacer frente a sus desafíos de negocios más complejos. Más de 225.000 profesionales de Deloitte están comprometidos en causar un impacto que trascienda.