SEVRI

1. Aspectos generales del SERVI:

* Ámbito de aplicación: aplica para las empresas con más de 30 funcionarios, que posean recursos mayores a 600 mil unidades y sea pública. Consiste en que la empresa deberá mantener en funcionamiento un SEVRI por áreas, sectores, actividades o tareas, de acuerdo con lo establecido anteriormente.
* Concepto del SEVRI: conjunto organizado de componentes de la Institución que interaccionan para la identificación, análisis, evaluación, administración, revisión, documentación y comunicación de los riesgos institucionales relevantes.
* Objetivo del SEVRI: Deberá producir información que ayuden a la empresa a la toma de decisiones para cumplir los objetivos.
* Productos del SEVRI: se crea una herramienta que apoye continuamente los procesos institucionales que contenga:
  + Información actualizada de los riesgos que impidan cumplir las metas requeridas
  + Medidas de contingencia para esos riesgos.
* Insumo del SEVRI: deberá poseer información interna y externa, que cumplan la presente normativa se debe considerar:
  + Planes nacionales, sectoriales e institucionales.
  + Análisis del entorno interno y externo.
  + Evaluaciones institucionales.
  + Descripción de la organización (procesos, presupuesto, sistema de control interno).
  + Normativa externa e interna asociada con la institución.
  + Documentos de operación diaria y de la evaluación periódica del desempeño del mismo
  + SEVRI.
* Características del SEVRI
  + Continuidad: componentes se establecen de manera permanente y las actividades se ejecutan constantemente.
  + Enfocado a resultados: componentes y actividades creadas para que la institución cumpla las metas.
  + Economía: componentes y actividades son prioritarias, y se ejecutan con herramientas existentes, buscando de reducir recursos.
  + Flexibilidad: se deberá actualizar, cuando los riesgos cambien.
  + Integración: funciona en conjunto con el resto de sistemas de la institución y se utiliza para la toma de decisiones.
  + Capacidad: el sistema deberá procesar la información interna y externa adecuadamente, que ayuden a cumplir los objetivos de la empresa.

Responsabilidad del SEVRI: los jefes son encargados de del establecimiento y funcionamiento del SEVRI, deberán:

* + Establecer y disponer las componentes del Sistema indicados en la sección Establecimiento.
  + Definir y ejecutar las actividades del Sistema indicados en la sección del funcionamiento del SERVI.
  + Evaluar y dar seguimiento al Sistema para verificar su eficacia y eficiencia en relación con el objetivo indicado en la directriz de objetivos de SEVRI
  + Verificar el cumplimiento de las responsabilidades establecidas en relación con el Sistema referidas en las directrices
  + Tomar las medidas necesarias para perfeccionar el Sistema y al cumplimiento de la presente normativa.
  + Comunicar a los sujetos interesados el estado del SEVRI y de las medidas que ha tomado para su fortalecimiento.

1. Establecimiento del SERVI.

* Descripción general: El funcionamiento del SEVRI se basa en:
  + Marco orientador.
  + Ambiente de apoyo.
  + Recursos.
  + Sujetos interesados.
  + Herramienta para la administración de información.
* Marco orientador: comprende la política de valoración del riesgo de la institución, además de la estrategia y la reglamentación, y deberá de contener al menos:
  + El enunciado de los objetivos de valoración del riesgo.
  + Los lineamientos institucionales para el establecimiento de niveles de riesgo aceptables,
  + La definición de las prioridades de la institución en relación con la valoración del riesgo.
  + Indicadores que permitan detectar el funcionamiento del SEVRI.
* Ambiente de Apoyo: La institución deberá de contar con una estructura organizacional, que apoye una cultura favorable al SERVI, promoviéndose lo siguiente:
  1. Conciencia en los funcionarios de la importancia de la valoración del riesgo para el cumplimiento de los objetivos institucionales.
  2. Uniformidad en el concepto de riesgo en los funcionarios de la institución.
  3. Actitud proactiva que permita establecer y tomar acciones anticipando las consecuencias que eventualmente puedan afectar los objetivos.
  4. Responsabilidades definidas claramente en relación con el SEVRI para los funcionarios de los diferentes niveles de la estructura organizacional.
  5. Mecanismos de coordinación y comunicación entre los funcionarios y las unidades internas para la debida operación del SEVRI.
* Recursos: se deberá contar con los recursos necesarios para el buen funcionamiento del SERVI.
* Sujetos interesados: Los sujetos interesados pueden ser internos o externos a la institución, y dentro de éstos, deberán incluirse al menos los siguientes grupos:
  1. Población objetivo de la institución,
  2. funcionarios de la institución, y sujetos de derecho privado que sean fiscalizadores de fondos públicos otorgados por la institución,
  3. Fiduciarios encargados de administrar fideicomisos constituidos con fondos públicos.

Los sujetos que forman parte de c) y d) deberán, al menos:

* + Brindar de forma periódica la información que requiera la institución, para determinar los riesgos asociados a dichos recursos.
  + Administrar los riesgos en relación con los recursos que recibe, según lo defina la institución que otorga los fondos o la que actúe como fideicomitente.
* Herramienta de apoyo para la administración de información: deberá una herramienta para los datos que generara el SERVI, y esta debe de contar con una bitácora de los riesgos, la herramienta deberá de cumplir estos aspectos:
  + relación costo beneficio,
  + volumen de información que debe procesar,
  + complejidad de los procesos organizacionales,
  + presupuesto institucional.

1. Funcionamiento del SERVI

* Descripción general: Las actividades para la documentación y comunicación de riesgos deberán realizarse, desde el inicio de operación del SERVI, de forma continua y paralela a las actividades que ejecuta el mismo.
* Identificación de riesgos: Se identificara por áreas, sectores, actividades, de conformidad con las particularidades de la institución, lo siguiente:
  + Los eventos que podrían afectar de forma significativa el cumplimiento de los objetivos institucionales.
  + Las posibles causas, internas y externas, y las posibles consecuencias de dichos eventos sobre el cumplimiento de los objetivos.
  + Las formas de ocurrencia de dichos eventos y el momento y lugar en el que podrían incurrir.
  + Las medidas de contingencia de riesgos existentes que se asocian con los riesgos identificados.
* Análisis de riesgos: para los eventos se tomara en cuenta: su posibilidad de ocurrencia, la magnitud de su eventual consecuencia a nivel de riesgo, sus factores de riesgo, y las medidas para su administración.
* Evaluación de riesgos: los riesgos se priorizaran tomando en cuenta lo siguiente: el nivel de riesgo, grado en que la institución puede afectar los factores de riesgo; la importancia de la solítica, proyecto, función o actividad afectado; y la eficacia y eficiencia de las medidas para la administración de riesgo existentes.
* Administración de riesgos: después de la evaluación de riesgos se debe establecer un plan de contingencia para cada riesgo tomando en cuenta: la relación costo-beneficio de llevar a cabo cada opción; la capacidad e idoneidad de los entes participantes internos y externos a la institución en cada opción; el cumplimiento del interés público y el resguardo de la hacienda pública; y la viabilidad jurídica, técnica y operacional de las opciones.
* Revisión de riesgos: en el transcurso de la ejecución del SERVI se debe de dar seguimiento a los riesgos, en estos puntos: el nivel de riesgo; los factores de riesgo; el grado de ejecución de las medidas para la administración de riesgos; la eficacia y la eficiencia de las medidas para la administración de riesgos ejecutadas.
* Documentación de riesgos: Deberá documentarse como mínimo su descripción, sus resultados esperados en tiempo y espacio, los recursos necesarios y responsables para llevarlas a cabo.
* Comunicación de riesgos: La institución deberá brindar periódicamente información a los sujetos interesados, internos y externos, de los riesgos institucionales, y viceversa.

1. Disposiciones Finales del SERVI

* Régimen sancionaría: los encargados que incumplan sus labores en el SERVI serán penalizados según la ley del régimen sancionatorio establecido en el artículo 39 de la Ley General de Control Interno.
* Obligatoriedad: De conformidad con el artículo 12 de la Ley Orgánica de la Contraloría General de la República y los artículos 3º y 18 de la Ley General de Control Interno, esta normativa es de acatamiento obligatorio. Cualquier otra normativa sobre valoración del riesgo que emitan entes u órganos que por ley regula o ejercen control externo sobre sujetos componentes de la Hacienda Pública, será complementaria a las emitidas por la Contraloría General, siempre y cuando su contenido no se oponga a lo establecido en la presente normativa, la cual prevalecerá.
* Implementación: Las presentes Directrices deben ser implementadas en forma gradual y programada por las administraciones, de conformidad con los parámetros que definirá la Contraloría General de la República. Para esos efectos la División de Fiscalización Operativa y Evaluativa de ese órgano contralor, determinará a través de la emisión de circulares específicas, la forma y el momento en que cada

Administración activa deberá ir implementando estas Directrices.

* Vigencia: Estas Normas entrarán a regir a partir del 1º de marzo del 2006.

Glosario

SERVI: Sistema Específico de Valoración Institucional.

Control interno TI

1. Normas de aplicación general:

* Marco Estratégico: Jerarcas debe de poner objetivos en la parte de TI, basado en un marco estratégico que respete las políticas de la institución
* Gestión de la calidad: La organización debe de proveer los recursos necesarios para que el departamento de TI desarrolle un trabajo eficiente.
* Gestión de Riesgos: Organización debe de poseer planes para la solución de los riesgos que afecten al departamento de TI
* Gestión de la seguridad de información: La organización debe proteger la información para que los datos privados de la empresa no salgan de la misma. Implementando políticas de seguridad cumpliendo los siguientes aspectos:
  + La implementación de un marco de seguridad de la información.
  + El compromiso del personal con la seguridad de la información.
  + La seguridad física y ambiental.
  + La seguridad en las operaciones y comunicaciones.
  + El control de acceso.
  + La seguridad en la implementación y mantenimiento de software e
  + infraestructura tecnológica.
  + La continuidad de los servicios de TI.

Además de establecer medidas de seguridad relacionadas ha:

* + El acceso a la información por parte de terceros y la contratación de servicios prestados por éstos.
  + El manejo de la documentación.
  + La terminación normal de contratos, su rescisión o resolución.
  + La salud y seguridad del personal.
* Implementación de un marco de seguridad:
  + Un marco metodológico que posea la información de los riesgos, y sus planes de contingencia.
  + Actualizando este marco periódicamente.
  + Posee una bitácora de las responsabilidades.
* Compromiso del personal con la seguridad e información: el personal debe de conocer y poseer un reglamento de confidencialidad, para eso se debe:
  + Capacitar al personal de TI sobre el reglamento
  + Mecanismos de cumplimiento de normas
  + Poseer normas específicas para casos específicos
* Seguridad física y ambiental : La organización debe de proteger sus recursos humano y material, brindando las condiciones adecuadas para su buen funcionamiento, como parte de la protección considerar lo siguiente:
  + Controles de acceso a las instalaciones
  + Componentes físicos, ubicados en una zona segura
  + Control en el mantenimiento del equipo
  + Control en el desecho de los artículos malos
  + Continuidad y seguridad de las redes de comunicación y electricidad
  + Registro de acceso de terceros
  + Riesgos asociados al ambiente
* Seguridad en las operaciones y comunicaciones :Normas relacionadas a la operación de recursos de TI tomando en cuenta
  + Mecanismos que permitan la no negación y seguridad de las transacciones de información
  + Procedimiento para el manejo de la información almacenada, y el manejo adecuado de los desechos, de los instrumentos que contengan esta información
  + Establecer medidas para el manejo de los malware o virus
* Control de acceso: protección de la información de acceso no autorizado cumpliendo
  + Normas relacionadas al acceso de la información y a las herramientas que la manejan
  + Clasificar los recursos de TI de acuerdo a los términos de sensibilidad
  + Definir propiedad, custodia y responsabilidad sobre los recursos de TI
  + Establecer procedimiento para la jerarquía del personal que accede a la información o utiliza los recursos
  + Asignar derechos de acceso a la información o recursos según su puesto jerárquico
  + Implementar maneras de autentificación de las personas que utilizan los recursos de TI
  + Establecer controles de acceso a la información impresa o visible en pantallas y proteger estos medios
  + Manejar de manera restringida la información sobre la seguridad de TI
* Seguridad en la implementación y mantenimiento de software e infraestructura tecnológica: Integridad en los procesos de implementación y mantenimiento de software e infraestructura tomando en cuenta:
  + Definir los requerimientos de seguridad en el mantenimiento y la infraestructura
  + Contar con procedimientos para el mantenimiento y puesta a producción
  + Acceso restringido en los ambientes de desarrollo, mantenimiento y producción
  + Controlar acceso a los programas fuente ya los datos de prueba
* Continuidad de los servicios de TI: continuidad razonable y la interrupción no puede provocar problemas a los demás usuarios
* Gestión de proyectos: administrar los proyectos de TI de manera que se cumplan las metas adecuadamente
* Decisiones sobre asuntos estratégicos de TI: El jerarca debe apoyar las decisiones sobre el futuro de TI y el cumplimiento de sus metas
* Cumplimiento de obligaciones relacionadas con la gestión de TI: velar por el cumplimiento del marco jurídico que se relacionan con TI

1. Planificación y organización

* Planificación de las tecnologías de información: Ti debe estar incluida en el cumplimiento de las metas de la organización
* Modelo de arquitectura de información: La organización debe de optimizar la integración de los sistemas para que muestren adecuadamente la información correspondiente
* Infraestructura tecnológica: la organización debe de tener meta fija y utilizar los recursos de TI adecuados para cumplirlas
* Independencia y recurso humano de la función de TI: El jerarca debe de asegurar la independencia del departamento de TI, sin perder la comunicación entre ellas
* Administración de recursos financieros: se deben de optimizar los recursos para el cumplimiento de los objetivos de la empresa

1. Implementación de tecnologías de información

* Consideraciones generales de la implementación de TI: mantener las TI de acuerdo en el marco estratégico para esto se debe:
  + Adoptar políticas para la implementación o mantenimiento de TI
  + Establecer un respaldo de los proyectos de TI
  + Garantizar la participación activa, de sus responsabilidades, y aprobar las implementaciones realizadas
  + Instaurar líderes de proyectos de manera clara
  + Analizar alternativas de solución con los lineamientos previamente establecidos
  + Definición clara de los requerimientos
  + Poseer previsiones para el manejo de los recursos y su agotamiento
  + Estrategias para que los proyectos cumplan sus objetivos
  + Promover independencia en hardware y software
* Implementación de software: se debe implementar software que satisfaga las necesidades de los usuarios tomando en cuenta:
  + Que aplique la norma de implementación de TI
  + Desarrollar un marco metodológico que contemplen los pasos del desarrollo de un proyecto
  + Establecer controles y asignar funciones al personal del proyecto
  + Comprobar la implementación del software en el ambiente de desarrollo
  + Definir criterios para los cambios que se realizaran
  + Controlar las versiones del programa que se desarrolla
* Implementación de infraestructura tecnológica: instalar la arquitectura que cumpla los requerimientos mínimos del software
* Contratación de terceros para la implementación y mantenimiento de software e infraestructura: la organización debe de contratar a los terceros que satisfagan sus necesidades como por ejemplo:
  + Que cumplan con las normas de implementación de hardware y software
  + Establecer una política para la contratación
  + Contar con una justificación de peso para subcontratar a terceros
  + Procedimientos para los términos de referencia
  + Aprobar criterios términos y pruebas de aceptación
  + Implementar un proceso de transición que cause los menores problemas posibles

1. Prestación de servicios y mantenimiento

* Definición de administración de acuerdos d servicio: claridad en los servicios que se requieren y los que se poseen. Se debe definir claramente los servicios y sus costos, definiendo las responsabilidades de los actores, que se adecuen al reglamento establecido, y actualizarlos periódicamente
* Administración de la plataforma tecnológica: Mantener una plataforma que falle lo menos posible tomando en cuenta: una reglamentación, vigilar los recursos físico, velar por los riesgos y futuros cambios de plataforma, mantener separados los ambientes de producción y desarrollo, definir rutinas de respaldo, y controlar los servicios externos
* Administración de datos: velar que los datos se procesen según las normas de la compañía
* Atención de los requerimientos de los usuarios de TI: Cumplir la peticiones de TI adecuadamente
* Manejo de incidentes: manejar adecuadamente los incidentes ocurridos en TI
* Administración de servicios prestados por terceros: organización debe velar que los servicios a terceros satisfagan los requerimientos de la empresa.

1. Seguimiento

* Seguimiento de los procesos de TI: La organización debe asegurar el logro de los objetivos propuestos como parte de la gestión de TI, para lo cual debe establecer un marco de referencia y un proceso de seguimiento en los que defina el alcance, la metodología y los mecanismos para vigilar la gestión de TI. Asimismo, debe determinar las responsabilidades del personal a cargo de dicho proceso.
* Seguimiento y evaluación del control interno en TI: El jerarca debe establecer y mantener el sistema de control interno asociado con la gestión de las TI, evaluar su efectividad y cumplimiento y mantener un registro de las excepciones que se presenten y de las medidas correctivas implementadas.
* Participación de la Auditoría Interna: La actividad de la Auditoría Interna respecto de la gestión de las TI debe orientarse a coadyuvar, de conformidad con sus competencias, a que el control interno en TI de la organización proporcione una garantía razonable del cumplimiento de los objetivos en esa materia.