PORTAFOLIO DE RIESGOS SEVRI-PJ

El documento que se desarrolla a continuación tiene como propósito orientar el trabajo que deben realizar los despachos y oficinas del Poder Judicial, con base en la administración del riesgo, de conformidad con lo establecido en la Ley general de control interno, vigente desde el 04 de setiembre de 2002, el Manual de normas de control interno y la normativa complementaria definida por la Contraloría General de la República y la Administración Superior del Poder Judicial.

Es pertinente aclarar que este portafolio de riesgos proporciona un marco mínimo de observación para la gestión de riesgos, que se complementa con la aplicación de la Metodología del SEVRI-PJ, aprobada por el Consejo Superior en la sesión N° 32-06, artículo XL, del 09 de mayo de 2006; así como con la naturaleza y situaciones particulares de cada despacho u oficina judicial.

Tomando en consideración que se deben gestionar los riesgos relevantes[1] que podrían evitar o dificultar el **logro de los objetivos del Poder Judicial**, a continuación se establecen una serie de aspectos básicos a considerar por los despachos y oficinas judiciales para un apropiado control de los riesgos identificados. Es oportuno indicar que al final de este portafolio de riesgos se incluye un glosario con términos técnicos para la gestión de riesgos, con el fin de orientar el trabajo por realizar.

1. Existen dos estados generales para la gestión de riesgos:

   1.1. **La fase inicial cuando se identifican y valoran los riesgos, así como la propuesta de las acciones concretas para llevar dichos riesgos a un nivel bajo aceptable para la organización**, en los términos establecidos por la Directriz R-CO-64 de la Contraloría General de la República, emitida el 1 de julio de 2005 y que entró en vigencia el primero de marzo de 2006. En esta etapa, los despachos cuentan con los conocimientos fundamentales para iniciar la gestión de riesgos.

   1.2. **Con la gestión de riesgos en funcionamiento**, cuando se evalúa la funcionalidad del sistema de control interno, en cuanto al apoyo que brinda para asegurar razonablemente el cumplimiento de los objetivos. Se trata de despachos con un grado de madurez medio o alto en la gestión de riesgos y las labores van enfocadas a verificar periódicamente la apropiada funcionalidad de las actividades de control y el éxito de las gestiones definidas para administrar los riesgos valorados. Se realizan los ajustes pertinentes.

Es necesario tener prudencia al definir el detalle con que se va a realizar el diseño y la implementación de los controles que se asocien a los riesgos valorados, pues podrían asignarse recursos y esfuerzos a acciones que aporten poco o nada a la gestión de los riesgos vinculados con los objetivos relevantes de la organización. En todo caso, para cualquier acción o control a implementar, es requisito indispensable realizar un estudio de costo-beneficio para la toma de decisiones pertinente.

La documentación para verificar la funcionalidad de los controles depende del tamaño de la organización. Por ejemplo, un despacho u oficina con más de 20 personas, debería tener procedimientos formales para que la jefatura se asegure razonablemente que los controles funcionan apropiadamente, como es el caso de la realización de inventarios de evidencias y expedientes, los

[1] La calificación de la relevancia del riesgo es criterio del Equipo de gestión de riesgos que haga la valoración, sin embargo, se tomarán en cuenta al menos las prioridades de la organización, establecidas en el Marco orientador del SEVRI-PJ, aprobado por la Corte Plena en sesión 07-06, artículo XXIV, del 3 de abril de 2006, así como el nivel de impacto y la probabilidad de ocurrencia del riesgo.

arqueos y las conciliaciones periódicas. En oficinas más pequeñas, podría ser suficiente con la observación directa de la jefatura (supervisión documentada) sobre la ejecución de las funciones asignadas, para obtener una idea clara de la funcionalidad de los controles establecidos.

El grado de formalidad de la documentación de la gestión de riesgos debe estar acorde con la normativa aplicable y circulares emitidas por la Administración Superior sobre este particular, tomando en consideración que siempre **debe existir evidencia de que los controles para gestionar los riesgos fueron diseñados y funcionan apropiadamente**.

El **Portafolio de riesgos del SEVRI-PJ** se estableció con base en la documentación aportada sobre los riesgos identificados y valorados, por más de 650 equipos de gestión de riesgos que fueron capacitados en talleres del Sistema específico de valoración del riesgo institucional; en los cuales han participado más de 3000 personas que laboran en despachos de todo el país.

Es pertinente mencionar que este portafolio de riesgos está definido de manera general y validado en función de aquellos objetivos considerados relevantes en nuestra organización y que forman parte de la planificación operativa de los despachos judiciales y además, su propósito principal es servir de guía para el trabajo de los equipos de gestión de riesgos, por lo cual no es un listado exhaustivo y por tanto se le podrán agregar otros riesgos si las circunstancias lo ameritan o como producto del avance en el grado de madurez de la gestión de riesgos que la organización vaya alcanzando; de tal manera que se publicará una versión electrónica actualizada de dicho documento al menos una vez al año.

El portafolio de riesgos del SEVRI-PJ está estructurado de la siguiente forma:

1. Riesgos externos (RE)

Son los eventos relevantes que se producen en el entorno de la organización y que, aún cuando el sistema de control interno no pueda actuar sobre ellos, en vista de que pueden impactar negativamente a la organización, es necesario estar alerta ante su comportamiento, concentrando los esfuerzos en predefinir las acciones a ejecutar cuando uno de estos riesgos se hace realidad; con el propósito de mitigar el impacto de sus consecuencias negativas.

La estructura mínima de riesgos externos que se deben valorar con el SEVRI-PJ es:

1.1. Riesgos de tipo legal

Son eventos vinculados con el cumplimiento de las leyes, decretos, normas, reglamentos y afines que se aprueban y que deben ser observadas en la ejecución de las funciones que se ejecutan en la organización, tales como:

1.1.1. Aprobación de nueva normativa (Leyes, decretos, acuerdos):

Genera cambios en las funciones por realizar, aumento de la carga de trabajo, incrementa las necesidades de capacitación, así como las expectativas de mayor calidad de servicio por parte de la ciudadanía. Por lo general se requieren recursos presupuestarios que no están previstos en la nueva legislación aprobada, lo cual también ocasiona serios trastornos al proceso de planificación de la entidad.

Las fuentes más comunes de este tipo de riesgos son: aprobación de nuevas leyes y decretos; normativa de la Contraloría General de la República y del Ministerio de Hacienda, dictámenes de la Procuraduría General de la República, circulares y otras disposiciones de la administración, etc.

Estrategias de control

Dar un seguimiento constante al entorno de la organización (proyectos de ley en la corriente legislativa, decisiones del gobierno central y otras entidades públicas, actividad de la Contraloría general de la república, noticias de prensa); así como a la documentación que se genera a lo interno del Poder Judicial, tal como actas de Corte y Consejo Superior, circulares, etc.

1.1.2. Sentencias judiciales

Son votos de las salas de la Corte Suprema de Justicia, así como sentencias de tribunales y juzgados, que generen cambios en la forma en que se desarrolla el trabajo o la calidad del servicio que se brinda. En muchos casos, este tipo de riesgo produce un aumento de demanda de personal, que aunado a los recursos de infraestructura y tecnología que requieren las nuevas personas contratadas, pueden ocasionar un desequilibrio presupuestario y aumentar el retraso judicial.

Estrategias de control

Seguimiento que se pueda dar a través de la consulta de las actas de Corte y Consejo Superior, sistemas de información en intranet judicial, comunicaciones internas, entre otras.

1.2. Fallas en las relaciones con otras dependencias

Se producen por la necesidad de realizar gestiones con diversas dependencias externas, ya sea con un despacho en particular o con una entidad externa, en las cuales pueden ocurrir errores, malos entendidos, falta de colaboración, etc., que ocasionen perjuicios a la tramitación. El impacto negativo de este tipo de evento se incrementa cuando hay cambios de gobierno o de jerarcas de alguna entidad pública con la cual se deben realizar trámites legales o se tiene algún tipo de acuerdo formal de cooperación o coordinación, o casos similares.

Ejemplos de este tipo de entidades pueden ser: Ministerio de seguridad pública, Policía de tránsito, PANI, ICE, entidades bancarias, municipalidades, organizaciones comunales, proveedores, arrendadores, contratistas, entre otros.

Estrategias de control

Valorar acciones tales como realizar esfuerzos para mantener una apropiada coordinación con entidades externas, promover la firma de convenios que se cumplan independientemente de que haya cambio de jefaturas, establecer canales de comunicación permanentes y dar seguimiento a las gestiones realizadas, establecer protocolos de actuación, aplicar un control de garantías y de ejecución de contratos.

1.3. Cambios en el entorno económico y social

Puede incluir políticas presupuestarias del gobierno central o de la administración superior, variaciones del tipo de cambio o tipos de interés, eventos estacionales (recolección de café, temporada de vacaciones, pago de aguinaldo y salario escolar), cambios en los índices de criminalidad, actividad de grupos de presión, intentos de corrupción, nuevos proyectos industriales o de entidades públicas. Este tipo de eventos producen un aumento del circulante y por tanto de la carga de trabajo, que generalmente los despachos deben afrontar con el mismo personal.

Estrategias de control

Seguimiento constante del entorno para solicitar con antelación refuerzos para momentos "picos" de actividad judicial o la actualización de los requerimientos de recursos materiales y personal, ya sea temporal o permanente, para evitar el deterioro del servicio.

Ejecutar un plan permanente de fortalecimiento de los valores y principios éticos que deben regir el comportamiento del personal en la ejecución de las funciones asignadas.

1.4. Cambios en el entorno tecnológico y de servicios

Son eventos que afecten las plataformas tecnológicas (nuevos sistemas y equipos, ataques de virus, ampliación de servicios, acción de hackers), fallas de los servicios tecnológicos y de fluido eléctrico, dependencia de proveedores, etc.; que generan suspensión del servicio, retrasos en la tramitación, aumento de costos, malestar del personal y de las personas usuarias, vencimiento de plazos, entre otros.

Estrategias de control

Establecer un plan de continuidad del servicio que se active si uno de estos riesgos se hace realidad, de tal forma que se pueda mitigar el impacto, especialmente en cuanto al deterioro de la calidad del servicio. Este plan debe estar en concordancia con el plan de continuidad del servicio institucional.

En caso de pérdida o destrucción de datos, es necesario contar con apropiados respaldos de las bases de datos de los sistemas de información vitales, de conformidad con los procedimientos que al respecto haya definido el Comité gerencial de Tecnología de información y la Dirección de Tecnología de Información (Dirección de TI).

Para los equipos vitales, definir un plan de sustitución de equipo, con base en parámetros de obsolescencia proporcionados por la Dirección de TI, con el fin de disminuir la probabilidad de falla por el uso de activos con la vida útil agotada.

Establecer un protocolo para la definición de los términos de referencia y la ejecución de los contratos de desarrollo de software.

1.5. Cambios en el entorno ambiental

Son eventos tales como inundaciones, terremotos, incendios, contaminación, actividad volcánica, etc., que podrían ocasionar perjuicios materiales y lesiones a la integridad física de las personas usuarias y las que laboran para la organización. También se podría generar situaciones tales como la suspensión de audiencias, dificultad o imposibilidad de acceso a los servicios de justicia, un aumento de costos e inclusive tener que afrontar demandas que también deterioren la imagen de la institución.

Estrategias de control

Establecer un plan de emergencias que se active si uno de estos riesgos se hace realidad, de tal forma que se pueda mitigar el impacto, especialmente en cuanto al deterioro de la calidad del servicio y el menoscabo de la integridad física o la salud de las personas afectadas. Dicho plan debe estar en concordancia con el plan de continuidad del servicio institucional.

2. Riesgos internos (RI)

Son los eventos relevantes que se producen dentro de la organización y que pueden ser apropiadamente gestionados si se cuenta con un robusto sistema de control interno. En este caso las respuestas al riesgo deben estar enfocadas principalmente a labores de prevención, es decir, a evitar que el riesgo se produzca. En el caso de que, aún con las medidas de control correctas y suficientes, el riesgo se haga realidad, deben estar definidas las acciones para minimizar el daño que produzca.

Con base en los datos recopilados sobre la identificación de riesgos realizada en los talleres del SEVRI-PJ, la estructura mínima de riesgos internos que se debe gestionar se compone de cinco grandes áreas en las cuales cualquier riesgo relevante que se produzca, pondría en serias dificultades a la organización como un todo; por lo cual las acciones para su control o mitigación deben ir dirigidas a brindar soluciones integrales, para maximizar el uso de los recursos disponibles. Dicha clasificación se detalla seguidamente:

2.1. Riesgos de Gestión

Son eventos vinculados con la ejecución de las funciones cotidianas asignadas a los despachos y oficinas judiciales, que por lo general están formalmente establecidas por la organización. De conformidad con la experiencia acumulada en nuestra entidad, los riesgos más relevantes que deben ser gestionados son:

2.1.1. Extravio o pérdida de expedientes o documentos confidenciales

Este riesgo siempre está latente en los despachos y oficinas judiciales por varias razones, entre las cuales tenemos: alto volumen de documentación, hacinamiento, rotación de personal, falta de inventarios y arqueos, desactualización de las bases de datos, descuido o negligencia del personal, actos de corrupción. Además de los expedientes judiciales, también existe variedad de documentos

de uso delicado: títulos valores, evidencia documental, boletas de seguridad, cheques, expedientes de contrataciones administrativas, informes de los órganos fiscalizadores y disciplinarios, entre otros.

Este tipo de situaciones podrían ocasionar serias consecuencias, tales como retraso en la tramitación, impunidad, revictimización, fuga de información, procesos disciplinarios, pérdidas patrimoniales y desconfianza entre el personal

Estrategias de control

Este riesgo, por su naturaleza, tiene la particularidad de que puede haberse hecho realidad sin que nos hayamos percatado de ello pues, por ejemplo, un expediente o documento puede llevar días o incluso meses de haber sido sustraído o estar incorrectamente archivado, pero esa condición se detecta hasta que es requerido para realizar algún trámite; lo cual nos obliga a estar siempre alerta y realizar inventarios periódicos y sorpresivos para corroborar que el inventario físico coincide con los datos del sistema de control de expedientes y documentos del despacho; así como para enviar a archivo aquellos que cumplan con los requisitos para este trámite.

Es pertinente llevar un estricto control de entrada y salida de expedientes y documentos de uso delicado ya sea para su traslado a otro despacho, para fotocopiado o cualquier otro trámite. Esto se logra apropiadamente con el establecimiento de una bitácora, preferiblemente electrónica, donde se registren los movimientos fuera del despacho de este tipo de documentación.

Otra actividad de control esencial corresponde a la ejecución de labores de supervisión, con el fin de corroborar que la documentación confidencial está debidamente custodiada y que existen procedimientos para su acceso restringido solo a las personas legalmente autorizadas.

Con respecto a la desactualización de las bases de datos, lo que corresponde es recordar periódicamente a las personas del despacho la obligación de poner al día los datos de estados y movimientos de los expedientes, tal y como reiteradamente lo ha establecido la Administración superior en sendas circulares.

Ejecutar un plan permanente de fortalecimiento de los valores y principios éticos que deben regir el comportamiento del personal en la ejecución de las funciones asignadas.

2.1.2. Suspensión de audiencias

En este caso, se trata específicamente de las audiencias que no se realizan debido a causas a lo interno de la organización. Es el caso de errores en el proceso de citación o notificación, falta de coordinación entre despachos, ausencia de personal clave para realizar el trámite, fallas en los equipos o servicios de tecnología de información; continuación de audiencias anteriores, ausentismo, “choques” de agenda, etc.

Entre las consecuencias de este tipo de situaciones tenemos la revictimización, incremento del circulante, prescripción de causas, aumento de la carga de trabajo, mayores costos de operación, procedimientos disciplinarios, demandas y pérdida de credibilidad.

Estrategias de control

Es necesario revisar que antes de cada audiencia, todos los trámites previos necesarios se hayan realizado apropiadamente, incluyendo la prueba del buen funcionamiento de los equipos y suministros informáticos. También es una buena práctica la de recordar a las partes, con anterioridad, el día y hora en que se realizará la audiencia para verificar que el proceso de citación o notificación fue efectivo.

En los casos en que corresponda, verificar que las acciones de coordinación con otras oficinas a lo interno o externo de la organización, se realizaron efectivamente.

2.1.3. Retraso en la tramitación

Existen múltiples causas por las cuales se puede dar el retraso en la tramitación, ya sea en el ámbito jurisdiccional, administrativo o auxiliar de justicia. Entre los motivos más comunes tenemos: alto volumen de trabajo, bajo desempeño, falta de capacitación, rotación de personal, fallas en los sistemas de información y comunicaciones, daños en los equipos, tardanza en recibir soporte técnico, inconvenientes para trasladarse a zonas alejadas o de difícil acceso, datos incorrectos o incompletos brindados por las personas usuarias, aumento de la complejidad de delitos y actos de corrupción.

De igual manera, las consecuencias negativas de este tipo de riesgo son múltiples y algunas de ellas podrían ser: vencimiento de plazos, prescripción de causas, impunidad, revictimización, malestar de las personas usuarias, aumento de costos y de carga de trabajo, procesos disciplinarios, malestar del personal y pérdida de credibilidad.

Estrategias de control

Para este tipo de evento, debe hacerse énfasis en acciones preventivas que están ligadas a la fortaleza del sistema de control interno, para lo cual es esencial contar con indicadores de desempeño, asignación de cargas de trabajo equitativas, contar con un programa continuo de capacitación, procurar una pronta respuesta cuando se presenta una falla en los sistemas o equipos necesarios para realizar el trabajo, programar las giras y coordinarlas con las instancias pertinentes, corroborar los datos que se reciben de las personas usuarias, mejorar las competencias del personal.

Ejecutar un plan permanente de fortalecimiento de los valores y principios éticos que deben regir el comportamiento del personal en la ejecución de las funciones asignadas.

2.1.4. Amenazas de Seguridad: agresiones, daños a la propiedad, robos, vandalismo, apropiación indebida de información o activos

Este tipo de evento es más evidente en los despachos que están aislados y que, en la mayoría de los casos, se encuentran en locales alquilados, sin embargo, también los edificios judiciales son susceptibles de enfrentar este tipo de riesgo especialmente por la naturaleza de nuestra organización, que frecuentemente es visitada por personas que manejan algún tipo de conflicto, por lo cual las funcionarias y funcionarios judiciales, así como las personas usuarias, podrían sufrir lesiones a su integridad física. Además, la infraestructura física y los activos necesarios para realizar las funciones

asignadas pueden ser dañados por robos y destrucción, con lo cual se compromete la continuidad del servició público y se incurre en costos de sustitución antes de que se extinga la vida útil de estos recursos.

Otras consecuencias negativas para la organización podrían ser la indisposición del personal, enfrentar demandas y pérdida de credibilidad.

Estrategias de control

Las acciones preventivas son las más apropiadas para controlar este tipo de riesgo, especialmente en cuanto a la puesta en práctica de medidas para la protección de las personas y evitar dejar al alcance de personas extrañas a la oficina los materiales o equipos que eventualmente podrían convertirse en armas; así como establecer requerimientos mínimos para las instalaciones alquiladas.

Es necesario que la organización realice un esfuerzo para que todos los despachos del país cuenten con personal de seguridad, ya sea propio o contratado, pues si un riesgo de este tipo se hace realidad, los efectos pueden ser muy graves, especialmente porque se debe proteger la integridad física de personas usuarias y el personal de la organización.

El control del ingreso de las personas a los edificios es esencial para minimizar la ocurrencia de este tipo de riesgo, así como la gestión para acondicionar apropiadamente los locales alquilados. Principalmente en los edificios judiciales, es conveniente que el personal de seguridad rote sus puestos, pues al permanecer por un extenso tiempo en un solo lugar, tienden a caer en excesos de confianza que se convierten en una vulnerabilidad más para el esquema de protección implantado.

2.1.5. Pérdida o desactualización de datos electrónicos

Es necesario detallar este riesgo por separado debido a la significativa inversión en tecnología de información y comunicaciones que ha realizado el Poder Judicial, como base para promover la excelencia del servicio a las personas usuarias y agilizar los procesos judiciales, especialmente con la introducción de la oralidad.

Dicha inversión hace que se cree una gran dependencia de los recursos de tecnología de información tales como: sistemas automatizados, equipos para el procesamiento y almacenamiento de datos, equipos y materiales para comunicaciones, etc. para los cuales es indispensable la activación de un esquema de seguridad que proteja los datos contra su pérdida, destrucción o acceso no autorizado, así como para que asegure razonablemente que estén disponibles oportunamente.

Entre las consecuencias de este tipo de riesgos podemos citar: retraso en la tramitación, aumento de la carga de trabajo, revictimización, impunidad, vencimiento de plazos, procesos disciplinarios, demandas, incremento de costos, malestar del personal y pérdida de credibilidad.

Estrategias de control

En relación con la pérdida de datos, es esencial contar con un esquema de seguridad definido formalmente y que se actualice constantemente, debido a que existen muchas vulnerabilidades inherentes a los activos electrónicos y también debido al acelerado ritmo con que se desarrollan las tecnologías de información y comunicaciones, que aceleran la obsolescencia de estos activos.

Con respecto a la desactualización de las bases de datos, lo que corresponde es recordar periódicamente a las personas del despacho la obligación de poner al día los datos de estados y movimientos de los expedientes, tal y como reiteradamente lo ha establecido la Administración superior en sendas circulares.

También es apropiado ejecutar un plan permanente para el fortalecimiento de los valores y principios éticos que deben regir el comportamiento del personal en la ejecución de las funciones asignadas.

2.1.6. Fallas en responsabilidad social organizacional

Esta situación se puede dar debido a falta de prácticas formales relacionadas con la gestión responsable, sostenible y transparente, lo cual puedo deteriorar la imagen de la organización con entidades internacionales y gubernamentales, asociaciones ambientalistas y en general la comunidad en la que se desarrolla un despacho u oficina judicial. Aspectos tales como contaminación, generación de residuos, uso ineficiente de energía y agua, desperdicio de papel e instalaciones inapropiadas pueden provocar la indisposición del personal, el malestar de las personas usuarias y deteriorar la imagen de la organización, así como el enfrentar demandas.

Estrategias de control

Este es un amplio campo de acción en el cual se hace necesario establecer una política de la organización para cumplir con la responsabilidad social que le corresponde como entidad pública. Los programas ya existentes patrocinados por la Comisión ambiental y la Comisión de cero papeles deben ser fortalecidos con el fin de enviar un claro mensaje a la comunidad nacional con respecto al compromiso que tiene el Poder Judicial en estos aspectos.

2.2. Riesgos de Ética

2.2.1. Ausentismo frecuente

Se refiere a cuando el personal se ausenta del despacho para realizar trámites personales o cumplir con alguna gestión del despacho. Es el caso de citas médicas, trámites bancarios, trámites en otros despachos judiciales, incapacidades sin sustitución, asistencia a actividades de capacitación, entre otros. Entre las consecuencias de esta situación están el retraso en la tramitación, suspensión de audiencias u otros trámites similares, molestias para las personas usuarias, malestar del personal, procesos disciplinarias, pérdida de imagen.

Estrategias de control

En vista de que muchos de los eventos mencionados son inevitables, lo que corresponde en estos casos es mitigar el impacto de este tipo de situaciones ya sea redistribuyendo equitativamente la carga de trabajo del personal que se ausenta y tratar de evitar la realización de trámites personales en el horario de trabajo. En algunos despachos se ha tenido éxito al establecer una programación para los trámites fuera de oficina, que puede incluir la definición de alguien que se encargue de realizar todos las gestiones del personal posibles, en una sola salida. También es posible reducir la incidencia de este riesgo a través del uso de Internet para realizar trámites bancarios y similares.

Ejecutar un plan permanente de fortalecimiento de los valores y principios éticos que deben regir el comportamiento del personal en la ejecución de las funciones asignadas.

2.2.2. Fuga de información

Este riesgo ha sido motivo de preocupación debido a que en varias ocasiones se ha hecho realidad y ha ocasionado un gran deterioro de la imagen de la organización. Si bien este riesgo se puede dar por inexperiencia o desconocimiento del personal, el principal motivo son acciones intencionales ejecutadas por personal de de la organización, con el fin de facilitar información confidencial a partes del proceso, ocultar o destruir documentación; favorecer a participantes en una licitación, etc. a cambio de algún tipo de dádiva.

Entre las consecuencias que podría tener la fuga de información tenemos la divulgación de asuntos privados, favorecimiento de una de las partes en un proceso, impunidad, revictimización, procesos disciplinarios, demandas y pérdida de credibilidad.

Estrategias de control

Este riesgo es crítico pues está demostrado que aún el mejor sistema de control interno es incapaz de detener a una persona o grupo de personas que se pongan de acuerdo para realizar un acto ilegal, como lo es facilitar el acceso a información confidencial a personas o entidades no autorizadas. Además de los controles que debe proveer el esquema de seguridad de los datos electrónicos, para los documentos, dependiendo de su grado de confidencialidad o criticidad, será necesario efectuar acciones como inventarios, arqueos, uso de cajas fuertes u otro tipo de custodia especial de documentos que lo requieran, restricción de acceso de personas a las oficinas, instalación de cámaras de vigilancia, etc.

En relación con la fuga de información en formato electrónico, es esencial contar con un esquema de seguridad robusto que se actualice constantemente, debido a que existen muchas vulnerabilidades inherentes a los recursos de tecnología de información y también porque el acelerado ritmo con que se desarrollan estas tecnologías favorece a la denominada “delincuencia cibernética”.

Es necesario que se defina y comunique formalmente al personal sobre el tipo de información que se puede brindar a las personas usuarias según sea su perfil y los canales para realizarlo (por escrito, correo electrónico, vía telefónica, oral, etc.)

Ejecutar un plan permanente de fortalecimiento de los valores y principios éticos que deben regir el comportamiento del personal en la ejecución de las funciones asignadas.

2.2.3. Actos de corrupción

En toda organización donde las personas son parte esencial para el logro de los objetivos, este riesgo estará latente; pues siempre habrá sujetos interesados en obtener algún tipo de ventaja a través del ofrecimiento de dádivas, el tráfico de influencias, etc. Por otro lado, en este aspecto es donde más se muestra vulnerable el sistema de control interno ya que, al ser ejercido por las personas de la organización, es posible que se burlen los controles intencionalmente, en aras de cometer un acto

incorrecto o ilícito. Una persona corrupta tendrá especial cuidado en eliminar cualquier rastro que le puede incriminar, lo cual hace más difícil que se puedan detectar y demostrar este tipo de delitos, con lo cual la impunidad se incrementa.

Este riesgo está directamente relacionado con la integridad de las personas y sus variantes más comunes son:

- **Fraude de funcionarias y funcionarios:** son acciones que el personal interno ejecuta por cuenta propia o de acuerdo con otras personas de la organización o externas (personas usuarias, proveedores, litigantes, etc.) con el propósito de realizar un acto ilegal que le produzca alguna ventaja indebida (patrimonial o de favorecimiento a una persona relacionada), que además puede evitar el logro de los objetivos del servicio de justicia y pérdidas patrimoniales.

- **Abuso en la utilización de recursos:** se da cuando el personal o terceros utiliza los activos de la organización para fines que no están autorizados, con lo cual obtendrán un beneficio (patrimonial o de favorecimiento a una persona relacionada). Esto ocasiona deterioro de la imagen de la organización y pérdidas patrimoniales.

- **Inacción por parte de funcionarias y funcionarios judiciales:** este escenario se presenta cuanto alguna persona de la organización detecta que se está dando una anomalía y no hace el reporte o denuncia a la instancia pertinente. También podría presentarse la omisión intencional de un trámite o control, con el fin de favorecer los intereses personales o de terceros. Por lo general, este tipo de situación ocasiona deterioro del servicio, pérdidas patrimoniales y de la imagen de la organización.

Con respecto al fraude, es necesario tener un completo dominio de cuáles son sus componentes, lo cual facilitará su detección y corrección a tiempo, para lo cual seguidamente se describe el modelo "Triángulo del fraude"[2] ideado por el criminónologo estadounidense Doctor Donald R. Cressey.

Dicho modelo consta de tres componentes, a saber:

Presión: razón o incentivo (necesidad real o percibida) para cometer el fraude, componente que representa la causa o razón; como es el caso de alcanzar ambiciosas metas de desempeño (resolución de casos o preferencia en la atención de cierto perfil de personas o entidades usuarias), obtener beneficios en función de resultados (ascensos o nombramientos en propiedad), mantener el puesto reportando logros ficticios, así como la existencia de deudas personales que pongan en dificultades el poder adquisitivo al personal.

Oportunidad: quienes cometen **el** fraude perciben que existe un entorno favorable para la ocurrencia de actos irregulares; a través del acceso, conocimiento y tiempo para realizar las anomalías. Las debilidades del sistema de control interno o la posibilidad de ponerse de acuerdo con otras personas cercanas o de otros niveles de la organización para cometer fraude (colusión) son ejemplos de oportunidades para incurrir en actos ilícitos.

[2] Donald R. Cressey, *Other People's Money* (Montclair: Patterson Smith, 1973)

Justificación o racionalización. La persona trata de convencerse a si misma (y a los demás, si es descubierta), consciente o inconscientemente, de que existen razones válidas que justifican su comportamiento indebido; o sea, trata de justificar el fraude que cometió. Es un mecanismo psicológico para enfrentar la falta de congruencia entre su propia percepción de honestidad y la naturaleza engañosa de sus acciones. Las excusas más comunes pueden ser: al tener bajo salario, la acción fraudulenta es para obtener una especie de compensación salarial o "préstamo"; tiene falta de reconocimiento en la organización y "racionaliza" pensando que el sistema permite la comisión de anomalías a otros empleados y/o jefaturas (si otras personas cometen acciones dolosas, el fraude propio está justificado).

Los autores David T. Wolfe y Dana R. Hermanson[3], mencionan que este modelo está incompleto pues las motivaciones para cometer el fraude están incompletas ya que no incluyen los factores de dinero, ideología, coerción y ego. Además, señalan que el aspecto de "racionalización" es difícil de identificar, puesto que no se puede saber qué están pensando las personas, por lo cual recomiendan sustituirlo por el término "integridad", ya que la ética relativa a la toma de determinada decisión, sí es susceptible de evaluación.

Con base en lo expuesto, dichos autores proponen un cuarto componente del fraude, a saber:

Capacidad: con la facultad de ciertas personas dentro de la organización (altos ejecutivos, personal clave o de confianza) para cometer y encubrir fraudes; es decir, su posición jerárquica dentro de la empresa les permite realizar la acción dolosa.

El riesgo de fraude es uno de los que mayor daño puede ocasionar a una organización, pues, además de las pérdidas patrimoniales, existen otros efectos negativos, tales como: disminución de la calidad del servicio de justicia, favorecimiento de una parte del proceso, impunidad, toma decisiones incorrectas por parte de la alta administración, desconfianza del personal, pérdida de credibilidad y procesos disciplinarios.

Estrategias de control

Además de fortalecer los procesos de reclutamiento y selección del personal que se contrata, es necesario ejecutar un plan permanente de fortalecimiento de los valores y principios éticos que deben regir el comportamiento del personal en la ejecución de las funciones asignadas, mantener comunicación fluida y constante con proveedores, establecer líneas abiertas para denuncias, garantizar confidencialidad y protección a personas denunciantes, dar seguimiento a personal clave, normas para corregir anomalías detectadas y realización de auditorías preventivas de fraudes.

También existen algunas medidas de tipo preventivo tales como la aplicación de políticas salariales que mantengan el poder adquisitivo del personal, programas de incentivos y campañas para mantener finanzas sanas, que son esenciales pues está demostrado que una persona con problemas económicos es más vulnerable. Las labores de supervisión deben ser consistentes y publicitadas, para dar a las personas un mensaje en el sentido de que se hace por precaución, no por desconfianza.

[3] "El Diamante de Fraude: Teniendo en cuenta los cuatro elementos del fraude"

2.3. Riesgos de Factor humano

2.3.1. Bajo desempeño

En términos generales, se trata de reducido rendimiento de las personas debido a aspectos tales como dificultad para el acceso a todos los recursos necesarios para realizar su labor, falta de competencias (lo cual puede significar debilidades en los procesos de reclutamiento y selección así como la desactualización de conocimientos), clima organizacional adverso, falta de oportunidades de progreso profesional, problemas familiares o de salud e incluso actitudes negativas, negligencia o falta de colaboración del personal, así como carencia de responsabilidad profesional.

Entre las consecuencias de este riesgo tenemos el retraso en la tramitación, el aumento de la carga de trabajo, disminución de la calidad del servicio de justicia, malestar de las personas usuarias, procesos disciplinarios, aumento de costos y desmotivación del personal.

Estrategias de control

Para este caso lo que corresponde es la mejora continua de los procesos de reclutamiento y selección, así como un programa continuo de capacitación que contribuya a la formación idónea del personal. También es necesario que se determine la pertinencia de tener un plan de incentivos y realizar actividades continuas que contribuyan a mejorar el clima organizacional.

Con base en los procesos de planificación, es necesario asegurar razonablemente que las personas dispondrán de todos los recursos y servicios necesarios para realizar sus labores apropiada y oportunamente. De igual forma, la Dirección de TI deberá proveer oportunamente los productos y servicios tecnológicos necesarios.

Ejecutar un plan permanente de fortalecimiento de los valores y principios éticos que deben regir el comportamiento del personal en la ejecución de las funciones asignadas.

2.3.2. Falta de competencia profesional

Es pertinente individualizar este riesgo, que se puede dar por debilidades en los procesos de reclutamiento y selección, pero que también se podría producir por falta de actualización de conocimientos o escasez de oferentes idóneos para ejercer ciertas labores principalmente en lugares alejados del área metropolitana (inopia). También podría ser resultado de la falta de una definición apropiada de las habilidades y formación que deben tener las personas para desempeñar determinados puestos, ya sea desde un principio, o por cambios en el entorno.

Este tipo de riesgo puede ocasionar errores de tramitación y por tanto retraso en la gestión, aumento de la carga de trabajo, revictimización, malestar de las personas usuarias, procesos disciplinarios y disminución de la calidad del servicio de justicia.

Estrategias de control

Para este caso lo que corresponde es la mejora continua de los procesos de reclutamiento y selección del personal que se contrata, pero también es esencial el fortalecimiento de los programas

de capacitación por el constante cambio en las leyes y otras normativas que deben aplicarse en nuestra organización dada su naturaleza. Sin embargo, es necesario atender la actualización en otras áreas del conocimiento tales como administración y tecnología de información, por ejemplo, pues estas son funciones que deben proveer los servicios, suministros y demás materiales para facilitar el trabajo de las demás especialidades que existen en la organización.

También es esencial continuar con los esfuerzos para crear o mantener alianzas estratégicas con las instituciones de educación superior, para promover la mejora continua de la calidad de la formación de las personas que en el futuro podrían ser contratadas por nuestra organización.

2.3.3. Rotación de personal

En una organización que brinda servicios, el factor humano es un recurso esencial. En el caso del Poder Judicial, al año 2012 se estima que laboraban unas 12 mil personas, entre puestos en propiedad e interinos, por tanto existe un alto volumen de movimientos de plazas, por lo cual la rotación de personal es un riesgo muy común cuyos efectos van desde la reducción de personal cuando no se pueda sustituir por ser periodos cortos (ascensos, asistencia a cursos, permisos, incapacidades, etc.), hasta el retraso en la tramitación pues es común que, aún con sustituto, un puesto tiende a disminuir el rendimiento cuando se integra una persona nueva.

También se pueden mencionar consecuencias tales como incertidumbre del personal cuando se trata de cambios de jefatura, aumento de costos por sustitución, vencimiento de plazos, entre otros.

Estrategias de control

Debido al tamaño de nuestra organización, es inevitable que se produzca el riesgo de rotación de personal, por tanto lo que corresponde es buscar medidas de mitigación dirigidas a minimizar sus efectos, como es el caso de redistribución de cargas de trabajo o solicitar personal supernumerario. Sin embargo, en algunos casos se podrían programar las ausencias a través de un plan anual de capacitación o anunciar con antelación la asistencia citas médicas, cuando sea posible, de tal forma que haya tiempo para establecer una respuesta ante el movimiento de personal que se va a generar.

Es pertinente llevar un registro de la rotación del personal del despacho y oficina, con el fin de obtener datos reales sobre su resultado para cierto periodo, información útil para medir el comportamiento de este riesgo y sus consecuencias.

2.3.4. Detrimento de la integridad de las personas

Este riesgo es inherente a la naturaleza de los servicios que brinda el Poder Judicial, pero también puede ocurrir si no existen medidas de control efectivas para proteger la integridad física de quienes laboran para la organización y las personas usuarias, lo cual podría acarrear responsabilidad administrativa, civil y penal. Además, no se pone la apropiada atención a este tipo de eventos, se podría ocasionar una reducción del rendimiento debido a la desmotivación del personal.

Estrategias de control

Es necesario reforzar las políticas de salud ocupacional, con el fin de brindar condiciones razonables de seguridad de las instalaciones, así como para promover una cultura dirigida a la prevención de

accidentes y el deterioro de la salud de las personas debido a condiciones inapropiadas de mobiliario, suministros, luz, ruido, gases tóxicos, etc.

2.4. Riesgos de Servicio a las personas usuarias

2.4.1. Fallas en la atención a personas usuarias

La ocurrencia de este riesgo incide directamente sobre la calidad del servicio a las personas usuarias, por lo cual se considera inaceptable. En muchos casos se da porque es común que se coloque frente al mostrador a una persona nueva en el despacho, por "castigo" o por rotación. Es necesario tomar en cuenta que para atender público se necesita cierta inteligencia emocional que no todas las personas poseen y esa condición dificulta que la atención que se preste sea la apropiada.

Una de las implicaciones mayores de este tipo de evento es que se puede dificultar o impedir el acceso a la justicia a las personas usuarias, como por ejemplo en los casos de violencia doméstica, donde a las personas agredidas se les dificulta tomar la decisión de acudir a los despachos judiciales en busca de protección y una mala atención puede hacer que desistan y por tanto continúen enfrentando situaciones que incluso ponen en peligro su integridad física. Otras posibles consecuencias son: revictimización, aumento de la carga de trabajo, procesos disciplinarios y pérdida de imagen.

Estrategias de control

Entre las acciones a seguir están la capacitación continua del personal que atiende público, poner frente al mostrador a las y los funcionarios que mejor se desempeñan en ese primer contacto con las personas usuarias (cuentan con la inteligencia emocional requerida) y realizar supervisión continua de lo que está pasando en la recepción del despacho.

Ejecutar un plan permanente de fortalecimiento de los valores y principios éticos que deben regir el comportamiento del personal cuando se está atendiendo a las personas usuarias.

2.4.2. Interrupción del servicio en los sistemas de información automatizados

Aunque este aspecto ya se mencionó anteriormente, en lo que se refiere a la atención directa de las personas usuarias es un riesgo a considerar pues frecuentemente solo a través de los datos que administran los sistemas de información automatizados es que se puede resolver una gestión, ya sea personalmente o de manera remota a través del acceso a los servicios de consulta de datos electrónicos y cuando se produce una falla en estos sistemas, se interrumpe su servicio y no se pueden resolver los trámites judiciales con la rapidez y exactitud requeridas. Aspectos como la innovación de sistemas, la dependencia de proveedores y la obsolescencia del hardware y el software, suelen ser críticos a la hora de valorar este tipo de riesgo.

Este tipo de fallas producen retraso en la tramitación, exceso de trabajo, aglomeraciones en los despachos, malestar del personal, pérdida de credibilidad, entre otros efectos negativos.

Estrategias de control

El mantenimiento preventivo, la disponibilidad de equipos de uso alterno y una terminal fuera de red con datos actualizados, son algunas de las acciones que se pueden aplicar para controlar este riesgo. También es esencial contar con procedimientos de respaldo de datos apropiados que contribuyan a que el servicio interrumpido se restablezca lo antes posible.

Por otro lado, es necesario reducir el tiempo de respuesta del soporte técnico para la atención de fallas en los sistemas, para lo cual es necesario llevar un registro histórico de las fallas ocurridas (tipo de falla, lugar donde ocurrió, solución exitosa, personal que intervino) con el fin de apoyar la toma de decisiones ante este tipo de inconvenientes.

Las acciones mencionadas deben estar en concordancia con el plan de continuidad del servicio institucional.

2.5. Riesgos de Recursos e infraestructura

2.5.1. Incumplimiento de la Ley 7600

Los riesgos de este ítem están relacionados con la obligación de facilitar el acceso a las instalaciones y dar una apropiada atención a todo tipo de personas usuarias, sin importar su condición, es decir, sin rechazar a nadie. Sin embargo, es común encontrarse barreras para el apropiado acceso al servicio de justicia, especialmente en locales alquilados que no cuentan con rampas, ascensores, etc.

Debe tomarse en cuenta que el incumplimiento de una ley es especialmente dañino para la imagen del Poder Judicial, además, al sentirse excluida, una persona puede plantear demandas. También se puede ocasionar malestar y frustración del personal de los despachos, especialmente las personas que tengan alguna condición especial.

Estrategias de control

Con base en los procesos de planificación, es necesario asegurar razonablemente que las instalaciones cuentan con las características necesarias para permitir el fácil ingreso de las personas usuarias, sin importar su condición, para lo cual tanto en los contratos de arrendamiento, como en los planos de edificios por construir, se deben considerar todas las especificaciones técnicas a cumplir para brindar dichas facilidades de acceso y en los edificios judiciales existentes, presupuestar la ejecución de las mejoras requeridas para cumplir con esta legislación.

2.5.2. Fallas en las plantas físicas

Este riesgo se da tanto en los edificios propiedad del Poder Judicial, cuanto en locales alquilados que no cumplen con las condiciones apropiadas para que las personas puedan realizar su trabajo, de tal forma que se da hacinamiento, acumulación de expedientes y otra documentación en sitios que no están destinados para archivo (pasillos, pisos, cocinas, etc.), que también pueden ser causas de otros riesgos vinculados con la seguridad o el extravío de expedientes y el bajo rendimiento, ya desarrollados en este documento.

Se han identificado gran cantidad de instalaciones físicas, propias y alquiladas, en las cuales existen serías deficiencias de tendidos eléctricos, así como la sobrecarga debido a un exceso de equipos

conectados a la red eléctrica (equipos para realizar las labores, pero también electrodomésticos de todo tipo) que aumentan la probabilidad del riesgo de incendio

También es común el caso del crecimiento de personal en un despacho que ocasiona el hacinamiento, pues en la misma instalación se debe incorporar el mobiliario y equipo de una nueva plaza, en el mismo espacio y capacidad que ya se tenía.

Estrategias de control

Con base en los procesos de planificación, es necesario asegurar razonablemente que las instalaciones cuentan con las características necesarias para que el personal de los despachos pueda laborar en condiciones apropiadas, sin importar su condición, para lo cual tanto en los contratos de arrendamiento, como en los planos de edificios por construir, se deben considerar todas las especificaciones técnicas a cumplir para brindar dichas facilidades de acceso y en los edificios judiciales existentes, presupuestar la ejecución de las mejoras pertinentes, para lo cual deben tenerse en cuenta los estudios técnicos pertinentes.

Adicionalmente, es necesario aplicar las directrices relativas al archivo de documentos, el programa cero papel y el teletrabajo, como aspectos que pueden contribuir a la mejora del espacio laboral, sin que signifique gastos extra en su implementación.

2.5.3. Fallas de los recursos y servicios de TI

Este riesgo ya fue desarrollado como parte de otras áreas de acción, sin embargo, es necesario individualizar algunos eventos de este tipo que podrían suceder en los despachos judiciales y las estrategias de control más comunes que, en todo caso, deberán estar en concordancia con el plan de continuidad del servicio institucional.

2.5.3.1. Acceso no autorizado a sistemas y bases de datos

Esta situación se puede dar ya sea de manera presencial directamente en los equipos de los despachos, como de manera remota a través de las redes de transmisión de datos. Entre las causas de este tipo de eventos podemos citar: mal uso de claves de acceso, errores en el tratamiento de los reportes de los sistemas, errores en la administración de las cuentas de correo electrónico, presencia de intrusos (hackers).

En la mayoría de los casos, el acceso no autorizado a sistemas y bases de datos pretende apropiarse de información confidencial para darle un mal uso, obtener ventajas ilícitas, destruir o corromper datos, entre otros.

Estrategias de control
La forma apropiada de controlar la ocurrencia de este riesgo es contar con un robusto sistema de seguridad física y lógica de los recursos de tecnología de información requeridos para la gestión en los despachos, aunado al desarrollo de una cultura de protección de dichos recursos por parte del personal.

2.5.3.2. Pérdida de integridad de los datos electrónicos

Esta situación ocurre cuando no se actualizan apropiadamente los datos de los sistemas, se comenten errores de digitación o se da algún acto intencional para borrar datos. Entre los efectos negativos de esta situación podemos citar la dificultad para ubicar los expedientes, decisiones erróneas por mala calidad de los datos producidos por los sistemas, dar información incorrecta a las personas usuarias y "corrupción" de las bases de datos.

Estrategias de control

Cumplir las circulares del Consejo Superior relacionadas con la actualización de los datos de los sistemas de información y aplicar un estricto esquema de seguridad física y lógica en los despachos.

2.5.3.3. Suspensión del servicio de los recursos de TI

Esta situación se puede dar por fallas en los sistemas o equipos, así como por interrupción del servicio de las redes de transmisión de datos o la falta de fluido eléctrico. Entre los efectos más dañinos de este riesgo tenemos la falta de disponibilidad de información para la gestión, lo cual podría retrasar los procesos e incluso suspender audiencias. Además, se produce un aumento de la carga de trabajo, un deterioro del servicio de justicia y una pérdida de credibilidad.

Estrategias de control

Establecer un procedimiento de solicitud de soporte técnico cuando se trate de fallas en los sistemas automatizados del despacho. Si las fallas se dan en las redes o el fluido eléctrico, activar procedimientos manuales alternativos con el fin de continuar dando el servicio, aunque sea disminuido, mientras se resuelve la situación.

Para los sistemas de información críticos para el servicio a las personas usuarias, es apropiado contar con una base de datos fuera de línea, que se debe actualizar periódicamente, con el fin de resolver las consultas urgentes.

Unidad de control interno
Área de gestión de riesgos

Portafolio de riesgos del Poder Judicial 2013
Glosario

- **Acción para gestionar riesgos**. *Disposición razonada establecida por la organización, de previo a la ocurrencia de un evento, para aceptar, transferir, prevenir o mitigar riesgos.*

- **Administración *de riesgos.*** *Cuarta actividad del proceso de valoración del riesgo que consiste en la identificación, evaluación, selección y ejecución de medidas para la administración de riesgos. (En normativas técnicas esta actividad también se denomina "tratamiento de riesgos").*

- ***Actividades de control.*** *Políticas y procedimientos que permiten obtener la seguridad de que se llevan a cabo las disposiciones emitidas por la Contraloría General de la República, por los jerarcas y los titulares subordinados para la consecución de los objetivos, incluyendo específicamente aquellas referentes al establecimiento y operación de las medidas para la administración de riesgos de la institución.*

- ***Análisis de riesgos.*** *Segunda actividad del proceso de valoración del riesgo que consiste en la determinación del nivel de riesgo a partir de la probabilidad y la consecuencia de los eventos identificados.*

- ***Atender riesgos.*** *Opción para administrar riesgos, que consiste en actuar ante las consecuencias de un evento, una vez que éste ocurra.*

- ***Comunicación de riesgos.*** *Actividad permanente del proceso de* ***valoración del riesgo*** *que consiste en la preparación, la distribución y la actualización de información oportuna sobre los riesgos a los sujetos interesados.*

- ***Consecuencia.*** *Conjunto de efectos derivados de la ocurrencia de un evento expresado cualitativa o cuantitativamente, sean pérdidas, perjuicios, desventajas o ganancias.*

- ***Documentación de riesgos.*** *Actividad permanente del proceso de valoración del riesgo que consiste en el registro y la sistematización de información asociada con los riesgos.*

- ***Estrategias de control.*** *Son acciones concretas que se requiere llevar a la práctica para evitar que el riesgo se haga realidad o mitigar su impacto, en caso de que ocurra. Dichas acciones pueden promover la mejora de los controles existentes o la implantación de nuevos controles.*
- ***Evaluación de riesgos.*** *Tercera actividad del proceso de valoración del riesgo que consiste en la determinación de las prioridades para la administración de riesgos.*
- ***Evento.*** *Incidente o situación que podría ocurrir en un lugar específico en un intervalo de tiempo particular.*
- ***Factor de riesgo.*** *Manifestación, característica o variable mensurable u observable que indica la presencia de un riesgo, lo provoca o modifica su nivel.*
- **Fuentes de riesgos:** *son las posibles causas de que el riesgo valorado se haga realidad. Las fuentes del riesgo son la información esencial para determinar su probabilidad de ocurrencia*.
- **Identificación *de riesgos.*** *Primera actividad del proceso de valoración del riesgo que consiste en la determinación y la descripción de los eventos de índole interno y externo que pueden afectar de manera significativa el cumplimiento de los objetivos fijados.*
- **Institución.** *Entidad u órgano integrante de la Administración Pública.*
- **Magnitud**. *Medida, cuantitativa o cualitativa, de la consecuencia de un riesgo.*
- ***Nivel de*** **riesgo**. *Grado de exposición al riesgo que se determina a partir del análisis de la probabilidad de ocurrencia del evento y de la magnitud de su consecuencia potencial sobre el cumplimiento de los objetivos fijados, permite establecer la importancia relativa del riesgo.*
- ***Nivel de riesgo aceptable.*** *Nivel de riesgo que la institución está dispuesta y en capacidad de retener para cumplir con sus objetivos, sin incurrir en costos ni efectos adversos excesivos en relación con sus beneficios esperados o ser incompatible con las expectativas de los sujetos interesados.*
- **Portafolio de riesgos.** *Es un marco de referencia para que las personas gestoras de los riesgos puedan identificar con mayor precisión las amenazas sobre las oficinas en particular y la organización en general. Este documento requiere de una revisión periódica con el fin de actualizar su definición, alcance y consecuencias*.

- ***Probabilidad.*** *Medida o descripción de la posibilidad de ocurrencia de un evento.*

- ***Revisión de riesgos.*** *Quinta actividad del proceso de valoración del riesgo que consiste en el seguimiento de los riesgos y de la eficacia y eficiencia de las medidas para la administración de riesgos ejecutadas.*
- ***Riesgo.*** *Probabilidad de que ocurran eventos que tendrían consecuencias sobre el cumplimiento de los objetivos fijados.*

- **Sistema de *control* interno:** Acciones diseñadas y ejecutadas por la administración activa de una organización que proporcionan seguridad razonable para el logro de sus objetivos.

- ***Sistema Específico de Valoración del Riesgo Institucional (SEVRI)****. Conjunto organizado de elementos que interaccionan para la identificación, análisis, evaluación, administración, revisión, documentación y comunicación de los riesgos institucionales.*

- ***Sujetos interesados****. Personas físicas o jurídicas, internas y externas a la institución, que pueden afectar o ser afectadas directamente por las decisiones y acciones institucionales.*

- ***Valoración del riesgo****. Identificación, análisis, evaluación, administración y revisión de los riesgos institucionales, tanto de fuentes internas como externas, relevantes para la consecución de los objetivos. (En normativas técnicas este proceso también se denomina "gestión de riesgos").*

Nota: los términos que aparecen en cursiva fueron tomados del documento: **DIRECTRICES GENERALES PARA EL ESTABLECIMIENTO Y FUNCIONAMIENTO DEL SISTEMA ESPECÍFICO DE VALORACIÓN DEL RIESGO INSTITUCIONAL (SEVRI) D-3-2005-CO-DFOE**, emitido por la Contraloría General de la República.