AIEVALUACION SOBRE LA ADMINISTRACIÓN Y CONTROL DEL DESARROLLO DE SOFTWARE INTERNO

1. INTRODUCCIÓN

1.1 Origen.

El informe se desarrolla conforme al Plan Estratégico de esta Auditoría Interna.

1.2. Aspectos objeto de estudio.

Comprobar el cumplimiento de la normativa relativa a control interno y administración de riesgos en el proceso denominado “Desarrollo del software interno”.

1.3 Alcance.

Los periodos comprendidos entre del 1° de enero de 2017 al 1° de enero de 2019.

1.4 Exposición a la administración.

Según consta en el acta No. AI-007-2019 del veintitrés de agosto del dos mil diecinueve, se presentan los resultados del estudio en mención al Director General Adjunto y jefatura de la Unidad de Informática, ambos de este Instituto.

1.5 Marco de referencia

- Ley No. 8292 General de Control Interno.
- Ley No. 8204 sobre Estupefacientes, sustancias psicotrópicas, drogas de uso no autorizado, financiamiento al terrorismo, legitimación de capitales y actividades conexas y sus reformas.
- Manual de Normas de Control Interno para las entidades sujetas a las disposiciones de la Contraloría General de la República.
- Manual de Normas para el ejercicio de la Auditoría Interna promulgado por la Contraloría General de la República.
- Manual Técnico de Normas para las Tecnologías de Información de la Contraloría General de la República.
- Directriz D-3-2005-CO-DFOE, La Gaceta No. 135 12 de julio de 2005.
- CMMI (Capability Maturity Model Integration)
- COBIT 5.

1.6 Limitación al alcance.

La Auditoría Interna de este instituto carece de un "auditor de sistemas", que fortalezca el ámbito de acción de la infraestructura tecnológica del ICD, no obstante, se emiten aspectos que contribuyan a mejorar el sistema de control interno y la valoración de riesgo del proceso objeto de estudio.

1.7 Generalidades.

En el presente apartado esta Auditoría detalla aspectos plasmados en el Plan Estratégico de la Unidad de Tecnologías de Información y que ayudaran a comprender las dimensiones y el marco de acción de dicha unidad.

Mediante el Catálogo de Productos y Servicios de Tecnologías de Información (TI), el Instituto Costarricense sobre Drogas da a conocer las sistematizaciones y gestiones tecnológicas que responde a las necesidades de un cliente interno o externo, potenciando el valor de estos y reduciendo el riesgo inherente a los sistemas.

De acuerdo con la Ley No. 8204[1], la Unidad de Informática es la responsable de promover la articulación y el óptimo funcionamiento de los sistemas y subsistemas que conforman el procedimiento de información institucional y sus procesos permanentes de captura, validación, selección, manipulación, procesamiento y comunicación, a partir de las demandas y necesidades de los usuarios

Entre una gama de funciones, se encuentra desarrollar y modernizar la plataforma tecnológica institucional, con el fin de satisfacer los requerimientos institucionales en materia de TI, así como, los de los usuarios institucionales, para optimizar y racionalizar los recursos disponibles es el objetivo general del ICD.

En relación con los productos y servicios brindados por TI a la institución corresponden a sistemas de información los cuales han sido categorizados de acuerdo con los procesos a los cuales brinda soporte:

- ✓ Sistemas para la Divulgación de información institucional.
- ✓ Sistemas de apoyo al proceso administrativo.
- ✓ Sistemas de apoyo y cumplimiento de la Ley 8204.

[1] Ley sobre estupefacientes, sustancias psicotrópicas, drogas de uso no autorizado, actividades conexas, legitimación de capitales y financiamiento al terrorismo

La metodología utilizada por TI se basa en un ciclo de vida el cual contiene las siguientes etapas:

1. Inicio: en la cual se incluye definición del proyecto, estudio de viabilidad y aprobación del proyecto.
2. Planificación.
3. Implementación: la cual contempla la especificación del sistema, prototipos, refinamiento y aprobación del prototipo.
4. Producción: incluye la elaboración del plan de pruebas, ejecución de las pruebas, preparación del manual de usuario, capacitación e instalación.
5. Final: fase compuesta por la aceptación y el resguardo de fuentes del sistema.

Desde la creación del Instituto con la Ley 8204 en el año 2002 la unidad de Tecnologías de Información ha desarrollado sistemas de información acordes a las necesidades institucionales y en apego a dicha normativa.

En el apartado siguiente se desarrollan los resultados del presente estudio y las oportunidades de mejora en administración y control.

2. RESULTADOS.

2.1 Desarrollo y uso de software interno.

Actualmente la plataforma tecnológica se conforma de veinticinco sistemas de software internos donde se almacena información relativa a bienes decomisados y comisados, expedientes judiciales, precursores químicos, operaciones sospechosas del sistema bancario, consumos y decomisos de drogas, gestión del recurso humano, procesos, mantenimiento y control de vehículos.

Los usuarios internos son: Unidad Recuperación de Activos, Unidad Inteligencia Financiera, Unidad Programas de Inteligencia, Unidad Administrativa Financiera, Precursores, Registro y Consulta; y en relación con los externos se tienen datos sobre embarcaciones, mapas de calor con información policial, perfil de sujetos y son: Ministerio de Seguridad Pública para uso de los diversos cuerpos policiales tales como Policía de Control de Drogas (PCD), Guardacostas y la Dirección de Inteligencia y Seguridad (DIS).

En el siguiente detalle se contabilizan los sistemas utilizados por las unidades:

Cantidad	Software/Unidad
5	Sitio Web-ICD Portal-SIDIEN-SIDOC-Foros (Todas las unidades)
1	UIE Portal (Unidad de Información y Estadística)
1	SIGMA (Unidad de Planificación)
1	SIREH (Recursos Humanos)
1	ICD Consejo (Dirección General)
1	PGAI (Comisión Ambiental)
1	SIGEVE (Servicios Generales)
2	Almacenamiento-ICD Repositorio (TI)
4	UIF Directo-UIF Reportes-ROS en línea-RRAG Gafilat (UIF)
3	SIREEM-AGEPOL-SICORE(UPI)
1	URC (Registro y Consultas)
2	URA-Venta Bienes-SAB (Unidad Recuperación de Activos)
1	SUAFI (Unidad Administrativa Financiera)
1	Precursores en línea (Unidad de Precursores)

En relación con el tema, se entrevistó a la jefatura de TI y los desarrolladores de software que ostentan el puesto de profesional de Informática 3[2], en la cual señalan que la metodología utilizada en dicho proceso se denomina “metodología ágil”, basada en scrum que es un sistema que permite la labor de manera ágil y regular, un conjunto de buenas prácticas para el trabajo en equipo, y los tiempos de respuesta por parte de TI para que los requerimientos de los usuarios se resuelvan en menor tiempo posible.

Del trabajo de campo realizado por esta auditoría, se determinan herramientas que no están siendo utilizadas, y que se describen de seguido:

1. SIDIEN (Sistema Dinámico de Encuestas Internas), cuyo desarrollo en el año 2014, la causa principal de la no utilización es la poca socialización en forma adecuada en la institución.
2. ICD CONSEJO, Sistema para el intercambio seguro de información entre la Dirección General y los miembros del Consejo Directivo, concluyo su desarrollo en el 2015, sin embargo, actualmente el software no está siendo utilizado.

3. El módulo FOROS puesto en producción en el año 2014 con el propósito de crear chat’s entre los usuarios para el intercambio de mensajes en tiempo real de una forma segura a través de la red institucional y aplicarlo en Teletrabajo, es un módulo pequeño el cual no ha sido socializado de forma adecuada por la unidad de TI.

[2] Actas Nos. AI-028-2019, AI-034-2019 y AI-035-2019 del 12 de junio y 10 de julio respectivamente.

4. Sistema URA Venta de Bienes, creado desde el año 2011, sin embargo, como los mencionados en párrafos anteriores no está siendo utilizado.

En entrevista con el titular de la unidad de TI indica que los sistemas FOROS y SIDIEN han sido impulsados y desarrollados de forma óptima, pero el uso de dichos sistemas se suspendió ante la ausencia de promoción e inducción por parte de dicha área, además no se le brindo la importancia requerida por parte de la administración, pero tampoco existe una razón justificada para que no utilice los sistemas en mención.

El desarrollo de software conlleva un trabajo que de no contar con una adecuada planificación deriva efectos negativos tales como subutilización de recurso humano y monetario, conocimiento nulo de los sistemas con los que cuenta la institución, esfuerzos mal enfocados sobre interés particulares de las unidades o los usuarios y sistemas obsoletos o poco prácticos para los procesos que se deben ejecutar por parte de los usuarios.

Al respecto, las normas del Manual de Normas Generales de Control Interno para el Sector Público mencionan:

> *"*5.7 Calidad de la Comunicación *El jerarca y los titulares subordinados, según sus competencias, deben establecer los procesos necesarios para asegurar razonablemente que la comunicación de la información se da a las instancias pertinentes y en el tiempo propicio, de acuerdo con 24 las necesidades de los usuarios, según los asuntos que se encuentran y son necesarios en su esfera de acción. Dichos procesos deben estar basados en un enfoque de efectividad y mejoramiento continuo.".*
>
> *"*5.9 Tecnologías de información *El jerarca y los titulares subordinados, según sus competencias, deben propiciar el aprovechamiento de tecnologías de información que apoyen la gestión institucional mediante el manejo apropiado de la información y la implementación de soluciones ágiles y de amplio alcance.".*

Por tanto, conviene la implementación de controles con el propósito de garantizar que los sistemas de información desarrollados por TI estén siendo aprovechados y utilizados al cien por ciento por los usuarios internos y externos, y que se fundamenten las razones por las cuales los sistemas SIDIEN, ICD Consejo, URA Venta de Bienes y FOROS no están siendo utilizados en la actualidad.

2.2 Políticas de desarrollo de software.

Para iniciar con el tema, es importante recordar que todo proyecto a desarrollarse relacionado con software, debe contemplar un estudio de viabilidad o anteproyecto que especifique necesidades, controles, costos, contingencia, impacto, riesgos asociados y beneficios que se desean adquirir.

Al respecto, no se conoció del análisis de los sistemas desarrollados al momento de solicitarse los requerimientos para el diseño, por cuanto no fue posible evidenciar en los expedientes mencionados datos que indiquen que las unidades solicitantes hayan presentado documentación previa justificando de manera técnica y operativa el desarrollo del software existente, como por ejemplo el llenado del formulario No. 2 denominado "Estudio de factibilidad" que según el documento Metodología para el desarrollo de sistemas de información debería estar incluido en el expediente de cada desarrollo.

Lo anterior, se respalda con lo dicho por el jefe de la unidad objeto de estudio, el cual afirma según el acta No. AI-028-2019[3] lo siguiente:

> *"No en una manera formal. No se levanta un criterio sobre la factibilidad. Pero en la práctica si se hace.".*

Por su parte el funcionario de TI que ocupa el puesto no. 501178 profesional de Informática 3, señala:

> *"Lo ideal es que el usuario presente un anteproyecto donde haya evaluado su entorno, flujo de proceso y reglas correspondientes."*[4].

Coincide con la afirmación del profesional de informática 3, con puesto No. 503892, mediante el acta No. AI-032-2019 del 10 de junio, resume:

> *"Lo que me gustaría es que en cada una no sea solo una persona la que indique los requerimientos, sino que sea un trabajo en equipo, un anteproyecto, sería lo ideal, los dueños de los procesos son los que conocen sus necesidades.".*

En relación con lo evidenciado y las afirmaciones expuestas, se determina que la causa principal radica en que la Unidad de Tecnologías de Información no

[3] Del 12 de junio 2019.
[4] Acta No. 031-2019 del 10 de julio.

mantiene una política de desarrollo dirigida a los usuarios sobre estudios y requisitos previos al inicio de los sistemas, los cuales son requeridos con el propósito de asegurar el cumplimiento de los objetivos y solventar las necesidades existentes.

La gestión de solicitudes de software no es la más adecuada, se requiere mayor criterio y procedimientos estándares para definir, evaluar y aceptar los requerimientos, así como documentos avalados con firmas de los responsables o los involucrados en cada proyecto que respalden la calidad y viabilidad de la información en relación con solicitudes de cambios, inconsistencias y acciones correctivas y obtener un histórico y asegurar la trazabilidad de los requerimientos.

Por tanto, no implica saber cuál será el mejor modelo para desarrollar un software, lo cierto es que la responsabilidad de TI es solicitar las estrategias, exigencias y necesidades de los usuarios internos; siendo prudente antes del desarrollo de un software, determinar la existencia de los estudios pertinentes para su elaboración, datos que solo los usuarios poseen, puesto que se interrelacionan diariamente con la operatividad del proceso.

La norma técnica para la gestión de la TI 3.1 Consideraciones generales de la implementación de TI señala:

> *"La organización debe implementar y mantener las TI requeridas en concordancia con su marco estratégico, planificación, modelo de arquitectura de información e infraestructura tecnológica, por lo que debe: adoptar políticas/establecer el respaldo claro y explicito para los proyectos/ garantizar la participación activa de las unidades/ instaurar líderes, analizar alternativas de solución/ contar con requerimientos claros y oportunos/ tomar previsiones/ formular y ejecutar estrategias entre otras.".*

Consecuentemente la norma 3.2 Implementación de software indica:

> *"La organización debe implementar el software que satisfaga los requerimientos de sus usuarios y soporte efectivamente sus procesos. En concreto el inciso e) definir los criterios para determinar la procedencia de cambios y accesos de emergencia al software y datos y los procedimientos de autorización, registro, supervisión y evaluación técnica, operativa y administrativa de los resultados de esos cambios y accesos.".*

Es oportuno que la Unidad de Tecnologías de Información implemente una política de desarrollo de software, señalando los criterios técnicos y operativos que

deberán cumplir los proyectos que deriven de las necesidades de todas las unidades del ICD, en procura de optimizar los recursos disponibles y la funcionalidad de los sistemas.

2.3 Soporte documental en desarrollo de software.

La ausencia de documentación consignada por los actores del proceso limitó comprobar la data de los documentos y su validez como se requería por parte de esta Auditoría, pues se determina que de los proyectos evaluados faltó documentación sobre el desarrollo, tales como formularios sobre requerimientos, ajustes y modificaciones del sistema y en lo que respecta a la unidad solicitante no se evidenciaron actas, acuerdos de compromiso, resoluciones en el expediente digital suministrado por TI, únicamente prevalecen correos electrónicos con solicitudes de cambios, manuales de usuario, y descripciones del software.

Por otro lado, el proceso es realizado de manera informal, sin formularios que aprueben los ajustes al sistema, posiblemente por la metodología ágil utilizada, que se basa en generar poca documentación y se analiza la solicitud para dar respuesta inmediata al requerimiento, no obstante, es importante recabar que los procesos independientemente de la metodología aplicada deben sustentarse en documentación que sirva para evaluar el desempeño, los tiempos y la calidad de los productos finales.

Considera esta unidad de Auditoría Interna, que la gestión de los datos no es debidamente documentada mediante un plan de gestión que incorpore requisitos de seguridad y privacidad. Se omite el seguimiento de las respuestas a las peticiones de los usuarios durante el desarrollo de software, por medio de bitácoras firmadas por las partes y los históricos correspondiente de los ajustes realizados por el desarrollador, únicamente correos electrónicos donde los usuarios solicitan los cambios al sistema que consideren necesarios.

Así las cosas, debe existir un registro de todos los problemas identificados y de las soluciones y acciones correctivas asociadas a cada petición de cambio, con el fin de determinar si el problema presentado radica en la gestión del desarrollador o bien en la de los usuarios; a la vez que la documentación soporta las acciones ejecutadas en ambas vías.

En relación con lo anterior, se produce el debilitamiento de la gestión documental y se limita la comprensión de las fases del desarrollo de los sistemas para los usuarios internos y externos, por ejemplo los desarrolladores, la auditoría interna u otros.

El capítulo IV sobre actividades de control de las Normas Generales de Control Interno señala en la Norma 4.4.1 Documentación y Registro de la gestión institucional:

> *"El jerarca y los titulares subordinados, según sus competencias deben establecer las medidas pertinentes para que los actos de la gestión institucional, sus resultados y otros eventos relevantes, se registren y documenten en el lapso adecuado y conveniente y se garanticen razonablemente la confidencialidad y el acceso a la información pública según corresponda.".*

La norma 4.4.2 Formularios uniformes indica: el jerarca y los titulares subordinados deben disponer lo pertinente para la emisión, la administración, el uso y la custodia por los medios atinentes de formularios uniformes para la documentación, el procesamiento y el registro de las transacciones.

La gestión documental idónea es digitalizar todos los documentos que se obtengan en los archivos físicos, pues con el avance de la tecnología, al no tener los documentos en formato digital puede suponer una gran pérdida de tiempo, esta unidad de Auditoría ha mantenido el criterio de la política "cero papeles", que consiste en pasar documentación física en formato digital, sin embargo, es necesario que los documentos se encuentren ordenados por un índice y que se pueda acceder fácilmente a ellos para futuras consultas.

EL ICD no cuenta con una política bien definida de gestión de documentos electrónicos con criterios y recomendaciones necesarios para garantizar la interoperabilidad, recuperación y conservación de documentos y expedientes digitales, así como ventajas que conllevan a la seguridad de la información, concientización de medio ambiente con la no impresión de documentos, compartir la información en forma ágil y segura a lo interno y externo de la institución, ahorro en costos de mantenimiento, deterioro en los papeles, aspectos importantes que se deben considerar para cambiar la cultura de generación de documentos.

Debe TI analizar la gestión documental de sus procesos de manera que se apoye en la colaboración de la encargada de archivo institucional y velar por mantener sus actividades y procesos debidamente documentados con el propósito de respaldar las acciones que se ejecutan en el desarrollo de software interno.

2.4 En el tema “gestión del riesgo.”.

En este apartado se revisaron y analizaron los expedientes de desarrollo de software, determinándose que la gestión de riesgos de los proyectos liderados por TI no son documentados ni monitoriados durante el ciclo de vida de este, es decir que no hubo asociación de riesgos a las tareas específicas de cada proyecto; únicamente se establecen riesgos generales para cada uno de los objetivos del proceso objeto de estudio plasmado en la POSI 2019 incorporada al módulo denominado Sistema de Gestión y Monitoreo de Actividades (SIGMA) herramienta que será evaluada por esta unidad a futuro.

En el SIGMA el proceso Desarrollo de Software Interno se presenta de la siguiente forma:

Código	Nombre	Estado	Opción
ICD-UI-001-POSI 2019	Desarrollo de Software	Activo	Detalles

En la opción detalles se incorporaron doce objetivos asociados al proceso Desarrollo de software que a su vez es parte de la Programación Operativa Sustantiva Institucional (POSI) 2019, sin embargo se determinó que los objetivos son generales y no contemplan los riesgos asociados de forma directa al proceso de desarrollo. Para mayor comprensión se toma el objetivo relativo a “Mantener actualizados los productos de software de desarrollo in house, para que respondan a las necesidades de las unidades que los utilizan”. El riesgo del citado objetivo tiene la codificación ICD/UI-GIR-1-OBJ-1-RIS-1-POSI 2019 y textualmente describe: “Atención a prioridades y situaciones emergentes que impliquen postergar las actualizaciones de los productos”, no obstante, no fue posible determinar mediante la herramienta SIGMA la probabilidad de ocurrencia, el impacto si se materializa, ni las acciones para mitigarlo.

De lo anterior, se determinan dos omisiones en la gestión del riesgo, la primera una inadecuada gestión del riesgo por parte de los responsables, por cuanto el análisis de riesgo para los objetivos plasmados no cumple todas las etapas que lo componen a saber: 1. Identificación del riesgo, 2. Análisis de consecuencias, 3. Cuantificación del riesgo y 4. Toma de decisiones, por lo tanto, no se conoció el nivel de riesgo para dichos objetivos.

En segundo término, se omite el análisis de riesgo para el “ciclo de vida” de los software desarrollados e implementados, no hubo evidencia en los diez expedientes revisados como muestra por esta unidad de Auditoría que demostrara lo contrario, lo que concluye que se desconoce el nivel de riesgo para dicho proceso.

Lo expuesto en párrafos preliminares, se comprueba al efectuarle consulta al jefe de TI[5], sobre la forma de minimizar riesgos para cumplir los objetivos de los proyectos o que no satisfagan sus requerimientos o no cumplan con los términos de tiempo y costo preestablecidos, señalando:

> *"El costo no se considera, los costos inherentes en el proceso de desarrollo son los salarios de los desarrolladores, sin embargo, si se tienen identificados los riesgos por los plazos que no se cumplan. No se ha requerido de una matriz de criterios para determinar la viabilidad de los proyectos.".*

Desde el punto de vista técnico, se describe a continuación a manera de ejemplificar, los criterios que deben contemplarse para medir y gestionar los riesgos:

- **Probabilidad:** posibilidad de ocurrencia de un evento. 1=Baja, 2=Media y 3= Alta.
- **Impacto:** magnitud de consecuencias potenciales que por distintas situaciones puede suceder si el riesgo se materializa. 1= Insignificante, 2= Menor, 3= Requiere atención, 4= Mayor, 5= Critico.
- **Nivel de riesgo:** es la probabilidad x impacto, la cual se ejemplifica en el siguiente recuadro:

PUNTUACIÓN DE RIESGO

IMPACTO					
	5	CRITICO	5	10	15
	4	MAYOR	4	8	12
	3	REQUIERE ATENCIÓN	3	6	9
	2	MENOR	2	4	6
	1	INSIGNIFICANTE	1	2	3
			1- BAJA	2- MEDIA	3- ALTA

PROBABILIDAD

NIVEL RIESGO		RANGO
BAJO		1 a 3
MEDIO		4 a 8
ALTO		9 a 15

Se manifiesta con base en lo anterior que la causa principal de lo expuesto es producto de que no se cuenta con estrategias para determinar los riesgos de los

[5] Acta No. AI-028-2019 del 12 junio, 2019.

procesos en las actividades y tareas, únicamente se definen riesgos para los objetivos establecidos de cada proceso, lo que incrementa el riesgo de proyectos inconclusos que requieren de reiteradas modificaciones en el caso del software, incumplimientos legales, sistemas inestables, omisiones de integridad de los datos, ineficacia de los servicios, desaprovechamiento de los recursos humanos y tecnológicos, inestabilidad de las operaciones, fraudes y corrupción que comprometen en forma general los objetivos institucionales.

Un adecuado proceso de implementación de gestión del riesgo consiste en: diagnostico que se refiere al entorno de control, evaluación de los riesgos, actividades de control, comunicación y supervisión. Generar cultura del riesgo que corresponde principalmente al compromiso de directivos, crear manual de gestión de riesgos, capacitación del personal, funciones de control. Valoración del riesgo en relación con la identificación, el análisis y la determinación del valor del riesgo. Estrategia de gestión que comprende el manejo y el nivel de riesgo y una vez cumplido el proceso de implementación, monitoreo que incluye la supervisión de todos los procesos, revisión del seguimiento y el mejoramiento continuo.

La Contraloría General de la Republica mediante la Resolución R-CO-64-2005 del primero de junio de 2005 emitió las Directrices Generales para el establecimiento y funcionamiento del Sistema Específico de Valoración del Riesgo Institucional (SEVRI)[6]. De igual manera la Ley General de Control Interno No. 8292 establece en el artículo No. 14:

> **"Valoración del riesgo**. En relación con la valoración del riesgo, serán deberes del jerarca y los titulares subordinados, entre otros, los siguientes:
> *a) Identificar y analizar los riesgos relevantes asociados al logro de los objetivos y las metas institucionales, definidos tanto en los planes anuales operativos como en los planes de mediano y de largo plazos".*
> *"Todo ente u órgano deberá contar con un sistema específico de valoración del riesgo institucional por áreas, sectores, actividades o tarea que, de conformidad con sus particularidades, permita identificar el nivel de riesgo institucional y adoptar los métodos de uso continuo y sistemático, a fin de analizar y administrar el nivel de dicho riesgo"[7].*

Por su parte, la norma 3.3 Vinculación con la Planificación institucional del Manual de normas generales de control interno establece:

[6] D-3-2005-CO-DFOE
[7] Ley General de Control Interno Art. 18 Sistema Específico de Valoración de Riesgo Institucional

> *"los resultados de la valoración del riesgo deben ser insumos para retroalimentar ese proceso de planificación, aportando elementos para que el jerarca y los titulares subordinados estén en* ***capacidad de revisar, evaluar y ajustar periódicamente los enunciados y supuestos que sustentan los procesos de planificación estratégica y operativa institucional****, para determinar su validez ante la dinámica del entorno y de los riesgos internos y externos".*

Es oportuno señalar además que la norma 4.7 documentación del riesgo del manual de normas de control interno establece que se deberá documentar la información sobre las medidas, administración y valoración en cada riesgo generado (identificación, análisis, evaluación, administración y revisión). Deberán establecerse registros de los mismos que incluyan como mínimo, la información sobre su probabilidad, consecuencia, nivel de riesgo asociado y medidas seleccionadas para su administración.

Debe la Unidad de Tecnologías de información replantear el análisis de riesgo consignado en el SIGMA, ajustarlo no solo a los objetivos planteados para dicho proceso, sino también incluir las etapas de ciclo de vida de los proyectos de desarrollo, con el fin de cubrir todos los niveles operativos y las actividades que se ejecutan en dicho procedimiento.

2.5 Actualización y aprobación de manuales.

En relación con este tema, a solicitud de esta Auditoría, la Contraloría General de la República indica en oficio No 1015 (FOE-PGA-37) del 06 de febrero del 2007, y entre lo que interesa señala[8]:

> *"En criterio de este órgano contralor, la competencia para la aprobación de este tipo de manual le corresponde al Consejo Directivo, toda vez que si bien no se trata de disposiciones con rango reglamentario, esos instrumentos mantienen importantes similitudes con este tipo de normativa, y al no existir una norma especial que atribuya expresamente su aprobación otra instancia, debería ser ese órgano colegiado dotado de la potestad reglamentaria interna el que los ponga en vigor; asimismo, debe tomarse en consideración que definir la estructura administrativa del Instituto, aspecto indisolublemente ligado a la emisión de ese tipo de instrumento es también potestad del Consejo Directivo".*

Posterior, la Dirección General de ese entonces, emite la circular DG- 010-2013[9] sobre "Manuales de Procesos y Procedimientos", informando sobre la delegación

[8] Pronunciamiento conocido por los jerarcas, Asesoría Legal y Dirección General del ICD
[9] 1° noviembre de 2013.

que realizó el órgano colegiado a la Dirección General, para la aprobación de los Manuales de Procedimiento institucionales; función que no le compete a la Dirección.

En relación con la actualización y aprobación de los manuales de procesos institucionales esta Auditoría ha sido clara en su criterio, respecto a que el Consejo Directivo del ICD es el único órgano quien puede aprobar la actualización y emisión de los manuales correspondientes en la institución. Sin embargo, se debe aclarar que los manuales deben ser responsabilidad de la Dirección General, Planificación y las diversas unidades la creación, actualización y ajustes que correspondan.

Queda demostrado una vez más, que todo lo relacionado a los manuales para el proceso de Desarrollo de software interno no se actualiza desde el año 2012, información suministrada por el jefe de la unidad evaluada mediante el Acta No. AI-028-2019 del 12 de junio.

Además, se comprueba que, en el 2006 se solicitó que el Manual de procesos y procedimientos de la Unidad de Tecnologías de información fuese sometido a conocimiento y aprobación del Consejo Directivo de este Instituto; no obstante, por directriz de dicho órgano, según acuerdo Ciento Veinticuatro Cero Siete- Dos Mil Trece de Sesión Ordinaria Número Siete del 31 de octubre del 2013, delega la aprobación en la Dirección General del ICD. Dicho documento fue aprobado el 20 de diciembre del 2013 por la Jefatura de la Unidad de Planificación y la Directora General Adjunta de ese entonces. Posteriormente, el 07 de enero del 2014 bajo el oficio M-DG-006- 2014 el jerarca informa que el Manual fue aprobado y por tanto fuese publicado en la red institucional: “carpeta publica/Manual de procesos y procedimientos”.

Por tanto, se concluye que existen elementos que se pueden ver comprometidos si la administración deja de lado la actualización de los manuales de procesos; entre ellos tareas, obligaciones y responsabilidades de los funcionarios, a la vez se crea un desfase entre la teoría y la práctica, recordando que los cambios en la práctica deben ser replicados en la teoría con el fin de dichos manuales estén lo más actualizados posible.

La función específica de estos manuales es instruir a los funcionarios sobre los distintos aspectos institucionales, procurando minimizar el desconocimiento de las obligaciones de cada uno, la duplicación o superposición de funciones con el objetivo de mejorar la eficiencia y productividad de cada una de sus áreas. La realización, aplicación y actualización de un manual de procesos, procedimientos y funciones es la versión detallada de la descripción de los objetivos, funciones, autoridad, responsabilidad de los distintos puestos de trabajo que componen la estructura de la institución.

Es deber de la administración activa por medio de TI, Planificación institucional y la Dirección General responder a las buenas prácticas de gestión, actualizar los manuales de procesos que correspondan y poner en conocimiento del Consejo Directivo los ajustes que se realicen al respecto, con el propósito de asegurar la aprobación de los jerarcas, en concordancia con los criterios establecidos por la Contraloría General de la República.

3 CONCLUSIONES.

Se determinó herramientas que no están siendo utilizadas, y se describen de seguido: 1. SIDIEN (Sistema Dinámico de Encuestas Internas), cuyo desarrollo en el año 2014, 2. ICD Consejo desarrollada para el intercambio seguro de información entre la Dirección General y los miembros del Consejo Directivo, desarrollado en el 2015. 3. El módulo FOROS puesto en producción en el año 2014 con el propósito de crear chat's entre los usuarios para el intercambio de mensajes en tiempo real de una forma segura a través de la red institucional y aplicarlo en Teletrabajo. 4. Sistema URA Venta de Bienes, creado desde el año 2011.

No se conoció del análisis por parte de los usuarios de los sistemas desarrollados en el momento de solicitarse los requerimientos de un sistema a diseñar, por cuanto no fue posible evidenciar en los expedientes mencionados datos que indiquen que las unidades solicitantes hayan presentado documentación previa que justifique de manera técnica y operativa el desarrollo del software existente. La Unidad de Tecnologías de Información no mantiene una política de desarrollo dirigida a los usuarios sobre estudios y requisitos previos al inicio de los sistemas.

Se comprobó que la unidad evaluada ha omitido cumplir a cabalidad con gestión documental formal. Por otro lado, el proceso es realizado de manera informal, sin formularios que aprueben los ajustes al sistema. La gestión de los datos no es debidamente documentada mediante un plan que incorpore requisitos de seguridad y privacidad.

Por otro lado, se evidenció que la gestión de riesgos de los proyectos liderados por TI no son documentados ni monitorizados durante el ciclo de vida de este, es decir que no hubo asociación de riesgos a las tareas específicas de cada proyecto.

Se determinan dos omisiones en la gestión del riesgo, la primera una inadecuada gestión del riesgo por parte de los responsables, por cuanto el análisis de riesgo para los objetivos plasmados no cumple todas las etapas que lo componen, además se omite el análisis de riesgo para el "ciclo de vida" de los software desarrollados e implementados.

Por último, todo lo relacionado a los manuales para el proceso de Desarrollo de software interno no se actualiza desde el año 2012.

4 RECOMENDACIONES.

AL JEFE DE TECNOLOGIAS DE INFORMACION.

1. Implementar controles con el propósito de garantizar que los sistemas de información desarrollados por TI estén siendo aprovechados y utilizados al cien por ciento por los usuarios internos y externos, y que se fundamenten las razones por las cuales los sistemas SIDIEN, ICD Consejo, URA Venta de Bienes y FOROS no están siendo utilizados en la actualidad. **(Ver punto 2.1 de este informe)**

2. Es oportuno que la Unidad de Tecnologías de Información establezca una política de desarrollo de software, señalando los criterios técnicos y operativos que deberán cumplir los proyectos que deriven de las necesidades de todas las unidades del ICD, en procura de optimizar los recursos disponibles y la funcionalidad de los sistemas. **(Diríjase al punto 2.2 de este informe)**

3. Deberá TI analizar la gestión documental de sus procesos, especialmente la que se desarrolla en este informe, solicitar la colaboración pertinente de los encargados de archivo institucional y velar por mantener sus actividades y procesos debidamente documentados con el propósito de respaldar las acciones que se ejecutan en el desarrollo de software interno. **(véase punto 2.3 de este informe)**

4. Replantear el análisis de riesgo consignado en el SIGMA, ajustarlo no solo a los objetivos planteados para dicho proceso, sino también incluir las etapas de ciclo de vida de los proyectos de desarrollo, con el fin de cubrir todos los niveles operativos y las actividades que se ejecutan en dicho proceso. **(Ver punto 2.4 del presente informe)**

5. Coordinar con Planificación institucional y la Dirección General para responder a las buenas prácticas de gestión, actualizar los manuales de procesos que correspondan y poner en conocimiento del Consejo Directivo los ajustes que se realicen al respecto, con el propósito de asegurar la aprobación de los jerarcas, en concordancia con los criterios establecidos por la Contraloría General de la República. **(diríjase al punto 2.5 de este informe)**

DEYANIRA BERMUDEZ CALDERON (FIRMA)

Firmado digitalmente por DEYANIRA BERMUDEZ CALDERON (FIRMA)
Fecha: 2019.09.03 14:43:14 -06'00'