DOCUMENTO FIRMADO CON CERTIFICADO DIGITAL
N ° 3957-00072427324A
MARVIN CALERO ALVAREZ

Informe
No.CR-INCOP-AI-I-2019-011
03 de diciembre de 2019

INSTITUTO COSTARRICENSE DE PUERTOS DEL PACÍFICO AUDITORÍA INTERNA ESTUDIO SOBRE: "Atención del Acuerdo No. 7 de la Sesión No. 4185 del 25 de setiembre de 2019, relacionado con solicitud de informe de seguimiento a recomendaciones de Tecnología de Información que se encuentran incumplidas".

DICIEMBRE- 2019

RESUMEN EJECUTIVO

El presente documento se realizó en cumplimiento a lo que establece la Ley General de Control Interno (8292) así como el Plan Anual de Trabajo de esta Auditoría para el período 2019, con el objeto de verificar el cumplimiento de las recomendaciones realizadas por Auditorías Externas y dirigidas a la Unidad de TI, con base en el Anexo 1 del informe AG-388-12 y pendientes de verificación técnica por parte de esta Auditoría Interna; a su vez, en cumplimiento del Acuerdo No. 7 tomado por la Junta Directiva en Sesión No. 4185, celebrada el 25 de setiembre de 2019.

De acuerdo con nuestros registros se determinó que existían dos (2) recomendaciones pendientes de cumplimiento del informe AG-388-12, las cuales corresponderían a las recomendaciones N°4.1 y N°4.3. La primera de ellas (N°4.1) es relativa al cumplimiento de las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información emitidas por la Contraloría General de la República; la cual quedó pendiente de verificación en el presente informe por las limitaciones de información oportuna por parte de la Unidad de TI; por lo que su estado de cumplimiento se informará en el próximo informe de labores según nuestro Plan Anual de Trabajo 2020 que se emitirá en el mes de febrero del mismo año.

La segunda recomendación (N°4.3), está relacionada con la elaboración de un plan de cumplimiento de recomendación anteriores, que incluye la atención de noventa y seis (96) observaciones vinculantes de cumplimiento, correspondientes a los informes AG-408-09 (24), AG-204-10 (1) y AG-302-11 (71) según consta en el Anexo N°1 del dicho informe AG-388-12, citado en el párrafo anterior.

Para la realización del presente seguimiento se partió de la valoración del contenido de la documentación suministrada por la Unidad de TI, así como el criterio técnico con que hoy cuenta la Auditoría Interna; considerando a su vez los aspectos “Relevancia y/o oportunidad de las recomendaciones brindadas.”

Sobre el particular el análisis llevado a cabo para la valoración del cumplimiento de las recomendaciones y observaciones antes indicadas sumó en total noventa y siete (97), dándose por cerradas noventa y dos (92) de ellas, lo que corresponde a un 95%.

Se concluye que la administración ha realizado un esfuerzo razonable para el cumplimiento de estas. Sin embargo, se debe fortalecer los mecanismos de comunicación y la efectividad de la información brindada por parte de la Unidad de TI, cuando se le solicita evidencia concreta sobre el cumplimiento de las recomendaciones objeto de seguimiento por parte de la Auditoría Interna.

VERIFICACION DE RECOMENDACIONES DE AUDITORÍAS EXTERNAS DE TI

Tabla de Contenido

DOCUMENTO FIRMADO CON CERTIFICADO DIGITAL
N ° 3957-00072427324A
MARVIN CALERO ALVAREZ

VERIFICACIÓN DE RECOMENDACIONES DE AUDITORIAS EXTERNAS DE TI

I. INTRODUCCIÓN

1.1 Origen del estudio

El presente estudio se efectuó en cumplimiento del Plan Anual de Trabajo de la Auditoría Interna para el año 2019 y en atención a lo dispuesto en el artículo No. 22 inciso g) de la Ley General de Control Interno (No. 8292[1]), la Norma 2.11[2] de las Normas para el Ejercicio de la Auditoria Interna en el Sector Público, así como la Norma 206[3] de las Normas Generales de Auditoría para el Sector Público. A su vez en cumplimiento del Acuerdo No. 7 tomado por la Junta Directiva en Sesión No. 4185, celebrada el 25 de setiembre de 2019.

1.2 Objetivo General

Evaluar el estado de las recomendaciones emitidas por Auditorías Externas contratadas por la Auditoría Interna dirigidas a la Unidad de TI, tomando como base el informe AG-388-12 y su Anexo N°1, para determinar su debido cumplimiento.

1.3 Alcance

El estudio comprendió la verificación y valoración de las acciones dispuestas por parte de la Unidad de TI con el fin de cumplir las recomendaciones emitidas por las auditoria externas, con base en el informe de cumplimiento de recomendaciones AG-388-12 elaborado por la empresa Dinámica Consultores; esto incluye las recomendaciones pendientes de cumplimiento N°4.1 y N°4.3 emitidas dentro de ese mismo informe, como aquellas recomendaciones contenidas en el Anexo N°1 del mismo, que contiene

[1] Del 4 de setiembre del 2002.

[2] **2.11 Seguimiento de acciones sobre resultados**: El auditor interno debe establecer, mantener y velar porque se aplique un proceso de seguimiento de las recomendaciones, observaciones y demás resultados derivados de los servicios de la auditoría interna, para asegurarse de que las acciones establecidas por las instancias **competentes se hayan implementado eficazmente y dentro de los plazos definidos** por la administración. Ese proceso también debe contemplar los resultados conocidos por la auditoría interna, de estudios de auditores externos, la Contraloría General de la República y demás instituciones de control y fiscalización que correspondan.

Tratándose de disposiciones de la Contraloría General de la República, debe observarse la normativa específica aplicable

[3] **206. Seguimiento** 01. Cada organización de auditoría del sector público debe establecer e implementar los mecanismos necesarios para verificar oportunamente el cumplimiento efectivo de las disposiciones o recomendaciones emitidas. 02. La Administración es responsable tanto de la acción correctiva como de implementar y dar seguimiento a las disposiciones y recomendaciones de manera oportuna y efectiva, por lo que deberá establecer políticas, procedimientos y sistemas para comprobar las acciones llevadas a cabo para asegurar el correcto y oportuno cumplimiento. Las auditorías internas deberán verificar el cumplimiento de las disposiciones o recomendaciones que otras organizaciones de auditoría hayan dirigido a la entidad u órgano de su competencia institucional.

las noventa y seis (96) observaciones vinculantes correspondientes a los informes AG-408-09 (24), AG-204-10 (1) y AG-302-11 (71).

1.4 Limitaciones

El presente estudio contó con una series de limitaciones, tales como: retrasos en la entrega de información, así como en forma y el contenido requerido por esta Auditoría para la respectiva valoración. Lo anterior quedó consignado mediante oficios N°. CR-INCOP-AI-2019-281 de fecha 14-10-2019, CR-INCOP-AI-2019-311 de fecha 11-11-2019, CR-INCOP-AI-2019-318 de fecha 13-11-2019, CR-INCOP-AI-2019-329 de fecha 19-11-2019, y finalmente CR-INCOP-AI-2019-335 de fecha 25-11-19, todos dirigidos a la Unidad de TI de manera reiterativa, solicitando la misma información y que se terminó de atender hasta que se recibió el oficio CR-INCOP-TI-2019-0197 en fecha 26-11-2019; no obstante, lo anterior limitó el tiempo para continuar el análisis de la recomendación faltante (N°4.1 del informe AG-388-12). Tal situación obligó a esta Auditoría solicitar a esa estimable Junta Directiva ampliar el plazo a una semana adicional, para entregar el presente informe.

II. RESULTADOS

La finalidad del seguimiento implementado por la Auditoría Interna, es determinar si se han cumplido razonablemente las recomendaciones (internas o externas) producto de los informes citados en el alcance del presente documento, los cuales han arrojado información sobre áreas de oportunidad susceptibles de mejora, con el afán de fortalecer el sistema de control interno institucional.

De acuerdo con nuestros registros se determinó que existen dos (2) recomendaciones pendientes de cumplimiento del informe AG-388-12, las cuales corresponderían a las recomendaciones N°4.1 y N°4.3. La primera de ellas (N°4.1) es relativa al cumplimiento de las *Normas Técnicas para la Gestión y el Control de las Tecnologías de Información emitidas por la Contraloría General de la República*; la cual quedará pendiente de verificación y no será considerada en el presente informe, por las razones detalladas en el apartado "1.4 Limitaciones"; por lo que su estado de cumplimiento se informará en el próximo informe de labores según nuestro Plan Anual de Trabajo 2020 que se emitirá en el mes de febrero del mismo año.

La segunda recomendación (N°4.3) está relacionada con la elaboración de un plan de cumplimiento de recomendación anteriores, que incluye la atención de noventa y seis (96) observaciones vinculantes de cumplimiento, correspondientes a los informes AG-408-09 (24), AG-204-10 (1) y AG-302-11 (71) según consta en el Anexo N°1 del dicho informe AG-388-12 citado en el párrafo anterior.

Todas estas recomendaciones fueron generadas por Auditorias Externas contratadas para auditar el tema de Tecnologías de Información. En total suman noventa y ocho (98) recomendaciones y por tanto están sujetas de verificación técnica para evaluar su cumplimiento (Ver Cuadro N°1).

Cuadro N°1
Cantidad de Recomendaciones Verificadas

Total de recomendaciones	98
Menos: Cantidad de Recomendaciones cuyas limitantes presentadas en el presente estudio, impiden su verificación (N°4.1 del informe AG-388-12).	1
Total de Recomendaciones objeto de verificación	**97**

Fuente: Elaboración propia con información del archivo gestión Auditoria Interna.

A continuación, se presenta un cuadro que muestra las recomendaciones objeto de verificación en el estudio.

Cuadro N°2
Cantidad de recomendaciones objeto de verificación

OFICIO	INFORME	RECOMENDACIONES SUJETAS A SEGUIMIENTO	OTROS ESTUDIOS	GRAN TOTAL
AG-388-2012	Auditoría especial para el Área de Tecnología de Información	4.1*		
		4.3		1
	Anexo N°1	96	AG-408-09	24
			AG-204-10	1
			AG-302-11	71
TOTAL				97

Fuente: Elaboración propia con información del archivo gestión Auditoria Interna. * Limitantes para su verificación.

2.1.- Estado de cumplimiento de las recomendaciones pendientes (N° 4.1 y N° 4.3) propias del informe AG-388-12

Tal como se indicó líneas anteriores, por la tardanza en la entrega de la información surge una limitante para poder evaluar el cumplimiento de la recomendación N°4.1 del informe AG-388-12, por lo cual su cumplimiento queda pendiente de verificación y los resultados se incorporarán en el próximo informe de labores según nuestro Plan Anual de Trabajo 2020 que se emitirá en el mes de febrero del mismo año.

En torno a la recomendación N° 4.3 de dicho informe AG-388-12 y con base en la información aportada por la Unidad de TI y análisis realizado por esta Auditoría, esta recomendación se da por cumplida.

Esto nos da un balance en el que de las dos últimas recomendaciones pendientes y propias del informe AG-388-12, una recomendación queda pendiente de verificación futura y una recomendación se da por cumplida o terminada.

2.2.- Estado de cumplimiento de las recomendaciones detalladas en el Anexo 1 del informe AG-388-12.

2.2.1 Recomendaciones pendientes de cumplimiento correspondientes al informe AG-408-09, según el Anexo N°1 del informe AG-388-12:

De conformidad con el Anexo N°1 del informe AG-388-12 se determinó un total de veinticuatro (24) recomendaciones pendientes de cumplimiento, provenientes del informe AG-408-09. A este respecto una vez analizadas y valoradas según la información a la que tuvo acceso esta Auditoría, se determina que diecinueve (19) de ellas se encuentran cumplidas, una (1) se encuentra obsoleta, tres (3) no aplican (de estas tres, una de ellas se traslada al cumplimiento de la recomendación N°4.2.1 del informe N° CR-INCOP-AI-I-008-2019 sobre vulnerabilidades físicas de TI) y una (1) de ellas quedó pendiente de cumplir, mostrando un avance de cumplimiento parcial de un 80% aproximadamente.

En términos más generales, lo anterior quiere decir que de las veinticuatro (24) recomendaciones pendientes de cumplimiento según el Anexo N°1 del informe AG-388-12 y pertenecientes al informe AG-408-09; veintitrés (23) de ellas se pueden dar por cerradas o atendidas y solo una de ellas se encuentra en estado pendiente de cumplimiento. La recomendación pendiente con un avance de cumplimiento parcial del 80%, es la N°23 la cual tiene que ver con la existencia de un "Plan de Continuidad" y mantiene esta condición por cuanto no se logró encontrar evidencia de que comprobara

que la efectividad del mismo haya sido sometida a prueba o simulacros. El detalle de esta recomendación puede encontrarse en el Anexo A del presente informe.

2.2.2 Recomendaciones pendientes de cumplimiento, correspondientes al informe AG-204-10, según el Anexo N°1 del informe AG-388-12:

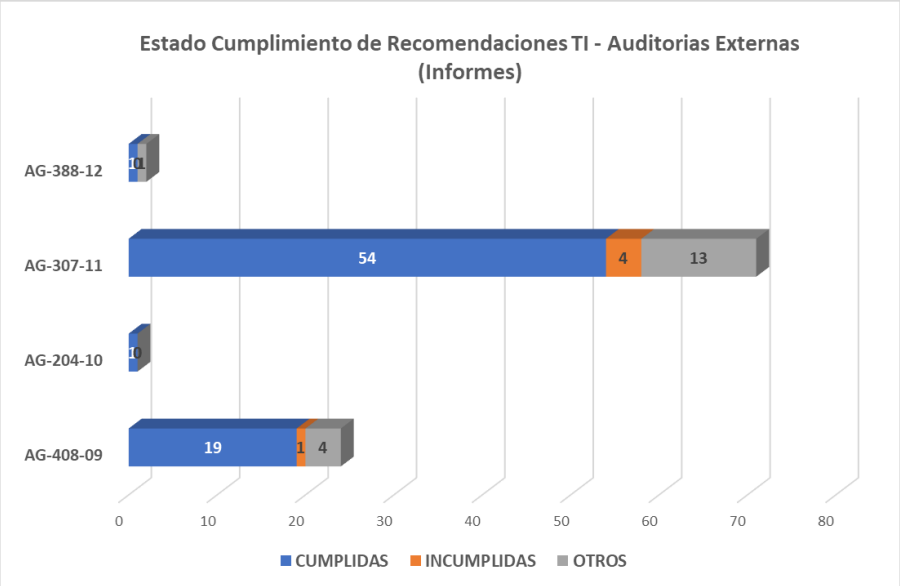
De conformidad con el Anexo N°1 del informe AG-388-12 se determinó un total de una (1) recomendación pendiente de cumplimiento, proveniente del informe AG-204-09. A este respecto una vez analizada y valorada según la información a la que tuvo acceso esta Auditoría, se determina que dicha recomendación (1) se encuentra cumplida.

2.2.3 Recomendaciones pendientes de cumplimiento correspondientes al informe AG-302-11, según el Anexo N°1 del informe AG-388-12:

De conformidad con el Anexo N°1 del informe AG-388-12 se determinó un total de setenta y una (71) recomendaciones pendientes de cumplimiento, provenientes del informe AG-302-11. A este respecto una vez analizadas y valoradas según la información a la que tuvo acceso esta Auditoría, se determina que cincuenta y cuatro (54) de ellas se encuentran cumplidas, tres (3) se encuentran obsoletas, diez (10) no aplican y cuatro (4) de ellas quedaron pendientes de cumplimiento, mostrando muy poco avance en su cumplimiento parcial sobre estas últimas.

En términos más generales, lo anterior quiere decir que de las setenta y una (71) recomendaciones pendientes de cumplimiento según el Anexo N°1 del informe AG-388-12 y pertenecientes al informe AG-302-11; sesenta y siete (67) de ellas se pueden dar por cerradas o atendidas y solo cuatro de ellas se encuentran en estado pendiente de cumplimiento. Las recomendaciones pendientes de cumplimiento son las N°42, N°43, N°44 y N°45; las cuales tienen relación con un mismo tema y es la "Administración de Configuraciones". El detalle de estas recomendaciones puede encontrarse en el Anexo A del presente informe.

RESULTADOS DE SEGUIMIENTO RECOMENDACIONES TI POR INFORME



Fuente: Elaboración propia según valoración de la auditoria interna.

Fuente: Elaboración propia según valoración de la auditoria interna.

III. CONCLUSIÓN

Se concluye que la administración, si bien ha realizado un esfuerzo razonable para el cumplimiento de las recomendaciones objeto de este seguimiento, no se muestra una cultura arraigada hacia el sentido de urgencia para instrumentalizar estas, con el fin de fortalecer el sistema de control interno concerniente al área de tecnología de información institucional.

También se extrañó una supervisión más activa y de seguimiento oportuno por quienes corresponda, hacia la gestión y resultados de la Unidad de TI, dejando entrever la necesidad de fortalecer el cumplimiento de las recomendaciones a esa área. Ello evidencia que el cumplimiento de la recomendación N°23 del informe AG-408-09 (Ver Anexo A) mantuviera hasta el día de hoy, un estancamiento en su nivel de cumplimiento cercano al 80%, por no ejecutarse pruebas y simulacros necesarios para validar la efectividad de los planes de Continuidad y Recuperación del Negocio, denotando cierto nivel de desatención por parte de la Unidad de TI y de aquellos que tienen a su cargo la supervisión de dicha unidad.

Finalmente, conviene indicar que el objetivo del presente estudio fue alcanzado, pese a las limitaciones de no poder evaluar una de las principales recomendaciones; pudiendo constatar que el 94% de las recomendaciones emitidas en informes anteriores y dirigidas a la Unidad de Tecnologías de Información se encuentran atendidas, lo cual representa una cifra razonable. A este respecto, lograr la implementación de las recomendaciones de Auditoría es importante, pues, a través de ello se ve fortalecido de modo continuo el Sistema de Control Interno en procura de la consecución de los objetivos institucionales.

IV. RECOMENDACIÓN

A la Junta Directiva.

4.1. Girar las instrucciones correspondientes a la Gerencia General para que se gestione ante las unidades administrativas involucradas, el cumplimiento cabal de las recomendaciones en estado incumplido, según lo informado en el presente informe (Ver Anexo A) y se establezcan controles efectivos y de seguimiento para evitar situaciones como las comentadas en el presente documento.

DOCUMENTO FIRMADO CON CERTIFICADO DIGITAL
N ° 3957-00072427324A
MARVIN CALERO ALVAREZ

Además, en un plazo de seis (6) meses, se brinde un informe a esa estimable Junta Directiva, con copia a esta Auditoría Interna, sobre los resultados finales de su cumplimiento.

Atentamente,

MARVIN CALERO ALVAREZ (FIRMA)
Firmado digitalmente por MARVIN CALERO ALVAREZ (FIRMA)
Fecha: 2019.12.03 12:48:22 -06'00'

Lic. Marvin Calero Alvarez
Auditor Interno

AI-07/2-SS-RI-RE

ANEXO A

Resultado de evaluación del estado de cumplimiento de recomendaciones de Auditorías Externas, pendientes de cumplimiento según Anexo N°1 de informe AG-388-12.

Recomendaciones	Estado
Seguimiento a los estudios de auditoría de TI para el periodo 2009 - AG-408-09	
1. Implementar la estructura organizacional contenida en la actualización del PETIC, ya aprobada por las instancias correspondientes y dotarla del personal faltante, según el proceso de selección establecido por el área de Recursos Humanos.	Obsoleta
2. Documentar los procesos de la función de TI.	Cumplida
3. Iniciar la ejecución del Plan de Capacitación del Período 2009 – 2012.	Cumplida
4. Observar los comentarios indicados en cada uno de los puntos del Diagnóstico, del Plan de Corto Plazo y del Plan Estratégico: Definición de funciones, Cantidad de recursos disponibles y Entrenamiento	Cumplida
5. El INCOP no cuenta con un Plan Estratégico Institucional.	Cumplida
6. No fue posible establecer el alineamiento institucional del Plan Estratégico de Tecnología de Información y Comunicación, PETIC.	Cumplida
7. Los riesgos ni los controles asociados con las funciones tecnológicas no son valorados con criterios uniformes que reduzcan la subjetividad y los criterios personales limitados.	Cumplida
8. Los actuales procesos utilizados para el SAI, serán desplazados por los que se implementarán para el SIAF, los que se encuentran actualmente en la etapa de levantamiento.	Cumplida
9. Por los cambios recientes, y el poco tiempo que ha tenido el personal para conocer, comprender, interiorizar y aplicar las disposiciones de seguridad lógica y física, su compromiso se mantiene en un nivel bajo.	Cumplida
10. Aunque están establecidos, no se aplican los procedimientos para el ingreso y salida de equipos computacionales en las instalaciones del INCOP.	Se traslada (N/A)
11. No se cuenta con control para la utilización de dispositivos móviles de almacenamiento de datos (llaves maya) en los equipos institucionales.	Cumplida
12. La Institución no cuenta con planes de Recuperación de Desastres ni Continuidad de Negocio.	Cumplida
13. La Unidad de Tecnologías de Información no participa en el desarrollo ni la implementación de los aplicativos Delphos e IDEA.	Cumplida
14. La Unidad de Tecnologías de Información no cuenta con la autoridad, nivel, posición ni recursos suficientes para ejecutar efectiva y eficientemente las funciones que le han sido asignadas.	Cumplida
15. El costo de los proyectos se registra por los costos directos involucrados, omitiendo otros conceptos que reflejen el verdadero costo total de estos.	N/A
16. En la revisión de cumplimiento observamos algunos requerimientos de la normativa no contemplados en las disposiciones de la Institución, otros pendientes de documentar, como procedimientos y guías.	Cumplida
17. No se cuenta con los procedimientos para formalizar los acuerdos de niveles de servicios, los cambios a estos y la evaluación de cumplimiento.	Cumplida
18. Actualmente no se ejerce un monitoreo continuo y sistemático de la capacidad de desempeño, y uso de la plataforma institucional.	Cumplida
Recomendaciones	**Estado**

19. El mantenimiento de los equipos que utilizan los usuarios, es prestado por una posición contratada por servicios profesionales, que vence próximamente y no puede ser renovado de inmediato.	Cumplida
20. El seguimiento que debe dar el Comité Gerencial de Tecnologías de Información a las funciones generales tecnológicas, no se ha venido aplicando con la continuidad, profundidad y rigurosidad que esta responsabilidad requiere.	Cumplida
21. La evaluación del control interno institucional no mantiene una estrecha vinculación con la valoración de los riesgos, de manera que esta se convierta en un insumo para la mejora continua.	Cumplida
22. La Auditoría Interna no cuenta con personal especializado para las evaluaciones complejas en el ámbito de las tecnologías de información.	N/A
23. Desarrollar, aprobar, difundir e implementar a la brevedad posible los planes de Recuperación de Desastres y de continuidad de negocio, realizando pruebas y simulacros periódicos de funcionamiento y dándoles el mantenimiento para que permanezcan actualizados y operativos en todo momento.	Parcial
24. En la cartera de proyectos se encuentra el desarrollo de una Contabilidad de Costos, cuyo modelo está siendo elaborado. Este módulo definitivamente debe estar integrado con el SIAF, aunque la administración del proyecto no se encuentre bajo la responsabilidad de la Unidad de Tecnologías de Información. También debe cumplir con todos los estándares, disposiciones y lineamientos para las tecnologías de información establecidos en INCOP.	Cumplida
Seguimiento a los estudios de auditoría de TI para el periodo 2010 – AG-204-10	
1. Documentar todos los procesos de TI.	Cumplida
Seguimiento a los estudios de auditoría de TI para el periodo 2011 – AG-302-11	
Hallazgo 1: Usuarios por Defecto de los Servidores Windows habilitados	
1. Evaluar la posibilidad de eliminar los privilegios asignados o deshabilitar la cuenta de "Administrador" en todos los servidores Windows, con el fin de que esta no pueda ser utilizada para la administración del sistema operativo.	Cumplida
2. Deben crearse cuentas de usuario alternas para realizar actividades de administración sobre dichos servidores, con eso se evita el uso de la cuenta "Administrador".	Cumplida
3. Establecer las acciones correctivas en el caso de detectase acceso no autorizado con la cuenta "Administrador".	Cumplida
4. Debe considerarse que antes de la implementación de las recomendaciones propuestas debe realizarse una evaluación de los servicios que se encuentran dependientes del usuario "Administrador" de manera que en el caso de que se deshabilite no se generan errores o problemas por la dependencia de dichos servicios al usuario indicado.	Cumplida
Hallazgo 2: Usuarios Genéricos activos en los Sistemas de Información	
5. Evaluar el uso de los usuarios genéricos y proceder a inactivar o eliminar los usuarios genéricos de manera que cada usuario utilice únicamente la cuenta de usuario asignada para uso de las aplicaciones.	Cumplida
6. Levantar una lista de las cuentas genéricas cuyo uso sea indispensable, donde se indique el responsable de la cuenta y el uso de esta. Esta lista debe encontrarse formalmente autorizada.	Cumplida
Hallazgo 3: Plan Integral de Seguridad de la Información	
Recomendaciones	**Estado**

7. Desarrollar un plan integral de seguridad de la información que contemple entre otros aspectos los siguientes: estrategia Integral de Seguridad de la Información, revisiones independientes de la seguridad de la información, identificación de riesgos relacionadas con partes externas, responsabilidades en la divulgación de información, perímetro de seguridad física, remoción de derechos de acceso, protección contra amenazas externas y del ambiente, directrices de clasificación de la información, propiedad de activos, respaldos de información, seguridad en el cableado, seguridad en la reutilización y eliminación de equipos, uso de contraseñas, entre otros.	Cumplida
8. Desarrollar un plan de capacitación y concientización en cuanto a seguridad de información en las áreas usuarias.	Cumplida
Hallazgo 4: Segregación de Funciones en los Perfiles de Usuario del Sistema SIAF	
9. Diseñar, aprobar, divulgar e implementar un procedimiento de revisión periódica, por parte de cada responsable, jefatura o gerencia correspondiente, de los privilegios asociados a los perfiles de usuario, con el fin de verificar la validez, vigencia y la adecuada segregación de funciones de cada uno de ellos, de forma tal que los responsables de cada área usuaria del INCOP garanticen los accesos asignados a los usuarios que tienen a su cargo. Es importante mantener evidencia documentada del resultado del proceso de revisión de accesos.	Cumplida
Hallazgo 5: Segregación de Funciones en la Administración de Seguridad del Sistema SIAF	
10. Definir un perfil de usuario único en la aplicación SIAF, al cual se le otorguen los privilegios para administrar la seguridad del aplicativo. Este perfil debería ser asignado solamente al personal responsable de la administración de la seguridad del sistema.	Cumplida
11. Al perfil administrador, definirle solamente los privilegios para administrar la seguridad del aplicativo, con el fin de que no cuente con privilegios ilimitados sobre los otros módulos de la aplicación	Cumplida
Hallazgo 6: Usuarios Administradores del Sistema SIAF y Base de Datos SQL	
12. Efectuar una revisión general sobre las cuentas de usuario con privilegios administrativos y corroborar que las cuentas con estos privilegios son usuarios autorizados que requieren dichos privilegios para efectuar sus funciones diarias.	Cumplida
13. Removerle los privilegios administrativos al usuario “optec”, ya que este no los requiere para efectuar sus funciones.	Cumplida
14. Ver la posibilidad de implementar ventanas de mantenimiento, en las cuales se le brinde acceso al proveedor para que realice el mantenimiento respectivo, una vez terminado dicho mantenimiento proceder a revocar los accesos otorgados al proveedor.	N/A
15. Efectuar un monitoreo periódico de las transacciones que realiza el proveedor, con el fin de identificar transacciones no autorizadas.	Obsoleta
Hallazgo 7: Bitácoras de Registro de Eventos en los Sistemas de Información y Bases de Datos	
16. Evaluar la posibilidad de habilitar el nivel de auditoría de la base de datos SQL, con el fin de que se registren los accesos fallidos y exitosos; además, habilitar el modo de auditoría C2 del SQL Server o identificar e implementar métodos alternativos para registrar los eventos ocasionados en la Base de Datos.	N/A
Hallazgo 8: Revisiones Periódicas de las Pistas de Auditoría	
17. Diseñar, aprobar, divulgar e implementar un procedimiento formal para la revisión periódica de las bitácoras de los sistemas información y base de datos.	Cumplida
Recomendaciones	**Estado**

18. Es importante que estas revisiones sean documentadas formalmente, así también las acciones a seguir en caso de identificar accesos no autorizados o algún tipo de incidente.	Cumplida
Hallazgo 9: Revisión Periódica de Privilegios de Usuario en el Sistema SIAF	
19. Diseñar, aprobar, divulgar e implementar un procedimiento formal para la revisión periódica, por parte de cada responsable, jefatura o gerencia correspondiente de los accesos otorgados a los usuarios en el sistema SIAF, con el fin de verificar la validez, vigencia y la adecuada segregación de funciones de cada uno de ellos, de forma tal que los las jefaturas, gerencias y direcciones, garanticen los accesos asignados a los usuarios que tienen a su cargo. Es importante mantener evidencia documentada del resultado del proceso de revisión de accesos.	N/A
Hallazgo 10: Parámetros de Contraseña en el Sistema SIAF	
20. Evaluar la posibilidad de agregarle seguridad a la conformación de las contraseñas de los usuarios en el sistema SIAF. Se recomienda parametrizar esta seguridad de la siguiente forma: Mínimo 6 caracteres de longitud en la contraseña, Vencimientos entre 30 a 60 días, Uso de históricos de contraseñas (al menos validar las últimas 6 contraseñas), uso de contraseñas complejas (Alfa-numéricas), bloqueo de contraseña después de 3 intentos fallidos.	Cumplida
Hallazgo 11: Vencimiento de Contraseñas	
21. Se recomienda parametrizar la caducidad de las contraseñas del Servidor de Dominio en un lapso de tiempo entre los 30 y 90 días y que esta política le sea aplicada a todos los usuarios, incluyendo los administradores de los sistemas. En caso de que existan usuarios especiales que deban quedar exentos de estos controles, debe mantenerse documentación formal en donde se autorice dicha excepción.	Cumplida
Hallazgo 12: Usuarios activos ligados Ex funcionarios del INCOP	
22. Deshabilitar los usuarios anteriormente indicados.	Cumplida
23. Desarrollar un procedimiento, en conjunto con Recursos Humanos o las áreas de la entidad que correspondan, para que se notifique de manera formal al departamento de Tecnología de Información, los retiros del personal.	Cumplida
24. Es importante mantener evidencia de las solicitudes de eliminación de accesos realizadas por el personal autorizado.	Cumplida
Hallazgo 13: Solicitud y Aprobación de Roles de Acceso a los Datos	
25. Fortalecer el procedimiento para la solicitud de y asignación de privilegios en el sistema SIAF, de tal manera que exista una autorización formal por parte de las jefaturas de las área de negocio, para los privilegios que posea cada usuario y que estas solicitudes se encuentren archivadas y	Cumplida
Hallazgo 14: Administración de Contraseñas Sensitivas	
26. Establecer un procedimiento formal para el resguardo y custodia de contraseñas sensitivas de la plataforma tecnológica en un lugar seguro dentro de la entidad. El procedimiento debe indicar el personal responsable de actualizar dicha información así como el personal autorizado para accederla.	Cumplida
27. Es conveniente que esta información se encuentre debidamente custodiada en una caja de seguridad con acceso restringido.	Cumplida
28. Se debe implementar un control de bitácora en donde se mantenga un registro de las personas que acceden a dicha información considerando la fecha, y el motivo para el cual se requiere.	Cumplida
Hallazgo 15: Sitio Alterno de Procesamiento de la Aplicación SIAF	
29. Evaluar la posibilidad de implementar un sitio alterno de procesamiento, en el cual se posea una plataforma de contingencia para el procesamiento de la información	Cumplida

del sistema SIAF, los cuales deben ser ubicados fuera de las instalaciones donde se encuentran situados los servidores de procesamiento principal.	
30. Implementar las siguientes medidas de seguridad física y ambiental para el resguardo de los servicios alternos de procesamiento del Sistema SIAF: Mecanismos para la detección y extinción de fuego, seguridad de acceso físico y monitoreo de los accesos que se presenten a la sala de los servidores, Aislar el centro de datos del tránsito de personas y de cualquier amenaza ambiental (Agua, fuego, polvo, etc.)	Cumplida
Hallazgo 16: Plan de Contingencias del Sistema SIAF	

Recomendaciones	Estado
31. Se debe diseñar, aprobar, difundir e implementar un procedimiento para el control de sus operaciones en un evento de contingencia. Este plan debe incluir, entre otros puntos, lo siguiente: análisis del impacto ante una contingencia, análisis de riesgo en los procesos críticos, definición de la estrategia de continuidad, manejo de crisis durante la contingencia, respuesta de emergencia, desarrollo y documentación del plan, pruebas para evaluación de la efectividad de las medidas tomadas, mantenimiento del plan ante cambios tecnológicos o de procesos críticos.	Cumplida
Hallazgo 17: Procedimiento para la Ejecución de Respaldos del Sistema SIAF	
32. Diseñar un procedimiento formal para la ejecución periódica de los respaldos del Sistema SIAF, el cual incluya al menos lo siguiente: información a respaldar, periodicidad de la ejecución de los respaldos, método de almacenamiento de los respaldos, periodicidad del almacenamiento externo de los respaldos, proceso de restauración periódica (Pruebas de legibilidad), control de ejecución de los respaldos y del almacenamiento, retención de respaldos (Respaldos Históricos (Mensuales, Anuales, etc.)	Cumplida
33. Definir diferentes procesos programados para la ejecución de los respaldos (una tardea por cada día de la semana), con el fin de que cada día cuente con su respaldo en diferentes archivos.	Cumplida
Hallazgo 18: Almacenamiento Externo de los Respaldos del Sistema SIAF	
34. Definir en conjunto con el negocio la frecuencia en la que los respaldos deben de almacenarse en un lugar externo, con el fin de minimizar la pérdida de información en caso de que se presente una contingencia. La frecuencia del almacenamiento externo de los respaldos, se debe definir mediante un análisis de impacto en el negocio, donde se debe identificar para cada uno de los procesos el tiempo de recuperación objetivo (RPO, por sus siglas en inglés), el cual se mide en unidades de tiempo: un RPO de cero segundos, significa que el proceso, cuando restaure su operación luego de una interrupción, debe mantener la misma información que antes del evento, un RPO de 1 hora significa que es aceptable perder hasta una hora de información cuando se restaure la operación.	Cumplida
Hallazgo 19: Cifrado de la Información en los Medios Externos de Respaldo	
35. No se establece una recomendación concreta, se deriva del nombre del hallazgo.	N/A
Hallazgo 20: Procedimiento para la Ejecución Periódica de Pruebas de Legibilidad de los Medios Externos de Respaldo	
36. Diseñar, implementar y divulgar un procedimiento para la ejecución de restauraciones de las cintas de respaldos periódicamente.	Obsoleto
37. Crear una bitácora de las restauraciones periódicas realizadas para guardar evidencia de la tarea realizada y su resultado.	N/A
Hallazgo 21: Procedimiento para la Destrucción de Medios Externos de Respaldo	

38. Diseñar, implementar y divulgar un procedimiento para la destrucción controlada de medios de almacenamiento externos.	Cumplida
39. Crear una bitácora de los medios de almacenamiento destruidos.	Cumplida
Hallazgo 22: Política de Clasificación de la Información	
40. El INCOP debe crear un procedimiento para la clasificación de la información que aplique a todo el Instituto, basado en que tan crítica y sensible es la información. Este esquema debe incluir detalles acerca de la propiedad de datos, la definición de niveles apropiados de seguridad, controles de protección y destrucción de datos.	Cumplida
41. Se recomienda utilizar un esquema de clasificación de la información para definir un conjunto apropiado de niveles de protección y comunicar la necesidad de medidas especiales de gestión.	Cumplida
Hallazgo 23: Repositorio Centralizado de Configuración	
Recomendaciones	**Estado**
42. Establecer un repositorio centralizado que contenga toda la información relevante sobre los elementos de configuración.	Incumplida
43. Mantener una línea base de los elementos de configuración para todos los sistemas y equipos sensitivos de la plataforma del Sistema SIAF.	Incumplida
44. Establecer procedimientos de configuración para soportar la gestión y rastro de todos los cambios al repositorio de configuración. Integrar estos procedimientos con la gestión de cambios.	Incumplida
45. Realizar una revisión periódica de los datos de configuración para verificar la integridad de la configuración actual e histórica. Reportar y corregir los errores en las configuraciones.	Incumplida
Hallazgo 24: Acuerdos de Niveles de Servicio (SLA´s) no Definidos	
46. Establecer cláusulas o “Service Level Agreement (SLA´s)”, en donde se establezcan los niveles mínimos de servicio a los que el proveedor se compromete a brindar durante el período de la relación contractual, considerando disponibilidad para solventar averías, tiempos de respuesta para la atención inicial, costos por incumplimiento de niveles de servicio ofrecido.	Cumplida
47. Crear una cláusula dentro del contrato definido anteriormente sobre la integridad, confidencialidad, no divulgación, calidad y documentación de los trabajos realizados y la propiedad intelectual del servicio recibido.	Cumplida
Hallazgo 25: Procedimiento para el Control de Cambios en el Sistema SIAF	
48. Adopción de una metodología estándar para los cambios desarrollados en el Sistema SIAF, que sea utilizada en forma consistente por todos los involucrados en este proceso.	Cumplida
49. Para toda modificación efectuada en el Sistema SIAF, se debe mantener documentación formal y autorizada del requerimiento y del pase a producción de dicha modificación.	Cumplida
Hallazgo 26: Documentación del Plan de Pruebas en los Cambios en el Sistema SIAF	
50. Establecer un plan de pruebas integral que defina roles, responsabilidades y criterios de éxito para cada uno de los cambios desarrollados en el Sistema SIAF.	Cumplida
51. El plan debe considerar la preparación de pruebas, requerimientos de entrenamiento, instalación o actualización de un ambiente de pruebas definido, planear / ejecutar / documentar / retener casos de prueba, manejo y corrección de errores y aprobación formal.	Cumplida
52. Debe mantenerse documentación formal de los planes de prueba establecidos y de los resultados obtenidos.	Cumplida
Hallazgo 27: Monitoreo Post Implementación de los Cambios Efectuados en el Sistema SIAF	

53. Establecer un procedimiento para la revisión post-implementación de los cambios realizados en el ambiente de producción del Sistema SIAF, con el fin de corroborar la completa satisfacción de los cambios efectuados.	Cumplida
Hallazgo 28: Procedimiento para Cambios de Emergencia en el Sistema SIAF	
54. Establecer un procedimiento para definir, plantear, evaluar y autorizar los cambios de emergencia que no sigan el proceso de cambio establecido. La documentación y pruebas se realizan, posiblemente, después de la implantación del cambio de emergencia.	Cumplida
55. Documentar y divulgar el procedimiento formal para la atención de cambios de emergencia que se presenten en el Sistema SIAF. El procedimiento debe contar con al menos lo siguiente: procedimiento para la autorización y puesta en marcha del cambio, proceso para documentar los procesos de solicitud y resultados del cambio de emergencia, pruebas efectuadas, si aplica, para la puesta en producción de los cambios de emergencia.	Cumplida
Hallazgo 29: Control de Versiones del Sistema SIAF	
Recomendaciones	**Estado**
56. Diseñar e implementar un procedimiento formal para el control de versiones de los cambios que se realizan al Sistema SIAF, donde se tengan en cuenta los siguientes aspectos: establecer un repositorio central de la configuración de la versiones, se considere información relevante como lo es el nombre, números de versión y detalles de licenciamiento, mantener una línea base de las versiones, de manera que exista un punto de control al cual se pueda retornar después de los cambios.	Cumplida
Hallazgo 30: Control de Ingreso de Datos	
57. Efectuar una revisión total de todas las interfaces de usuario que son utilizadas para ingresar datos y corroborar que el sistema valide de manera correcta la información que es ingresada por los usuarios finales.	N/A
Hallazgo 31: Integridad de Datos entre el Sistema de Facturación y el Sistema SIAF	
58. Corroborar el proceso actual de facturación y el correcto funcionamiento de la interfaz con el sistema SIAF	Cumplida
59. Establecer procedimientos formales para el proceso de facturación y transferencia de información al sistema SIAF, con el fin de que haya una estrecha comunicación entre los responsables de incluir y anular facturas y los responsables de contabilizarlas.	Cumplida
60. Realizar conciliaciones periódicas de la información que se posee en el Sistema de Facturación contra la información de facturas que se encuentra en el Sistema SIAF.	Obsoleto
Hallazgo 32: Transferencia del Archivo de Nómina	
61. Establecer medidas de seguridad en la generación del archivo de la nómina, con el fin de que este archivo no sea posible modificarlo.	Cumplida
62. Validar la posibilidad de que el archivo de la nómina no sea transferido vía correo electrónico. Se debe tener acceso a un portal web del banco para que los sistemas del banco carguen este archivo directamente y mitigar el riesgo de su alteración no autorizada.	Cumplida
Hallazgo 33: Usuarios Finales sin Unidades de Energía Alterna	
63. A la brevedad posible, corregir los fallos que está presentando la UPS que soporta los equipos de los funcionarios del INCOP. Además, validar la posibilidad que la planta eléctrica que brinda redundancia al centro de datos, brinde redundancia también a los usuarios finales de INCOP.	N/A

64. Establecer un mantenimiento preventivo para este y otros dispositivos, con el fin de mitigar el riesgo de que fallen y así evitar contratiempos en caso de un incidente.	N/A
Hallazgo 34: Mantenimiento Preventivo de Dispositivos	
65. Establecer un mantenimiento periódico preventivo para las UPS y Sistema Contra Incendios, con el fin de garantizar su correcto mantenimiento. Es importante dejar evidencia de los reportes de estos mantenimientos.	N/A
Hallazgo 35: Deficiencias Identificadas en el Contrato con el Proveedor OPTEC	
66. Se recomienda que para futuros contratos con el proveedor OPTEC o con cualquier otro proveedor, se tomen en cuenta las situaciones descritas anteriormente, con el fin de que el contrato proteja en una gran medida los servicios que son brindados por los proveedores como los recursos internos del INCOP.	Cumplida
Hallazgo 36: Procedimiento Formal para la Autorización de Cambios Directos de Datos en la Base de Datos	
67. Para futuras modificaciones directas a los datos, analizar y documentar las causas específicas del error en la aplicación, formular una solución basada en el análisis realizado y obtener la aprobación formal por parte de la Gerencia.	Cumplida
68. Establecer un procedimiento para guiar el proceso de modificaciones directas a los datos de la aplicación.	Cumplida
69. No realizar ninguna modificación directamente en la base de datos si es factible solucionar el error por medio de las funciones de anulación o reversión de la aplicación.	Cumplida

Recomendaciones	**Estado**
Hallazgo 37: Calidad de los Datos	
70. Efectuar una revisión profunda y detallada en conjunto con el proveedor, con el fin de corroborar cual fue la causa del por qué estos documentos no se encuentran en la base de datos.	N/A
71. Definir procedimientos formalmente autorizados para la modificación de información directa en la base, donde se establezcan los niveles de autorización para efectuar este tipo movimientos	Cumplida