Benemérito Cuerpo de Bomberos de
Costa Rica
(Cuerpo de Bomberos)

Informe de auditoría externa de sistemas de información del Cuerpo de Bomberos

Al 31 de diciembre de 2020

Crowe Horwath CR, S.A.

Benemérito Cuerpo de Bomberos de Costa Rica
(Cuerpo de Bomberos)

Informe de auditoría externa de Sistemas de Información del Cuerpo de Bomberos

Al 31 de diciembre de 2020

Benemérito Cuerpo de Bomberos de Costa Rica
(Cuerpo de Bomberos)

Índice de contenido

Página

Anexo A Revisión de los sistemas de información según LA 2021LA-000012-0012800001

I. Objetivos	- 5 -
II. Responsabilidad de la Administración	- 5 -
III. Responsabilidad de los auditores y marco normativo	- 5 -
IV. Alcance	- 6 -
V. Procedimientos	- 9 -
VI. Delimitaciones	- 9 -
VII. Metodología de evaluación	- 10 -
VIII. Resultados del periodo 2020 con oportunidades de mejora	- 13 -
IX. Mapa de calor de los riesgos evidenciados al cierre de este informe	- 15 -
X. Estado de los apartados de la Normas Técnicas de Gestión y Control de las TI	- 16 -
XI. Seguimiento de las recomendaciones de periodos anteriores.	- 50 -
Conclusiones	- 60 -
Cuadro # 1	- 61 -

Crowe Horwath CR, S.A.
2442 Avenida 2
Apdo. 7108-1000
San José, Costa Rica
Tel + (506) 2221 4657
Fax + (506) 2233 8072
www.crowe.cr

24 de setiembre de 2021

Señores
Consejo Directivo
Benemérito Cuerpo de Bomberos de Costa Rica
Atención: Sr. Allan Mosquera Vargas,
Auditor Interno

ASUNTO: INFORME DE AUDITORÍA EXTERNA SOBRE LOS SISTEMAS DE INFORMACIÓN

Hemos realizado el trabajo de auditoría convenido con el Benemérito Cuerpo de Bomberos de Costa Rica (BCBCR) específicamente para evaluar, según los términos de la contratación CBCR-018522-2021-PRB-00779, Licitación Abreviada 2021LA-000012-0012800001, el servicio de auditoría externa en Sistemas de Información del BCBCR, con el fin de que evalúe y dé criterio sobre los sistemas de información que se encuentran en funcionamiento o en desarrollo en el BCBCR y el respectivo seguimiento de recomendaciones, referente a las soluciones automatizadas, la adquisición y el mantenimiento que se brinda al software aplicativo, la adquisición y el mantenimiento de la infraestructura tecnológica, la facilidad de operación y uso de los sistemas, la administración de cambios, la seguridad y continuidad de los sistemas, los riesgos que enfrentan los sistemas a nivel local y en la Nube en lo aplicable, adjuntamos informe de auditoría externa.

Los temas tratados no se refieren a empleados en particular y tienen por objeto informar sobre los resultados de los procedimientos de auditoría, conclusiones y recomendaciones.

Nuestra responsabilidad sobre el diagnóstico del informe de auditoría externa sobre los sistemas de información al 31 de diciembre de 2020 se extiende hasta el día 24 de setiembre de 2021. La fecha del diagnóstico del informe de auditoría externa sobre los sistemas de información indica al usuario, que el auditor ha considerado el efecto de los hechos y de las transacciones de los que ha tenido conocimiento y que han ocurrido hasta dicha fecha; en consecuencia, no se amplía por la referencia de la fecha en que se firme digitalmente.

Atentamente,

FABIAN ZAMORA AZOFEIFA (FIRMA)

Firmado digitalmente por FABIAN ZAMORA AZOFEIFA (FIRMA)
Fecha: 2021.10.28 09:14:54 -06'00'

Fabian Zamora Azofeifa
Socio

cc: Presidente del Comité de Tecnología de Información

Crowe Horwath CR, S.A.
2442 Avenida 2
Apdo. 7108-1000
San José, Costa Rica
Tel + (506) 2221 4657
Fax + (506) 2233 8072
www.crowe.cr

Informe del contador público independiente sobre compromisos de seguridad sobre la razonabilidad de los sistemas de información.

Responsabilidad de la Administración

La administración del Benemérito Cuerpo de Bomberos de Costa Rica (BCBCR) es responsable de la administración y control de los sistemas de información que inciden en el resultado Anexo A, que de acuerdo con la NITA 3000 es el presente informe. La responsabilidad de la administración de los Sistemas de Información que se encuentren en funcionamiento incluye establecer los mecanismos y procedimientos necesarios para garantizar razonablemente la confiabilidad, pertinencia, relevancia y oportunidad de la información que se produce de las operaciones del BCBCR, para la salvaguarda de los activos y que sirva de apoyo en la toma de decisiones y en la rendición de cuentas como sana medida de control.

Responsabilidad del Auditor Externo

Hemos realizado el trabajo de auditoría convenido con el BCBCR específicamente para evaluar, según los términos de la contratación CBCR-018522-2021-PRB-00779, Licitación Abreviada 2021LA-000012-0012800001, el servicio de auditoría externa en Sistemas de Información del BCBCR, con el fin de que evalúe y dé criterio con base en el resultado de los procedimientos indicado en el Anexo A, sobre la efectividad de su grado de correspondencia sobre las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE) emitida por la Contraloría General de la República (CGR) y de conformidad con la Ley General de Control Interno de los sistemas de información que se encuentran en funcionamiento o en desarrollo en el BCBCR y el respectivo seguimiento de recomendaciones, referente a las soluciones automatizadas, la adquisición y el mantenimiento que se brinda al software aplicativo, la adquisición y el mantenimiento de la infraestructura tecnológica, la facilidad de operación y uso de los sistemas, la administración de cambios, la seguridad y continuidad de los sistemas, los riesgos que enfrentan los sistemas a nivel local y en la Nube en lo aplicable, adjuntamos informe de auditoría externa.

Se detallan los procedimientos realizados con el fin de expresar criterio si los Sistemas de Información en producción, cumplen con la normativa aplicable a los sistemas de información del BCBCR de forma razonable en cumplimiento de las normas y procedimientos de auditoría que se encuentren vigentes por parte de la Contraloría General de la República (CGR) para la gestión y el control de las Tecnologías de Información o la normativa aplicable vigente, establecida por las autoridades competentes.

Se realizó el trabajo de acuerdo con la Norma Internacional sobre compromisos de seguridad, (NITA 3000), Trabajos para atestiguar distintos a auditorías o de revisiones de información financiera histórica.

Dichas normas requieren planificar y realizar el trabajo para obtener seguridad razonable acerca de las afirmaciones de la administración que son objeto de este estudio.

El trabajo consistió en:

A. Realizar una evaluación integral de la adquisición, planeación, uso, desarrollo, ejecución y control de los Sistemas de Información y de su uso en las diferentes dependencias del BCBCR.

B. Evaluar la adquisición y el mantenimiento de la infraestructura tecnológica, la facilidad de operación y uso de los sistemas, la administración de cambios, la seguridad y continuidad de los sistemas y los riesgos que enfrentan los mismos.

C. Valorar y determinar la racionalidad, transparencia, veracidad y seguridad en los procedimientos llevados a cabo en la institución, referentes a la administración, trámite de los Sistemas de Información y riesgos a nivel local y en la Nube en lo aplicable.

D. Valorar el procedimiento de las transacciones electrónicas que se realizan en el BCBCR, en aras de garantizar su pertinencia y confiabilidad.

E. Evaluar elementos relacionados con las pruebas a los sistemas de información, el gobierno de la Unidad de Tecnologías de Información y Comunicación, el uso y justificación de mejores prácticas para Administrar Proyectos.

F. Evaluar el control de la adquisición, del uso y manejo de activos a cargo de la Unidad de Tecnologías.

G. Probar la vulnerabilidad de los Sistemas, información y/o Apps que están con acceso por la WEB.

H. Verificar la efectividad de los controles de la correspondencia formal y el archivo electrónico.

I. Dar el debido seguimiento a las recomendaciones de periodos anteriores que se encuentren pendientes de ejecutar por la Administración, según último informe emitido de auditoría externa en Sistemas de información del BCBCR.

Cuadro A: Sistemas de información:

N°	Nombre del sistema	Función
1	SICOF - Sistema Institucional de Correo Formal	Sistema centralizado utilizado para la generación de los documentos con número de consecutivo del BCBCR.
2	SIGSA - Sistema Integrado para la Gestión de Seguridad y Accesos de las Aplicaciones	Sistema centralizado para la gestión de accesos y permisos a los sistemas de información institucionales.
3	SIGAE - Sistema de Información Geográfica para la Atención de Emergencias	Sistema centralizado para gestión administrativa y operativa de las Estaciones de Bomberos. Por el tipo de información administrativa que este sistema mantiene, también es utilizado por las dependencias que brindan servicios a las Estaciones de Bomberos, para el despacho de recursos que atienden emergencias, y para la generación de datos estadísticos de la atención de emergencias del país.

N°	Nombre del sistema	Función
4	SIBA - Sistema Integrado de Bitácoras	Sistema centralizado para el registro de transacciones y pistas de auditoría, de los sistemas de información institucionales, que integra a todos los sistemas que BCBCR ha ido desarrollando.
5	SUATT - Sistema Único de Atención a Trámites de Tecnologías	Sistema centralizado para la gestión de requerimientos de los Usuarios institucionales, ante Tecnologías de Información y Comunicaciones.
6	SIABO - Sistema de la Academia de Bomberos	Sistema para la gestión (matrícula, control, recertificaciones) de los procesos de capacitación internos y externos del personal del BCBCR.
7	WebSIIS - Sistema Integrado de Información en Salud	Sistema para la administración de información médica del personal del BCBCR.
8	MIF - Módulo Integrado de Facturación	Módulo para gestión de facturas por venta de servicios u otros ingresos del BCBCR.
9	EVA - Evaluación del Desempeño del Personal	Sistema para la gestión de las Evaluaciones del desempeño del personal del BCBCR.
10	Evolution Main	Sistema utilizado para la gestión de la flotilla vehicular del BCBCR, procesos tales como el registro legal, características técnicas, mantenimiento y reparaciones.
11	ENTERPRISE	Sistema financiero administrativo del BCBCR. Sistema saliente que será sustituido por el sistema Excelsior, actualmente en desarrollo. Sistema integrado administrativo Enterprise: Es un sistema financiero administrativo (ERP), está conformado por los siguientes módulos: Contabilidad, Cuentas por Pagar, Control de Activos, Manejo de Presupuesto, Compras, Control de Inventario, Control y Registro de Personal, Reclutamiento y Selección de Personal, Capacitación de Personal, Pistas de Auditoría, Seguridad y Parametrización.
12	EXCELSIOR	Sistema para la gestión financiera administrativa del BCBCR. Sistema en desarrollo que sustituirá paulatinamente el sistema Enterprise.
13	INSIDE	Sistema centralizado para la publicación de información de uso institucional a disposición del personal del BCBCR, así como los accesos directos a los sistemas informáticos publicados en la web.
14	Módulo de Personal Externo	Registro de personal externo a la Institución que brinda apoyo o es proveedor.
15	PASE	Plataforma de Atención y Servicio de la Academia Nacional de Bomberos.
16	SIMAV Sistema Integrado Mantenimiento Vehicular	Módulo que automatiza el Proceso de Gestión de Contratos, principalmente las funcionalidades de mantenimiento preventivo, mantenimiento correctivo, gira de llantas y gira de baterías a cargo de la Unidad de Mantenimiento Vehicular.
17	SWS	Star Web Sistemas - Factura electrónica (Alquilado).
18	CGP Consola SINPE	Centro de Gestión de Pagos SINPE. (Alquilado).
19	Gestión Virtual del Talento (GVT)	Sistema de apoyo en el proceso de Evaluación del Desempeño.
20	Accesos Web a información: SIAA, SIAA Adm, SIDEB, Outlook Web y Apps como el DTR, Bomberos CR, BomberosCR F5, BomberosCR-Info, Matrícula SIABO, Marcas, Inventarios	Seguridad en el acceso a sistemas y Apps que se consulta vía Web.

Consideramos que el trabajo realizado proporciona un sustento razonable para la opinión.

En consecuencia, y en nuestra opinión, nada ha llegado a nuestro conocimiento que nos haga pensar según los resultados de los procedimientos del Anexo A, que el proceso de la gestión a las soluciones automatizadas, la adquisición y el mantenimiento que se brinda al software aplicativo, la adquisición y el mantenimiento de la infraestructura tecnológica, la facilidad de operación y uso de los sistemas, la administración de cambios, la seguridad y continuidad de los sistemas, los riesgos que enfrentan los sistemas a nivel local y en la Nube al 31 de diciembre de 2020 no es efectivo en relación con Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE) emitida por la Contraloría General de la República (CGR) y de conformidad con la Ley General de Control Interno, en todos los aspectos importantes, excepto por lo indicado en los factores evaluados en 1.4, 1.4.6, y 1.4.7.

Llamamos la atención a lo indicado en la sección VIII de este informe "Resultados del periodo 2020" respecto a la brecha para cumplir con los procedimientos de control que se encuentren vigentes por parte de la Contraloría General de la República (CGR) para la gestión y el control de las Tecnologías de Información.

Llamamos la atención de lo indicado en la sección VI de este informe sobre "Delimitaciones"

No me alcanzan las limitaciones del artículo 9 de la Ley 1038, ni los artículos 20 y 21 del Reglamento a la Ley, ni el artículo 11 del Código de Ética Profesional del Colegio de Contadores Públicos de Costa Rica, para expedir este informe.

Se extiende a solicitud del Benemérito Cuerpo de Bomberos de Costa Rica (BCBCR) según los lineamientos para la contratación del trabajo para atestiguar con seguridad razonable según lo establecido en la Licitación Abreviada N° 2021LA-000012-0012800001.

Nuestra responsabilidad sobre el diagnóstico del informe de auditoría externa sobre los sistemas de información al 31 de diciembre de 2020 se extiende hasta el día 24 de setiembre de 2021. La fecha del diagnóstico del informe de auditoría externa sobre los sistemas de información indica al usuario, que el auditor ha considerado el efecto de los hechos y de las transacciones de los que ha tenido conocimiento y que han ocurrido hasta dicha fecha; en consecuencia, no se amplía por la referencia de la fecha en que se firme digitalmente.

Dada en la ciudad de San José el 24 de setiembre de 2021.

Dictamen firmado por
Fabián Zamora Azofeifa N° 2186
Pol. 0116 FIG 7 V.30-9-2022
Timbre Ley 6663 ¢1.000
Adherido al original

FABIAN ZAMORA AZOFEIFA (FIRMA)

Firmado digitalmente por FABIAN ZAMORA AZOFEIFA (FIRMA)
Fecha: 2021.10.28 09:16:05 -06'00'



Anexo A

Benemérito Cuerpo de Bomberos de
Costa Rica
(BCBCR)

Informe de auditoría externa de sistemas de información del BCBCR

Al 31 de diciembre de 2020

I. Objetivos

Expresar según los términos del Cartel de Contratación, un criterio sobre los Sistemas de Información que tiene en funcionamiento y evaluar las soluciones automatizadas, la adquisición y el mantenimiento que se brinda al software aplicativo, la adquisición y el mantenimiento de la infraestructura tecnológica, la facilidad de operación y uso de los sistemas, la administración de cambios, la seguridad y continuidad de los sistemas, los riesgos que enfrentan los sistemas a nivel local y en la Nube.

Realizar una evaluación del cumplimiento de las "Normas Técnicas para la Gestión y el Control de las Tecnologías de Información" emitidas por la Contraloría General de la República.

Dar seguimiento a las recomendaciones realizadas en los años 2016, 2017, 2018 y 2019 sobre este mismo tema.

II. Responsabilidad de la Administración

La administración del Benemérito Cuerpo de Bomberos de Costa Rica es responsable de la administración y control de los sistemas de información que inciden en el resultado del informe del Anexo A. La responsabilidad de la administración de los Sistemas de Información que se encuentren en funcionamiento incluye establecer los mecanismos y procedimientos necesarios para garantizar razonablemente la confiabilidad, pertinencia, relevancia y oportunidad de la información que se produce de las operaciones del BCBCR, para salvaguardar los activos y que sirva de apoyo en la toma de decisiones y en la rendición de cuentas.

III. Responsabilidad de los auditores y marco normativo

Nuestra responsabilidad consiste en emitir un criterio sobre los Sistemas de Información que están en funcionamiento y evaluar las soluciones automatizadas, la adquisición y el mantenimiento que se brinda al software aplicativo, la adquisición y el mantenimiento de la infraestructura tecnológica, la facilidad de operación y uso de los sistemas, la administración de cambios, la seguridad y continuidad de los sistemas, los riesgos que enfrentan los sistemas, a nivel local y en la nube, para cumplimiento de las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE) emitida por la Contraloría General de la República (CGR).

Los estándares de TI como guías, herramientas y técnicas para auditoría, aseguramiento y control profesional emitidos por ISACA y las buenas prácticas como COBIT, son considerados como criterio y no de acatamiento regulatorio.

La NITA 3000 se refiere a trabajos para atestiguar distintos de auditorías o de revisiones de información financiera histórica, cumpliendo con requisitos éticos así como con la planificación y el desempeño de la auditoría para obtener comprensión del asunto evaluado y otras circunstancias del compromiso, suficiente para identificar y evaluar el riesgo de representaciones erróneas de importancia relativa y suficiente para diseñar y llevar a cabo los procedimientos de obtención de evidencia de auditoría.

Consideramos que el trabajo realizado proporciona un sustento razonable para el reporte.

IV. Alcance

1. Los factores evaluados de las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE) emitida por la Contraloría General de la República (CGR) y de conformidad con la Ley General de Control Interno, se detallan a continuación:

Normas de aplicación general

En la revisión de esta área se verificó lo siguiente:

1. Plan estratégico específico para TI acorde con los objetivos y estrategias de la entidad.
2. Gestión de calidad sobre los servicios y productos de TI.
3. Adecuada valoración de riesgos institucionales.
4. Políticas y procedimientos de seguridad de la información debidamente documentada e implementada.
5. Marco metodológico de Tecnología de Información.
6. Documentación, actualización y capacitación de las responsabilidades del personal interno y de terceros relacionados con seguridad.
7. Ambiente físico seguro y controlado que proteja los recursos de Tecnología de Información.
8. Controles de acceso.
9. Controles para el desecho y reutilización de recursos de Tecnología de Información.
10. Mecanismos de control que aseguren la autenticidad, integridad y confidencialidad de las transacciones.
11. Procedimientos para proteger la información almacenada.
12. Medidas preventivas, detectivas y correctivas para el tratamiento del software malicioso y virus.
13. Políticas y procedimientos para el acceso a la información, al software de las bases de datos y de aplicación.
14. Adecuada clasificación de los recursos de Tecnología de Información de acuerdo con los términos de sensibilidad.
15. Procedimiento de definición de propiedad, custodia y responsabilidad de los recursos de Tecnología de Información.

16. Procedimiento para la definición de perfiles de usuarios.
17. Derechos de acceso a los usuarios de los recursos de Tecnología de Información, de conformidad con las políticas de la entidad bajo el principio de necesidad de saber o menor privilegio.
18. Implementación de medios de autenticación y existencia de un procedimiento que permita controlar dichos medios.
19. Controles de acceso a la información impresa o almacenada en medios físicos.
20. Pistas de auditoría.
21. Manejo de la información sobre seguridad de las Tecnología de Información de manera restringida y controlada.
22. Definición de requerimientos, procedimientos y controles sobre la seguridad en la implementación y mantenimiento de software e infraestructura tecnológica.
23. Procedimientos y documentación de la continuidad de los servicios de Tecnología de Información.
24. Administración de los proyectos de Tecnología de Información.
25. Manejo de la toma de decisiones sobre aspectos estratégicos de Tecnología de Información.
26. Cumplimiento de obligaciones relacionadas con la gestión de Tecnología de Información.

Planificación y organización

27. Procesos de planificación de Tecnología de Información.
28. Modelo de arquitectura de información.
29. Optimización del uso de la infraestructura tecnológica.
30. Independencia y recurso humano de la función de Tecnología de Información.
31. Optimización del uso de los recursos financieros en la gestión de Tecnología de Información.

Implementación de tecnologías de información

32. Consideraciones generales de la implementación de Tecnología de Información.
33. Marco metodológico y controles sobre la implementación del software.
34. Implementación de infraestructura tecnológica.
35. Procedimientos para la contratación de terceros para la implementación y mantenimiento de software e infraestructura.

Prestación de servicios y mantenimiento

36. Procedimientos y controles para la definición y administración de acuerdos de servicio.
37. Procedimientos y controles para la administración y operación de la plataforma tecnológica.
38. Controles para la administración de datos.
39. Atención de requerimientos de los usuarios de Tecnología de Información.
40. Análisis y seguimiento para el manejo de incidentes.
41. Procedimientos para la administración de servicios prestados por terceros.

Seguimiento a los procesos de Tecnología de Información

42. Seguimiento a la implementación de los procesos de Tecnología de Información.
43. Seguimiento a la evaluación del control interno de Tecnología de Información realizado por la administración.
44. Participación de la Auditoría Interna en la evaluación de las operaciones, registros, transacciones y cumplimiento normativo.

2. Realizar una evaluación integral de la adquisición, planeación, uso, desarrollo, ejecución y control de los Sistemas de Información siguientes y de su uso en las diferentes dependencias del BCBCR.

    1. Sistema de Correspondencia Oficial (SICOF)
    2. Sistema para la Gestión de Accesos de las Aplicaciones (SIGSA)
    3. Sistema de Información Geográfica para la Atención de Emergencias (SIGAE)
    4. Sistema para el Registro de Bitácoras (SIBA)
    5. Sistema Único para la Atención de Trámite de Tecnología (SUATT)
    6. Sistema de Academia de Bomberos (SIABO)
    7. Sistema Integrado de Información en Salud (WEBSIIS)
    8. Módulo Integrado de Facturación (MIIF)
    9. Evaluación del Desempeño del Personal (EVA)
    10. Evolution Main (EVOLUTION)
    11. Sistema Financiero Administrativo (ENTERPRISE)
    12. Sistema Financiero Administrativo (EXCELSIOR)
    13. Sistema INSIDE
    14. Módulo de Personal Externo
    15. Plataforma de Atención y Servicio de la Academia Nacional de Bomberos (PASE)
    16. Sistema Integrado Mantenimiento Vehicular (SIMAV)
    17. Sistemas - Factura electrónica (SWS)
    18. Centro de Gestión de Pagos (SINPE)
    19. Sistema de Gestión Virtual del Talento (GVT)
    20. Accesos Web

3. Evaluar la adquisición y el mantenimiento de la infraestructura tecnológica, la facilidad de operación y uso de los sistemas, la administración de cambios, la seguridad y continuidad de los sistemas y los riesgos que enfrentan los mismos.

4. Valorar y determinar la racionalidad, transparencia, veracidad y seguridad en los procedimientos llevados a cabo en la institución, referentes a la administración, trámite de los Sistemas de Información y riesgos a nivel local y en la Nube en lo aplicable.

5. Valorar el procedimiento de las transacciones electrónicas que se realizan en el BCBCR, en aras de garantizar su pertinencia y confiabilidad.

6. Evaluar elementos relacionados con las pruebas a los sistemas de información, el gobierno de la Unidad de Tecnologías de Información y Comunicación, el uso y justificación de mejores prácticas para Administrar Proyectos.

7. Evaluar el control de la adquisición, del uso y manejo de activos a cargo de la Unidad de Tecnologías.

8. Probar la vulnerabilidad de los Sistemas, información y/o Apps que están con acceso por la WEB.

9. Verificar la efectividad de los controles de la correspondencia formal y el archivo electrónico.

10. Dar el debido seguimiento a las recomendaciones de periodos anteriores que se encuentren pendientes de ejecutar por la Administración, según último informe emitido de auditoría externa en Sistemas de información del BCBCR.

V. Procedimientos

Se planeó y ejecutó la auditoría para la evaluación de las áreas mencionadas en el apartado anterior. Las acciones, los resultados de la revisión, las recomendaciones y la evidencia de auditoría específicas por la aplicación de tales procedimientos son detallados en el Anexo A de este informe.

VI. Delimitaciones

Por no tener la normativa legal una matriz de ponderación por magnitud basada en riesgos para la evaluación de las Normas Técnicas de la Contraloría General de la República, se utiliza la ponderación promedio de los atributos evaluados, indicada en el Anexo A.

El Sistema Financiero Administrativo (EXCELSIOR) está compuesto de los módulos Contabilidad, Tesorería, Presupuesto (Formulación y Planificación), Activos Fijos y Aprovisionamiento; existen otros módulos que serán desarrollados cuando se adjudique el proveedor para el desarrollo respectivo.

El nivel de cumplimiento y capacidad de COBIT no se encuentra evaluado en sus 37 procesos, al no estar implementado en la gestión de procesos de tecnología por lo que en esta auditoría se utilizaron los objetivos de COBIT en algunos criterios de este trabajo para reforzar las recomendaciones y no de acatamiento obligatorio.

Los “estándares de Tecnología de Información, guías, herramientas y técnicas para auditoría, aseguramiento y control profesional” emitidos por el ISACA no son evaluados en su totalidad; se utilizan las herramientas y técnicas de auditoría en el proceso de evaluación para este informe.

Para la auditoría de Tecnología de Información se valida la efectividad, seguridad, integridad, automatización y control en los sistemas de información.

El informe corresponde a la evaluación del periodo 2020, con la presentación de evidencia al 31 de agosto de 2021.

VII. Metodología de evaluación

A. Normas técnicas de la Contraloría General de la República

En la evaluación de las Normas Técnicas de la Contraloría General de la República, se aplicó un modelo por medio de un cuestionario, para validar el cumplimiento de cada objetivo a través de los controles establecidos, aunado a la recopilación y análisis de la información y entrevistas in situ, para identificar la situación actual.

Los criterios generales para establecer la ubicación de cada factor conforme al cumplimiento normativo son:

Cumplimiento	Descripción
Cumple	Se muestra desempeño adecuado respecto al factor evaluado.
Cumplimiento parcial alto	Se muestran deficiencias, pero en general el desempeño del factor evaluado es satisfactorio.
Cumplimiento parcial bajo	Se muestra débil desempeño respecto al factor evaluado.
No cumple	La entidad muestra desempeño crítico respecto al factor evaluado, por lo que no es aceptable clasificarlo en ninguno de los tres niveles anteriores.

Las categorías de riesgo se describen a continuación[1]:

Nivel de riesgo	Descripción
Oportunidad	Nivel de riesgo muy bajo, en el cual las oportunidades de ahorro de costos pueden ser disminuir el grado de control o determinar en cuáles oportunidades pueden asumirse mayores riesgos.
Normal	Nivel aceptable de riesgo, por lo general sin realizar una acción en especial excepto para el mantenimiento de los actuales controles u otras respuestas.
Elevado	Riesgo elevado, por encima del riesgo tolerable; la entidad puede, como política interna, mitigar el riesgo u otra respuesta adecuada definida dentro de un tiempo límite.
Inaceptable	Se estima que este nivel de riesgo es mucho más allá de su riesgo tolerable; cualquier riesgo que se encuentre en esta clasificación puede desencadenar una respuesta inmediata al riesgo.

[1] Datos tomados del Manual CRISC (*Certified in Risk and Information Systems Control*), emitido por el ISACA.

B. Sistemas de información

En la evaluación de los sistemas de información en producción se hace una valoración integral de la adquisición, planeación, uso, desarrollo, ejecución, seguridad, continuidad y control de los sistemas de información y de su uso. Se aplicaron cuestionarios y entrevistas de forma virtual con los usuarios expertos, jefaturas y técnicos, previa planificación y coordinación con las áreas.

Los resultados fueron tabulados, analizados y se presentan en el informe los sistemas que generaron una oportunidad de mejora se desarrollan en la sección de resultados.

En los casos requeridos se hizo solicitud de evidencia para respaldar los resultados identificados y dar seguimiento a los comentarios del periodo anterior.

Se identificaron oportunidades de mejora que son comunicadas.

C. Seguimiento a las recomendaciones anteriores

Se ejecutaron las siguientes acciones:

a) Revisar el informe de auditoría de sistemas de información externo del periodo 2019.
b) Extraer y preparar una matriz con las recomendaciones, para darle seguimiento por medio de la Auditoría Interna, Planificación y las validaciones respectivas en el cumplimiento de las recomendaciones.
c) Evaluar la evidencia recibida, las entrevistas y las pruebas aplicadas para indicar el estado de los hallazgos por medio de los siguientes estados:

Respuesta	Descripción
Atendido	Se ha cumplido y revisado lo indicado en la recomendación
En proceso	Se han ejecutado acciones, pero faltan para cumplir las observaciones
Pendiente	No se han realizado acciones para atender la (s) recomendación (es)
N/A	La recomendación no aplica, por eventos o acciones realizadas.

d) Aplicar la siguiente metodología de riesgos cualitativos para valorar las recomendaciones.

   De acuerdo con la evaluación de control interno de la Unidad Tecnología de Información y con base en el riesgo que representa para los recursos de Tecnología de Información (aplicaciones, información, infraestructura y personas), se presenta el mapa de riesgos que resume la relación entre el impacto para la organización y la probabilidad de materialización del riesgo que garantice la alineación con los criterios de información (efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad).

D. Determinación del cumplimiento y nivel de exposición al riesgo

Para obtener el nivel de exposición al riesgo nos hemos basado en la aplicación de una matriz de 25 cuadrantes (5 verticales y 5 horizontales), en la cual el riesgo de los factores es determinado por su ocurrencia e impacto.

Para cada acción evaluada que presenta incumplimiento hemos determinado el nivel de impacto y ocurrencia y obtuvimos el nivel de exposición al riesgo basados en la matriz indicada anteriormente.

La frecuencia (cuadrantes horizontales) se basa en la verificación de las siguientes categorías:

Muy baja	La probabilidad de ocurrencia es insignificante, puede ocurrir solo en circunstancias excepcionales.
Baja	Tiene poca probabilidad de ocurrencia; no se espera que ocurra en cierto periodo de tiempo.
Frecuente	El evento ocurrirá más de una ocasión en un determinado lapso.
Alta	Se espera que suceda en muchas ocasiones en un periodo de tiempo dado, en circunstancias definidas.
Muy alta	Se materializa de forma continua y ocurrirá bajo muchas circunstancias.

El impacto (cuadrantes verticales) se basa en las siguientes categorías:

Insignificante	El costo no afecta la entidad. No es necesario tomar medidas al respecto.
Mínimo	La materialización podría traer un costo para la entidad, sin embargo, no es de importancia para los resultados de la entidad. Debe valorarse los motivos de la materialización del riesgo.
Moderado	Su materialización conlleva un costo para la entidad que puede incluir pérdidas. Deben establecerse medidas de prevención para posibles eventos.
Serio	Representa un costo elevado. Las medidas que deben tomarse son correctivas y preventivas.
Crítico	El costo asumido no es tolerable y es necesario tomar medidas correctivas inmediatas.

A continuación, presentamos la matriz de 5 x 5 cuadrantes

		Frecuencia				
Impacto		**Muy baja**	**Baja**	**Frecuente**	**Alta**	**Muy alta**
	Crítico	5	10	15	20	25
	Serio	4	8	12	16	20
	Moderado	3	6	9	12	15
	Mínimo	2	4	6	8	10
	Insignificante	1	2	3	4	5

Calificaciones:

Basado en los resultados de los análisis por acción se determina el nivel de exposición al riesgo de acuerdo con los siguientes rangos:

De 1 a 2:	El nivel de riesgo es de oportunidad.
De 3 a 9:	El nivel de riesgo es normal.
De 10 a 12:	El nivel de riesgo es elevado.
De 15 a 25:	El nivel de riesgo es inaceptable.

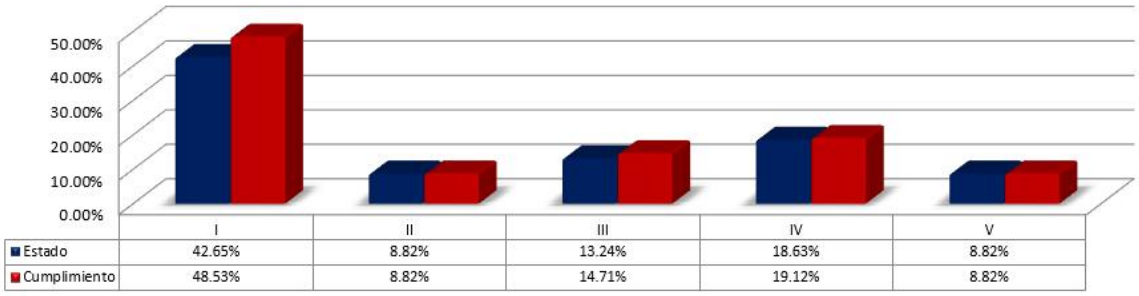
VIII. Resultados del periodo 2020 con oportunidades de mejora y en proceso de atención de los apartados de las Normas Técnicas de la Contraloría General de la República

Ref.	Descripción del criterio	Nivel de cumplimiento	Nivel de riesgo
1.1	Marco Estratégico de TI	Cumple	Normal
1.2	Gestión de la calidad	Cumple	Normal
1.3	Gestión de riesgos	Cumple	Normal
1.4	Gestión de la seguridad de la información	Cumplimiento parcial bajo	Elevado
1.4.1	Implementación de un marco de seguridad de la información	Cumplimiento parcial alto	Normal
1.4.2	Compromiso del personal con la seguridad de la información	Cumple	Normal
1.4.3	Seguridad física y ambiental	Cumple	Normal
1.4.4	Seguridad en las operaciones y comunicaciones	Cumplimiento parcial alto	Normal
1.4.5	Control de acceso	Cumple	Normal
1.4.6	Seguridad en la implementación y mantenimiento de software e infraestructura tecnológica	Cumplimiento parcial bajo	Elevado
1.4.7	Continuidad de los servicios de TI	Cumplimiento parcial bajo	Elevado
1.5	Gestión de proyectos	Cumplimiento parcial alto	Normal
1.6	Decisiones sobre asuntos estratégicos de TI	Cumplimiento parcial alto	Normal
1.7	Cumplimiento de obligaciones relacionadas con la gestión de TI	Cumplimiento parcial alto	Normal
2.1	Planificación de las tecnologías de información	Cumple	Normal
2.2	Modelo de Arquitectura de información	Cumple	Normal
2.3	Infraestructura Tecnológica	Cumple	Normal
2.4	Independencia y recursos humanos de la Función TI	Cumple	Normal
2.5	Administración de recursos financieros	Cumple	Normal
3.1	Consideraciones generales de la implementación de TI	Cumplimiento parcial alto	Normal
3.2	Implementación de Software	Cumplimiento parcial alto	Normal
3.3	Implementación de infraestructura tecnológica	Cumple	Normal
3.4	Contratación de terceros para la implementación y mantenimiento de software e infraestructura	Cumple	Normal
4.1	Definición y administración de acuerdos de servicio	Cumple	Normal
4.2	Administración y operación de la plataforma tecnológica	Cumple	Normal
4.3	Administración de los datos	Cumplimiento parcial alto	Normal
4.4	Atención de requerimientos de los usuarios de TI	Cumple	Normal
4.5	Manejo de incidentes	Cumple	Normal
4.6	Administración de servicios prestados por terceros	Cumple	Normal
5.1	Seguimiento de los procesos de TI	Cumple	Normal
5.2	Seguimiento y evaluación del control interno en TI	Cumple	Normal
5.3	Participación de la Auditoría Interna	Cumple	Normal

Normas Técnicas de la Contraloría General de la Republica

Gráfico resumen con la evaluación obtenida y la metodología aplicada.

Contraloría			
Capítulo		Cumplimiento	% Esperado
I	NORMAS DE APLICACIÓN GENERAL	42.65%	48.53%
II	PLANIFICACIÓN Y ORGANIZACIÓN	8.82%	8.82%
III	IMPLEMENTACIÓN DE TECNOLOGIAS DE INFORMACION	13.24%	14.71%
IV	PRESTACION DE SERVICIOS Y MANTENIMIENTO	18.63%	19.12%
V	SEGUIMIENTO	8.82%	8.82%
ESTADO GENERAL		92.16%	100.00%



Capítulo I Normas de aplicación general

Ref.	Oportunidades de mejora	Nivel de cumplimiento	Impacto	Frecuencia	Categoría de riesgo
IX.1	Normativa sobre reglas en las direcciones de correo electrónico	Cumplimiento parcial bajo	Serio	Frecuente	Elevado
IX.2	Saltos en los consecutivos y duplicados en SICOF	Cumplimiento parcial bajo	Serio	Frecuente	Elevado

Capítulo III Implementación de tecnologías de información

Ref.	Oportunidades de mejora	Nivel de cumplimiento	Impacto	Frecuencia	Categoría de riesgo
IX.3	Actualización de manuales para la funcionalidad y operatividad de los sistemas	Cumplimiento parcial alto	Moderado	Frecuente	Normal

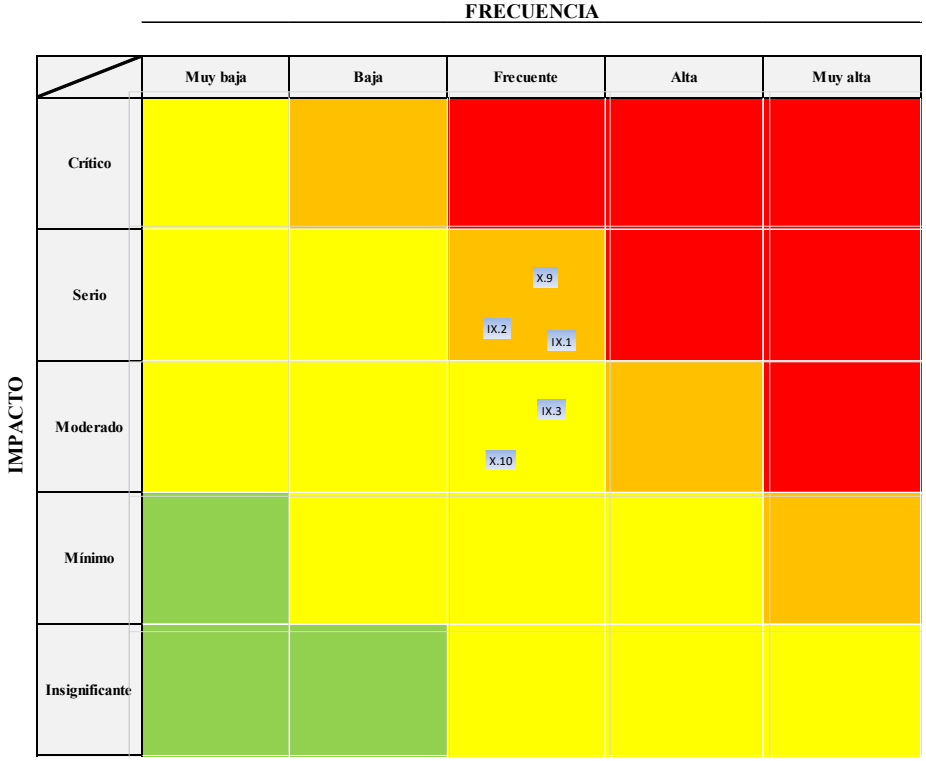
Seguimiento de las recomendaciones de periodo anteriores

Se encuentran en proceso de atención los siguientes 2 hallazgos:

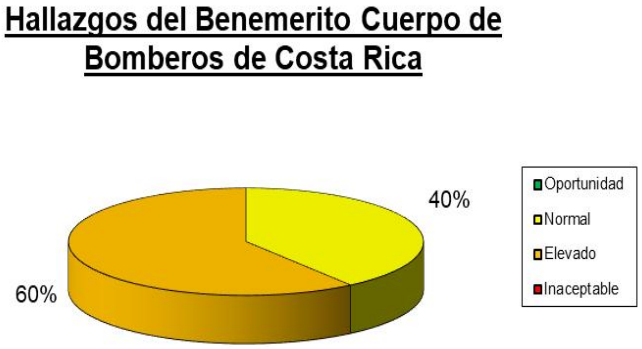
Año	Ref.	Oportunidades de mejora	Nivel de cumplimiento	Impacto	Frecuencia	Categoría de riesgo
2019	X.9	IX.1 Actualización y aplicación del proceso de continuidad (1.4.7)	Cumplimiento parcial bajo	Serio	Frecuente	Elevado
2019	X.10	IX.2 Mejorar la gestión para proyectos con metodologías ágiles SCRUM (1.5)	Cumplimiento parcial alto	Moderado	Frecuente	Normal

IX. Mapa de calor de los riesgos evidenciados al cierre de este informe

De acuerdo con nuestra revisión y a la metodología de calificación del nivel de exposición al riesgo, presentamos a continuación la matriz de 25 cuadrantes donde se resume de manera gráfica, las observaciones que incluimos en nuestro informe y su nivel de riesgo.



Mapa de riesgos identificado para las oportunidades de mejora para la Unidad de TIC de periodos anteriores y 2020.



Como resultado del periodo 2020 y las observaciones de seguimiento, se identifican 5 observaciones, se distribuye en un 40% de riesgo normal y un 60% de riesgo elevado, clasificadas en las categorías de riesgo que se encuentran ubicados de la siguiente forma:

- 2 de riesgo normal
- 3 de riesgo elevado

X. Estado de los apartados de la Normas Técnicas de Gestión y Control de las Tecnologías de Información

1.1 Marco estratégico de TI

El jerarca debe traducir sus aspiraciones en materia de TI en prácticas cotidianas de la organización, mediante un proceso continuo de promulgación y divulgación de un marco estratégico constituido por políticas organizacionales que el personal comprenda y con las que esté comprometido.

Situación actual

Se cuenta con un plan estratégico institucional 2019-2023, un plan estratégico de Tecnologías de Información y Comunicación para los periodos 2019-2023 y un PAO para cada periodo, que se encuentran alineados, son evaluados de acuerdo con los objetivos establecidos y aprobados, se comunican a la institución, pero requieren de un proceso de capacitación que garantice el conocimiento y compromiso del marco estratégico en TIC.

Cumplimiento:

Cumple.

Nivel de riesgo:

Normal.

Evidencia de auditoría

1. Requerimientos de información del proceso.
2. Entrevistas con la Unidad de Tecnologías de Información y Comunicación.
3. Cuestionarios aplicados.

1.2 Gestión de la calidad

La organización debe generar los productos y servicios de TI de conformidad con los requerimientos de sus usuarios con base en un enfoque de eficiencia y mejoramiento continuo.

Situación actual

Existe un manual oficial de TIC: “Manual de Políticas de Tecnologías de Información y Comunicación”, en cuyo Capítulo VIII trata sobre el Ámbito de la gestión de la calidad de los servicios de las tecnologías; no obstante, no se ha implementado.

Se cuenta con un “Procedimiento para la Atención de Solicitudes de los Usuarios a la Unidad de Tecnologías de Información y Comunicación”; que se aplica por medio de la herramienta llamada “SUATT”, para la atención de requerimientos.

Existe una metodología para Administración de Proyectos y un estándar de implementación de software y arquitectura llamado "Estándar de implementación software e infraestructura de Tecnologías de Información y Comunicación". Se aplica un procedimiento para la "Administración y Control de Cambios de TI".

Por medio de recurso outsourcing se desarrolla la metodología de calidad y luego la aplicación respectiva.

Cumplimiento:

Cumple.

Nivel de riesgo:

Normal.

Evidencia de auditoría

1. Requerimientos de información del proceso.
2. Entrevistas con la Unidad de Tecnologías de Información y Comunicación.
3. Entrevistas con usuarios finales.

1.3 Gestión de riesgos

La organización debe responder adecuadamente a las amenazas que puedan afectar la gestión de las TI, mediante una gestión continua de riesgos que esté integrada al sistema específico de valoración del riesgo institucional y considere el marco normativo que le resulte aplicable.

Situación actual

Se cuenta con una metodología de gestión de riesgos para el cumplimiento del SEVRI, con fases como: identificación, análisis, valoración, gestión y seguimiento de riesgos. Con evaluaciones internas y externas para el cumplimiento de los procedimientos y la metodología.

Es de buena práctica una gestión de riesgos integral en la gestión de proyectos y desarrollo de sistemas.

Cumplimiento:

Cumple.

Nivel de riesgo:

Normal.

Evidencia de auditoría

1. Requerimientos de información del proceso.
2. Entrevistas con la Unidad de Tecnologías de Información y Comunicación.
3. Entrevista con la Unidad de Planificación.
4. Entrevistas con usuarios finales.

1.4 Gestión de la seguridad de la información

La organización debe garantizar, de manera razonable, la confidencialidad, integridad y disponibilidad de la información, lo que implica protegerla contra uso, divulgación o modificación no autorizados, daño o pérdida u otros factores disfuncionales.

Para ello debe documentar e implementar una política de seguridad de la información y los procedimientos correspondientes, asignar los recursos necesarios para lograr los niveles de seguridad requeridos y considerar lo que establece la presente normativa en relación con los siguientes aspectos:

- La implementación de un marco de seguridad de la información.
- El compromiso del personal con la seguridad de la información.
- La seguridad física y ambiental.
- La seguridad en las operaciones y comunicaciones.
- El control de acceso.
- La seguridad en la implementación y mantenimiento de software e infraestructura tecnológica.
- La continuidad de los servicios de TI.

Además, debe establecer las medidas de seguridad relacionadas con:

- El acceso a la información por parte de terceros y la contratación de servicios prestados por éstos.
- El manejo de la documentación.
- La terminación normal de contratos, su rescisión o resolución.
- La salud y seguridad del personal.

Las medidas o mecanismos de protección que se establezcan deben mantener una proporción razonable entre su costo y los riesgos asociados.

Situación actual

Existe un marco normativo de seguridad que se gestiona por medio de la política, procedimientos y estrategia, aspectos como: protección de activos de tecnologías, acceso a esquemas en sistemas de información, acceso a servidores institucionales, gestión de perfiles, accesos, integridad y privilegios, bases de datos, generación y actualización de documentos, sistemas de información, seguridad física. Existe un procedimiento “2-03-04-160, Procedimiento para el Control y Seguimiento de la Seguridad de la Información”, y un procedimiento “2-03-04-157, Procedimiento para la Gestión de Identidad de Accesos” que definen que todos los usuarios están identificados de manera única y tienen derechos de acceso de acuerdo con sus roles en el negocio.

Aun no se ha gestionado la clasificación de la información. Existen autoevaluaciones de periodos 2017, 2018 y 2019 que se encuentran en proceso de atención sobre prácticas de monitoreo e implementación del marco de seguridad. Los resultados de la autoevaluación de 2020 y 2021 se presentaron en julio 2021 y se encuentran en proceso de atención.

Cumplimiento:

Parcial bajo.

Nivel de riesgo:

Elevado.

Evidencia de auditoría

1. Requerimientos de información del proceso.
2. Entrevistas con la Unidad de Tecnologías de Información y Comunicación.
3. Entrevistas con usuarios finales.
4. Encuesta aplicada.
5. Aplicación de pruebas en sistemas

1.4.1 Implementación de un marco de seguridad de la información

La organización debe implementar un marco de seguridad de la información, para lo cual debe:

a) Establecer un marco metodológico que incluya la clasificación de los recursos de TI según su criticidad, la identificación y evaluación de riesgos, la elaboración e implementación de un plan para el establecimiento de medidas de seguridad, la evaluación periódica del impacto de esas medidas y la ejecución de procesos de concienciación y capacitación del personal.

b) Mantener una vigilancia constante sobre todo el marco de seguridad y definir y ejecutar periódicamente acciones para su actualización.

c) Documentar y mantener actualizadas las responsabilidades tanto del personal de la organización como de terceros relacionados.

Situación actual

Se aplican controles de seguridad en el acceso a las instalaciones y existen controles ambientales en el Data Center.

Se cuenta con procedimientos para el Control y Seguimiento de la Seguridad de la Información. Para el seguimiento de los procesos de TI, la Gestión de Identidad de Accesos establece los aspectos para definir e implantar las medidas de seguridad de la información.

Existen oportunidades de mejora para reforzar la clasificación de los activos de la información, la aplicación de un plan de acuerdo con la estrategia sobre la seguridad de la información.

Cumplimiento:

Parcial alto.

Nivel de riesgo:

Normal.

Evidencia de auditoría

1. Requerimientos de información del proceso.
2. Entrevistas con la Unidad de Tecnologías de Información y Comunicación.
3. Entrevistas con usuarios finales.
4. Encuesta aplicada.

1.4.2 Compromiso del personal con la seguridad de la información

El personal de la organización debe conocer y estar comprometido con las regulaciones sobre seguridad y confidencialidad, con el fin de reducir los riesgos de error humano, robo, fraude o uso inadecuado de los recursos de TI.

Para ello, el jerarca, debe:

a) Informar y capacitar a los empleados sobre sus responsabilidades en materia de seguridad, confidencialidad y riesgos asociados con el uso de las TI.
b) Implementar mecanismos para vigilar el debido cumplimiento de dichas responsabilidades.
c) Establecer, cuando corresponda, acuerdos de confidencialidad y medidas de seguridad específicas relacionadas con el manejo de la documentación y rescisión de contratos.

Situación actual

En los planes de trabajo del área de control interno de TI se incluyen actividades de validación de pistas de auditoría, planes de pruebas para el monitoreo del correo, cumplimiento y aplicación de las políticas y procedimientos.

Existen procedimientos para el acceso a los recursos de Tecnologías de Información y Comunicación, que son solicitados por las jefaturas y en los casos requeridos por el área de Recursos Humanos. Se aplican las políticas de Active Directory para la creación de usuarios.

Existen acuerdos de confidencialidad de los empleados mediante la convención colectiva y a los proveedores mediante cláusulas de contratos.
Cumplimiento:

Cumple.

Nivel de riesgo:

Normal.

Evidencia de auditoría

1. Requerimientos de información del proceso.
2. Entrevistas con la Unidad de Tecnologías de Información y Comunicación.
3. Encuesta aplicada.

1.4.3 Seguridad física y ambiental

La organización debe proteger los recursos de TI estableciendo un ambiente físico seguro y controlado, con medidas de protección suficientemente fundamentadas en políticas vigentes y análisis de riesgos.

Como parte de esa protección debe considerar:

a) Los controles de acceso a las instalaciones: seguridad perimetral, mecanismos de control de acceso a recintos o áreas de trabajo, protección de oficinas, separación adecuada de áreas.
b) La ubicación física segura de los recursos de TI.
c) El ingreso y salida de equipos de la organización.
d) El debido control de los servicios de mantenimiento.
e) Los controles para el desecho y reutilización de recursos de TI.
f) La continuidad, seguridad y control del suministro de energía eléctrica, del cableado de datos y de las comunicaciones inalámbricas.
g) El acceso de terceros.
h) Los riesgos asociados con el ambiente.

Situación actual

Al ingresar a las instalaciones administrativas se cuenta con oficiales de seguridad para anunciar el ingreso de terceros; se utilizan carne de identificación de visitantes. El Data Center cuenta con controles ambientales adecuados y medidas de protección de acuerdo con los procedimientos.

Existen UPS para mantener el fluido eléctrico en ausencia de energía; se cuenta con una planta eléctrica y su plan de mantenimiento preventivo.

Se cuenta con brigadas y procedimientos para el simulacro y evacuaciones respectivas.

Se utilizan las medidas sanitarias requeridas para el ingreso a las instalaciones y se han actividades periodos de teletrabajo por la COVID, actualmente se aplica el trabajo remoto en ciertos puestos y perfiles.
Cumplimiento:

Cumple.

Nivel de riesgo:

Normal.

Evidencia de auditoría

1. Requerimientos de información del proceso.
2. Entrevistas con la Unidad de Tecnologías de Información y Comunicación.
3. Entrevistas con usuarios finales.

1.4.4 Seguridad en las operaciones y comunicaciones

La organización debe implementar las medidas de seguridad relacionadas con la operación de los recursos de TI y las comunicaciones, minimizar su riesgo de fallas y proteger la integridad del software y de la información.

Para ello debe:

a) Implementar los mecanismos de control que permitan asegurar la no negación, la autenticidad, la integridad y la confidencialidad de las transacciones y de la transferencia o intercambio de información.
b) Establecer procedimientos para proteger la información almacenada en cualquier tipo de medio fijo o removible (papel, cintas, discos, otros medios), incluso los relativos al manejo y desecho de esos medios.
c) Establecer medidas preventivas, detectivas y correctivas con respecto a software "malicioso" o virus.

Situación actual

Existen procedimientos para el uso de medios de almacenamientos de respaldos y recuperaciones y estos son aplicados correctamente en referencia a las Bases de Datos.

El acceso a los sistemas y a la red se ejecuta por medio de autentificación a través de clave y contraseña que debe ser actualizada con regularidad. En los sistemas de información se mantienen bitácoras activas para el rendimiento de cuentas por usuarios en casos requeridos o reconstrucción de transacciones. Se cuenta con antivirus McAfee para la prevención y detección de intrusos de acuerdo con las políticas de configuración.

Se aplican procedimientos de respaldo y restauración de base de datos, traslado y custodia de respaldos institucionales.

Existen mecanismos configurados para la detección de paquetes externos o en la red privada como los firewalls.

Es necesario hacer aplicación de prácticas de ciberseguridad de la información y establecer a nivel institucional el Sistema de Gestión de la Seguridad de la Información según la estrategia de seguridad aprobada en el mes de agosto de 2021. Se está en proceso de atención el plan de acción sobre informe de vulnerabilidades 2019.

Cumplimiento:

Parcial alto.

Nivel de riesgo:

Normal.

Evidencia de auditoría

1. Requerimientos de información del proceso.
2. Entrevistas con la Unidad de Tecnologías de Información y Comunicación.
3. Entrevistas con usuarios finales.
4. Encuesta aplicada.

1.4.5 Control de acceso

La organización debe proteger la información de accesos no autorizados.

Para dicho propósito debe:

a) Establecer un conjunto de políticas, reglas y procedimientos relacionados con el acceso a la información, al software de base y de aplicación, a las bases de datos y a las terminales y otros recursos de comunicación.
b) Clasificar los recursos de TI en forma explícita, formal y uniforme de acuerdo con términos de sensibilidad.
c) Definir la propiedad, custodia y responsabilidad sobre los recursos de TI.
d) Establecer procedimientos para la definición de perfiles, roles y niveles de privilegio, y para la identificación y autenticación para el acceso a la información, tanto para usuarios como para recursos de TI.
e) Asignar los derechos de acceso a los usuarios de los recursos de TI, de conformidad con las políticas de la organización bajo el principio de necesidad de saber o menor privilegio. Los propietarios de la información son responsables de definir quiénes tienen acceso a la información y con qué limitaciones o restricciones.
f) Implementar el uso y control de medios de autenticación (identificación de usuario, contraseñas y otros medios) que permitan identificar y responsabilizar a quienes utilizan los recursos de TI. Ello debe acompañarse de un procedimiento que contemple la requisición, aprobación, establecimiento, suspensión y desactivación de tales medios de autenticación, así como para su revisión y actualización periódica y atención de usos irregulares.
g) Establecer controles de acceso a la información impresa, visible en pantallas o almacenada en medios físicos y proteger adecuadamente dichos medios.
h) Establecer los mecanismos necesarios (pistas de auditoría) que permitan un adecuado y periódico seguimiento al acceso a las TI.
i) Manejar de manera restringida y controlada la información sobre la seguridad de las TI.

Situación actual

Se aplican procedimientos de control establecidos en la normativa interna de acatamiento institucional, para el acceso a la información, software de base de datos y de aplicación. Se ejecuta una administración de contraseñas junto con la creación de usuarios por medio del Active Directory.

Existen procedimientos para otorgar accesos y eliminar o modificar los permisos de los usuarios a los recursos de Tecnologías de Información y Comunicación, los accesos a la información cuentan con los controles requeridos para su gestión, respaldo y restricción.

Cumplimiento:

Cumple.

Nivel de riesgo:

Normal.

Evidencia de auditoría

1. Requerimientos de información del proceso.
2. Entrevistas con la Unidad de Tecnologías de Información y Comunicación.
3. Entrevistas con usuarios finales.
4. Encuesta aplicada.

1.4.6 Seguridad en la implementación y mantenimiento de software e infraestructura tecnológica

La organización debe mantener la integridad de los procesos de implementación y mantenimiento de software e infraestructura tecnológica y evitar el acceso no autorizado, daño o pérdida de información.

Para ello debe:

a) Definir previamente los requerimientos de seguridad que deben ser considerados en la implementación y mantenimiento de software e infraestructura.
b) Contar con procedimientos claramente definidos para el mantenimiento y puesta en producción del software e infraestructura.
c) Mantener un acceso restringido y los controles necesarios sobre los ambientes de desarrollo, mantenimiento y producción.
d) Controlar el acceso a los programas fuente y a los datos de prueba.

Situación actual

Existe un "Estándar de implementación de software e infraestructura de TIC" que define los requerimientos en el mantenimiento y puesta en producción del software e infraestructura.

Se aplican controles en la implementación y mantenimiento de software, se gestionan los requerimientos por medio del SUATT, se cuenta con ambientes separados para el desarrollo y pruebas de los sistemas en producción. Se requiere reforzar por medio de la metodología el aseguramiento de la calidad para recibir los entregables y ponerlos en producción de acuerdo con lo diseñado.

Se cuenta con un plan de infraestructura tecnológica para el periodo 2020.

Existe un repositorio de fuentes que por medio del procedimiento gestiona el acceso a los programas fuentes, datos de prueba y versionamiento.

X.1 Normativa sobre reglas en las direcciones de correo electrónico

Condición

Se cuenta con el procedimiento "2-03-04-015 Gestión de Usuarios de Correo Electrónico" en donde se identifican los pasos para inactivar o eliminar usuarios de correo electrónico. Existe el "procedimiento para la Gestión de Identidad de Accesos", el cual establece el área, los pasos y la herramienta a ser utilizada (SUATT) para inactivar accesos de los usuarios por diversas razones indicadas en el procedimiento.

Se identifica el siguiente evento:

1. Por jubilación el Señor Bermudez deja el puesto de Auditor Interno, por medio de los mecanismos de control interno y el SUATT 9213-2020 inactivan correo electrónico y eliminan accesos a sistemas.
2. Mediante oficio CBCR-047352-2020-DGB-01737, se nombra al señor Marco Antonio Bermúdez Alvarado como Bombero Voluntario Adscrito a la Dirección General el 26 de noviembre de 2020.
3. Debido al nombramiento se restable la contraseña y se habilita la misma dirección de correo electrónico (MBermudez@bomberos.go.cr)
4. En el mes de junio 2021 se identifican 2 correos enviados al ex auditor, que no correspondía a una tarea como Bombero Voluntario Adscrito, debido a la utilización de la misma cuenta de correo electrónico.
5. En el SUATT 4489-2021 se solicita inhabilitar y eliminar la cuenta denominada mbermudez@bomberos.go.cr y crear nueva dirección electrónica con una denominación distinta, pero con el mismo dominio.
6. La cuenta asignada fue mabermudeza@bomberos.go.cr y la anterior se encuentra inhabilitada de acuerdo con la verificación del 26/08/2021.

Se evidencia la falta de normativa para la gestión de las reglas en la formulación de las direcciones de correo electrónico, con el fin minimizar el impacto en el envío de información a personas fuera de la institución o que no desempeñen los puestos de trabajo.

Causa

No se cuenta con un procedimiento o normativa aprobada para la gestión de las reglas en las direcciones de correo institucional.

Efecto

Visibilidad de información confidencial e institucional a un exempleado por jubilación o renuncia al recibir correos por haberse habilitado el mismo correo electrónico.

Recomendación

Documentar y aprobar un estándar con reglas de las direcciones electrónicas que se aplican en la práctica. Se consideren e identifiquen aspectos como los siguientes de acuerdo con la información sensible que se puede incorporar en los correos:

a) habilitar correos a exfuncionarios que se incorporan como bomberos voluntarios.
b) traslado de bomberos voluntarios a fijos o viceversa en caso de existir información que no se comparta o reciba.

X.2 Saltos en los consecutivos y duplicados en SICOF

Condición

En la revisión del Sistema de Correspondencia Oficial (SICOF) se evidencia por medio de la extracción en la base de datos por el personal del área de TI saltos en consecutivos y duplicados en la numeración institucional y por dependencias para el periodo 2020 y 7 meses del periodo 2021.

Se incorporan recortes de la revisión efectuada para 2020 y 2021 la totalidad de errores o inconsistencias se encuentra identificada en la prueba respectiva.

Se detectaron 2415 registros duplicados en el 2020 de acuerdo con la secuencia revisada:

Codigo global	Codigo institucional	Dependencia	Consecutivo Dependencia	Codigo institucional	OriginalRow	DupSequence
CBCR-031835-2020-OPB-01400	031835	OPB-	1400	31835	437	2
CBCR-031835-2020-OPB-01400	031835	OPB-	1400	31835	438	2
CBCR-031835-2020-OPB-01400	031835	OPB-	1400	31835	439	2
CBCR-031835-2020-OPB-01400	031835	OPB-	1400	31835	440	2
CBCR-032420-2020-OPB-01425	032420	OPB-	1425	32420	1,000	3
CBCR-032420-2020-OPB-01425	032420	OPB-	1425	32420	1,001	3
CBCR-032420-2020-OPB-01425	032420	OPB-	1425	32420	1,002	3
CBCR-032420-2020-OPB-01425	032420	OPB-	1425	32420	1,003	3
CBCR-032420-2020-OPB-01425	032420	OPB-	1425	32420	1,004	3
CBCR-032420-2020-OPB-01425	032420	OPB-	1425	32420	1,005	3
CBCR-032649-2020-OPB-01440	032649	OPB-	1440	32649	1,228	4
CBCR-032649-2020-OPB-01440	032649	OPB-	1440	32649	1,229	4
CBCR-032708-2020-OPB-01444	032708	OPB-	1444	32708	1,282	5
CBCR-032708-2020-OPB-01444	032708	OPB-	1444	32708	1,283	5
CBCR-032872-2020-OPB-01451	032872	OPB-	1451	32872	1,441	6
CBCR-032872-2020-OPB-01451	032872	OPB-	1451	32872	1,442	6

Se identifican 1192 códigos faltantes para el período 2020, según la secuencia (31450 hasta 51998):

Resultado	Secuencia Global
2 items missing	Items: 31494 - 31495
2 items missing	Items: 31497 - 31498
1 item missing	Item: 31502
1 item missing	Item: 31511
1 item missing	Item: 31519
1 item missing	Item: 31531
1 item missing	Item: 31571
1 item missing	Item: 31587
1 item missing	Item: 31601
1 item missing	Item: 31604
1 item missing	Item: 31637
1 item missing	Item: 31660
1 item missing	Item: 31674
6 items missing	Items: 31686 - 31691
1 item missing	Item: 31703
3 items missing	Items: 31705 - 31707
1 item missing	Item: 31718
2 items missing	Items: 31734 - 31735
1 item missing	Item: 31738
1 item missing	Item: 31756
2 items missing	Items: 31801 - 31802
1 item missing	Item: 31815

1192 missing items found

Se detectaron 2744 registros duplicados en el 2021 de acuerdo con la secuencia revisada de la uno a la 33.147:

Codigo global	Codigo institucional	Dependencia	Consecutivo Dependencia	Codigo institucional	OriginalRow	DupSequence
CBCR-001375-2021-DGB-00160	001375	DGB-	0160	1375	1,191	3
CBCR-001375-2021-DGB-00160	001375	DGB-	0160	1375	1,192	3
CBCR-001375-2021-DGB-00160	001375	DGB-	0160	1375	1,193	3
CBCR-001375-2021-DGB-00160	001375	DGB-	0160	1375	1,194	3
CBCR-001554-2021-ANB-00018	001554	ANB-	0018	1554	1,361	4
CBCR-001554-2021-ANB-00018	001554	ANB-	0018	1554	1,362	4
CBCR-001599-2021-222-00020	001599	222-	0020	1599	1,391	5
CBCR-001599-2021-222-00020	001599	222-	0020	1599	1,392	5
CBCR-001828-2021-DGB-00218	001828	DGB-	0218	1828	1,589	6
CBCR-001828-2021-DGB-00218	001828	DGB-	0218	1828	1,590	6
CBCR-001828-2021-DGB-00218	001828	DGB-	0218	1828	1,591	6
CBCR-001857-2021-DOB-00020	001857	DOB-	0020	1857	1,614	7
CBCR-001857-2021-DOB-00020	001857	DOB-	0020	1857	1,615	7
CBCR-001857-2021-DOB-00020	001857	DOB-	0020	1857	1,616	7
CBCR-001894-2021-SIB-00001	001894	SIB-	0001	1894	1,651	8
CBCR-001894-2021-SIB-00001	001894	SIB-	0001	1894	1,652	8
CBCR-001894-2021-SIB-00001	001894	SIB-	0001	1894	1,653	8
CBCR-001894-2021-SIB-00001	001894	SIB-	0001	1894	1,654	8
CBCR-001894-2021-SIB-00001	001894	SIB-	0001	1894	1,655	8
CBCR-001894-2021-SIB-00001	001894	SIB-	0001	1894	1,656	8

Se identifican 2043 códigos faltantes para el período 2021, según la secuencia (1 hasta 33147):

Resultado	Secuencia Global
1 item missing	Item: 225
1 item missing	Item: 227
3 items missing	Items: 244 - 246
2 items missing	Items: 284 - 285
1 item missing	Item: 326
2 items missing	Items: 357 - 358
1 item missing	Item: 392
3 items missing	Items: 443 - 445
2 items missing	Items: 448 - 449
2 items missing	Items: 456 - 457
4 items missing	Items: 459 - 462
2 items missing	Items: 471 - 472
15 items missing	Items: 474 - 488
6 items missing	Items: 496 - 501
6 items missing	Items: 504 - 509
2 items missing	Items: 516 - 517
1 item missing	Item: 527
2 items missing	Items: 532 - 533
4 items missing	Items: 535 - 538
19 items missing	Items: 540 - 558
4 items missing	Items: 563 - 566

2043 missing items found

Causas

No se cuenta con otros mecanismos de verificación como reporte o bitácora para verificar lo que sucede con los saltos y duplicados institucionales y por dependencias.

Existe en proceso de atención vulnerabilidades del estudio de vulnerabilidad del 2020 sobre debilidades en las configuraciones en equipos críticos como firewalls en donde por el lenguaje de programación y versión de software da conflictos hacia el Active Directory, tiempo (latencia) de respaldo en el servidor sobre los datos del SICOF y la configuración del “Master Key Passphrase”.

Con el lenguaje de programación del SICOF actual (JAVA) no se ha logrado subsanar aspectos de configuración y seguridad, sería oportuno considerar otro lenguaje para atender las debilidades identificadas.

Efectos

Podría ser utilizada numeración duplicada para diferentes envíos de oficios entre dependencias.

No permite garantizar la omisión de oficios que son emitidos por las distintas dependencias de la Institución.

No se puede validar los saltos a nivel de la base de datos al no existir bitácora que guarde los consecutivos no utilizados por las dependencias de acuerdo con la revisión y las pruebas realizadas con el dueño del sistema y el líder técnico.

Pérdida de credibilidad en la asignación numérica automatizada.

Recomendaciones

Evaluar la lógica del sistema donde se asigna el consecutivo y documentar en una bitácora los números duplicados y faltantes en un registro para ser revisados.

Identificar por medio de un análisis de causa raíz la anomalía identificada en SICOF para que los tomadores de decisión evalúan el riesgo y se logren acciones de atención al sistema por el riesgo operativo y de seguridad que se está materializando.

Comentario de la administración

De parte de la Administración se acota que la situación del SICOF se conoce desde el año 2019, y desde entonces se ha invertido en tratar de identificar la causa raíz del problema que se ocasiona las situaciones que reporta el presente informe, al respecto se conoce que en primera instancia el SICOF no duplica consecutivos, lo que duplica son registros del mismo correo que se genera, por lo que tanto el consecutivo como el contenido del mismo, así como sus remitentes y destinatarios son los mismos.

Por otra parte, se presenta el “salto” de consecutivos, en ambas condiciones se llegó a la conclusión a inicios del 2021 de que las situaciones no corresponden a un problema en el código fuente de la herramienta, sino más bien a una situación de incompatibilidad en las versiones de los sistemas que soportan el sistema SICOF, ya que el sistema fue desarrollado hacia el 2013 en un lenguaje JAVA, específicamente en el servidor Glassfish sobre Windows Server, lo cual está ocasionando una “delay” o tiempo de desconexión.

Producto de lo anterior, ya la Administración optó por desarrollar una nueva versión del SICOF que no requiera el uso del Glassfish, y que en su lugar se recurra a un servidor IIS (Internet Information Server, por sus siglas en inglés) de Windows, a fin de evitar los inconvenientes que se manifiestan.

Cumplimiento:

Parcial bajo.

Nivel de riesgo:

Elevado.

Evidencia de auditoría

1. Requerimientos de información del proceso.
2. Entrevistas con la Unidad de Tecnologías de Información y Comunicación.
3. Entrevista con la Auditoría Interna.
4. Entrevistas con usuarios finales.
5. Prueba en sistema de información.

1.4.7 Continuidad de los servicios de TI

La organización debe mantener una continuidad razonable de sus procesos y su interrupción no debe afectar significativamente a sus usuarios.

Como parte de ese esfuerzo se deben documentar y poner en práctica, en forma efectiva y oportuna, las acciones preventivas y correctivas necesarias con base en los planes de mediano y largo plazo de la organización, la evaluación e impacto de los riesgos y la clasificación de sus recursos de TI según su criticidad.

Se cuenta con controles y procedimientos para la atención de interrupciones, sin llevar a cabo un plan de pruebas que a la fecha han minimizado la probabilidad y el impacto de interrupciones mayores en los servicios de TI, a pesar de que en la sección de evaluación de sistemas se hace referencia a las debilidades y riesgos de no haber aplicado escenarios de pruebas para la continuidad de operaciones como se indica en el proceso de la confección de planillas.

Se aplican procedimientos de redundancia, respaldos y pruebas de restauración de datos. En la sección de seguimiento se encuentran observaciones en proceso de atención.

Cumplimiento:

Parcial bajo.

Nivel de riesgo:

Elevado.

Evidencia de auditoría

1. Requerimientos de información del proceso y su análisis.
2. Entrevistas con la Unidad de Planificación.
3. Entrevistas con usuarios de áreas de negocio.

1.5 Gestión de proyectos

La organización debe administrar sus proyectos de TI de manera que logre sus objetivos, satisfaga los requerimientos y cumpla con los términos de calidad, tiempo y presupuesto óptimos preestablecidos.

Situación actual

Se cuenta con una metodología para la administración de proyectos; estos se encuentran alineados a los objetivos estratégicos del Plan Estratégico de Tecnologías de Información y Comunicación. Por medio del portafolio se gestionan y se trabaja en ellos a través de los Planes Operativos Institucionales.

Se han presentado desfaces en el cumplimiento de los proyectos que han sido reprogramados e informados a la Administración.

Es necesario claridad en los criterios para la ejecución del guion de pruebas y aplicar la metodología de proyectos de TIC y cumplir con los tiempos y calidad requerida.

De acuerdo con el informe de autoevaluación de control interno 2020-2021 emitido en julio 2021 se evidencia debilidades relaciones con la gestión de proyectos, donde recomendamos dar seguimiento con el fin de minimizar la exposición al riesgo operativo, la observación es: “1.5 - 2021. Debilidades entorno a la implementación de Gestión de Proyectos”.

En la sección de seguimiento se encuentran observaciones en proceso de atención.

Cumplimiento:

Parcial alto.

Nivel de riesgo:

Normal.

Evidencia de auditoría

1. Requerimientos de información del proceso.
2. Entrevistas con la Unidad de Tecnologías de Información y Comunicación.
3. Entrevistas con usuarios finales.

1.6 Decisiones sobre asuntos estratégicos de TI

El jerarca debe apoyar sus decisiones sobre asuntos estratégicos de TI en la asesoría de una representación razonable de la organización que coadyuve a mantener la concordancia con la estrategia institucional, a establecer las prioridades de los proyectos de TI, a lograr un equilibrio en la asignación de recursos y a la adecuada atención de los requerimientos de todas las unidades de la organización.

Situación actual

Se encuentran formalizadas las actividades por medio del procedimiento para "Decisiones sobre Asuntos Estratégicos de TI", que se encuentra implementado. El plan estratégico de TI se encuentra alineado al plan estratégico institucional.

Existe un Comité de Tecnología formalmente establecido. Se encuentran los canales de comunicación formalizados entre la jefatura de TI y las Gerencias de la institución.

De acuerdo con el informe de autoevaluación de control interno 2020-2021 emitido en julio 2021, se evidencia debilidades entorno con las decisiones sobre asuntos estratégicos, debido a la no ejecución de los planes que podrían impedir el logro de objetivos; a fin de evaluar oportunamente el impacto en el presupuesto, recursos, entrega de capacidades y beneficios de TI para orientar los cambios necesarios oportunamente.

Cumplimiento:

Parcial alto.

Nivel de riesgo:

Normal.

Evidencia de auditoría

1. Requerimientos de información del proceso.
2. Entrevistas con la Unidad de Tecnologías de Información y Comunicación.
3. Entrevistas con usuarios finales.

1.7 Cumplimiento de obligaciones relacionadas con la gestión de TI

La organización debe identificar y velar por el cumplimiento del marco jurídico que tiene incidencia sobre la gestión de TI con el propósito de evitar posibles conflictos legales que pudieran ocasionar eventuales perjuicios económicos y de otra naturaleza.

Situación actual

Se cuenta con la "Política 6. Cumplimiento de Obligaciones Relacionadas con la Gestión de TI" y el procedimiento "2-03-04-162, Procedimiento para el Cumplimiento de las Obligaciones Relacionadas con la Gestión de TI".

Se llevan a cabo revisiones internas y externas de los sistemas de información, procesos, infraestructura tecnológica, proyectos, metodologías, procedimientos y cumplimiento del marco normativo. Existen seguimientos de las recomendaciones en proceso de atención.

De los informes de autoevaluación interna de TI, de los periodos 2017 al 2020 se encuentran entre algunas acciones sin atender las siguientes:

- ✓ Pruebas de continuidad.
- ✓ Clasificación de los activos de TI.
- ✓ Gestión de proyectos.
- ✓ Decisiones estratégicas sobre cumplimiento de los planes (PAO, PETIC).

Cumplimiento:

Parcial alto.

Nivel de riesgo:

Normal.

Evidencia de auditoría

1. Requerimientos de información del proceso.
2. Entrevistas con la Unidad de Tecnologías de Información y Comunicación.
3. Entrevistas con usuarios finales.

2.1 Planificación de las tecnologías de información

La organización debe lograr que las TI apoyen su misión, visión y objetivos estratégicos mediante procesos de planificación que logren el balance óptimo entre sus requerimientos, su capacidad presupuestaria y las oportunidades que brindan las tecnologías existentes y emergentes.

Situación actual

De acuerdo con el presupuesto aprobado para Tecnologías de Información y Comunicación se distribuye y organiza sus planes, mediante una planificación de acuerdo con los recursos y metas del PAO (Plan Anual Operativo). Se han presentado desfaces en el cumplimiento de los proyectos que están alineados a los objetivos del PAO.

TIC cuenta con un presupuesto que responde a las metas y acciones alineadas a los planes operativos. El presupuesto cuenta con contenido presupuestario definido por devengo que garantiza la ejecución de los proyectos de TIC, de los cuales se han presentado atrasos e incumplimientos de finalización de proyectos a pesar de los esfuerzos internos; hay carencia de personal con perfiles profesionales para la gestión de proyectos, gestión de la seguridad y gestión de la Calidad (QA).

A lo interno se han reforzado los procedimientos de cambios, riesgos y control de los desarrollos de sistemas de información.

Cumplimiento:

Cumple

Nivel de riesgo:

Normal.

Evidencia de auditoría

1. Requerimientos de información del proceso.
2. Entrevistas con la Unidad de Tecnologías de Información y Comunicación.
3. Entrevistas con usuarios finales.

2.2 Modelo de arquitectura de información

La organización debe optimizar la integración, uso y estandarización de sus sistemas de información de manera que se identifique, capture y comunique, en forma completa, exacta y oportuna, sólo la información que sus procesos requieren.

Situación actual

El modelo de arquitectura se encuentra compuesto por:

- ✓ Política 17, Definición del Modelo de Arquitectura y Estandarización de TI.
- ✓ 2-03-04-164, Procedimiento para Definición de Estándares de los Sistemas de Información de TI.
- ✓ 2-03-04-188, Estándar de implementación de software e infraestructura de TIC.
- ✓ 2-03-04-185, Estándares de Seguridad en la Información.
- ✓ 2-03-04-186, Estándar de clasificación de la documentación.
- ✓ 2-03-04-189, Estándar de Base de Datos.
- ✓ 2-03-04-200, Estándar de Programación.

Se atienden los desarrollos y mantenimiento a los sistemas por medio de proveedores externos. Es necesario valorar prácticas y actividades de aseguramiento de la calidad cuando se inicie el desarrollo de los módulos del EXCELSIOR.

Se cuenta con un plan de infraestructura para la configuración y estandarización de la plataforma tecnológica.

Cumplimiento:

Cumple.

Nivel de riesgo:

Normal.

Evidencia de auditoría

1. Requerimientos de información del proceso.
2. Entrevistas con la Unidad de Tecnologías de Información y Comunicación.
3. Entrevistas con usuarios finales.

2.3 Infraestructura tecnológica

La organización debe tener una perspectiva clara de su dirección y condiciones en materia tecnológica, así como de la tendencia de las TI para optimizar el uso de su infraestructura tecnológica, manteniendo el equilibrio entre sus requerimientos y la dinámica y evolución de las TI.

Situación actual

Existe un proceso de monitoreo sobre la Infraestructura vigente, documentado mediante un Plan de mantenimiento de infraestructura Tecnológica; se ha planeado un conjunto de actividades para asegurar un óptimo uso de los recursos.

Se cuenta con el Plan de Infraestructura que permite definir el crecimiento y actualización de la tecnología acorde a la planeación estratégica, el cual considera aspectos de componentes de la infraestructura (almacenamiento, bases de datos y sistemas), así como orientación para la adquisición.

Cumplimiento:

Cumple.

Nivel de riesgo:

Normal.

Evidencia de auditoría

1. Requerimientos de información del proceso.
2. Entrevistas con la Unidad de Tecnologías de Información y Comunicación.
3. Entrevistas con usuarios finales.
4. Cuestionarios aplicados.

2.4 Independencia y recurso humano de la función de TI

El jerarca debe asegurar la independencia de la función de TI respecto de las áreas usuarias y que ésta mantenga la coordinación y comunicación con las demás dependencias tanto internas y externas.

Además, debe brindar el apoyo necesario para que dicha Función de TI cuente con una fuerza de trabajo motivada, suficiente, competente y a la que se le haya definido, de manera clara y formal, su responsabilidad, autoridad y funciones.

Situación actual

Se cuenta con un organigrama del área de TI que apoya la comunicación entre las áreas de acuerdo con los programas y sus funciones. Se trabaja en función del PAO y los planes tácticos para cumplir con el Plan Estratégico de Tecnologías de Información y Comunicación y estar alineados al Plan Estratégico Institucional.

Se cuenta con un Plan de Gestión de recurso humano en Tecnologías de Información y Comunicación, que considera un plan de capacitación, un plan de sucesión, evaluaciones de desempeño, entre otros.

Cumplimiento:

Cumple.

Nivel de riesgo:

Normal.

Evidencia de auditoría

1. Requerimientos de información del proceso.
2. Entrevistas con la Unidad de Tecnologías de Información y Comunicación.
3. Entrevistas con usuarios finales.
4. Cuestionarios aplicados.

2.5 Administración de recursos financieros

La organización debe optimizar el uso de los recursos financieros invertidos en la gestión de TI procurando el logro de los objetivos de esa inversión, controlando en forma efectiva dichos recursos y observando el marco jurídico que al efecto le resulte aplicable.

Situación actual

Por medio de la aprobación del presupuesto anual, se administran las inversiones, compras, renovaciones, proyectos, recursos para TI de acuerdo con las metas institucionales del PAO y a las evaluaciones respectivas. En Tecnologías de Información y Comunicación se lleva control del presupuesto disponible versus el consumido.

Se cuenta con el procedimiento “2-03-04-168, Procedimiento para la Administración de Recursos Financieros Tecnologías de Información y Comunicación”.

Cumplimiento:

Cumple.

Nivel de riesgo:

Normal.

Evidencia de auditoría

1. Requerimientos de información del proceso.
2. Entrevistas con la Unidad de Tecnologías de Información y Comunicación.
3. Entrevistas con usuarios finales.

3.1 Consideraciones generales de la implementación de TI

La organización debe implementar y mantener las TI requeridas en concordancia con su marco estratégico, planificación, modelo de arquitectura de información e infraestructura tecnológica.

Para esa implementación y mantenimiento debe:

a) Adoptar políticas sobre la justificación, autorización y documentación de solicitudes de implementación o mantenimiento de TI.
b) Establecer el respaldo claro y explícito para los proyectos de TI tanto del jerarca como de las áreas usuarias.
c) Garantizar la participación de las unidades o áreas usuarias, las cuales deben tener una asignación clara de responsabilidades y aprobar formalmente las implementaciones realizadas.
d) Instaurar líderes de proyecto con una asignación clara, detallada y documentada de su autoridad y responsabilidad.
e) Analizar alternativas de solución de acuerdo con criterios técnicos, económicos, operativos y jurídicos, y lineamientos previamente establecidos.
f) Contar con una definición clara, completa y oportuna de los requerimientos, como parte de los cuales debe incorporar aspectos de control, seguridad y auditoría bajo un contexto de costo – beneficio.
g) Tomar las previsiones correspondientes para garantizar la disponibilidad de los recursos económicos, técnicos y humanos requeridos.
h) Formular y ejecutar estrategias de implementación que incluyan todas las medidas para minimizar el riesgo de que los proyectos no logren sus objetivos, no satisfagan los requerimientos o no cumplan con los términos de tiempo y costo preestablecidos.
i) Promover su independencia de proveedores de hardware, software, instalaciones y servicios.

Situación actual

Se cuenta con procedimientos, políticas, herramientas y sistemas de información para el mantenimiento y atención de solicitudes de los usuarios por medio del sistema SUATT.

Se cuenta con un estándar de implementación de software e infraestructura “2-03-04-188, Estándar de implementación de software e infraestructura de Tecnologías de Información y Comunicación”, que establece pautas en concordancia con los requerimientos vigentes en materia de infraestructura y software.

En la gestión de proveedores, infraestructura y servicios se aplican mecanismos de control de contratación administrativa, fiscalización de contratos, cumplimiento de soporte o mantenimiento del software.

Se requiere gestionar e implementar la calidad del software y adicionalmente validar la aplicación de la metodología Scrum aplicada por el proveedor en el desarrollo de sistemas y requerimientos que se reciben, aunado a las pruebas que son ejecutadas a lo interno. Existen oportunidades de mejora en proceso de atención.

Cumplimiento:

Parcial alto.

Nivel de riesgo:

Normal.

Evidencia de auditoría

1. Requerimientos de información del proceso.
2. Entrevistas con la Unidad de Tecnologías de Información y Comunicación.
3. Entrevistas con usuarios finales.

3.2 Implementación de software

La organización debe implementar el software que satisfaga los requerimientos de sus usuarios y soporte efectivamente sus procesos, para lo cual debe:

a) Observar lo que resulte aplicable de la norma 3.1 anterior.
b) Desarrollar y aplicar un marco metodológico que guíe los procesos de implementación y considere la definición de requerimientos, los estudios de factibilidad, la elaboración de diseños, la programación y pruebas, el desarrollo de la documentación, la conversión de datos y la puesta en producción, así como también la evaluación post-implantación de la satisfacción de los requerimientos.
c) Establecer los controles y asignar las funciones, responsabilidades y permisos de acceso al personal a cargo de las labores de implementación y mantenimiento de software.
d) Controlar la implementación del software en el ambiente de producción y garantizar la integridad de datos y programas en los procesos de conversión y migración.
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.
f) Controlar las distintas versiones de los programas que se generen, como parte de su mantenimiento.

Situación actual

En el estándar de implementación de software e infraestructura de Tecnologías de Información y Comunicación, se establecen los lineamientos en la implementación: levantamiento de requerimientos, condiciones generales de desarrollo de sistemas de información, estudio de factibilidad, especificación de casos de uso, plan de pruebas, resultado de pruebas, entre otros.

Existen responsables de repositorio "2-03-04-159 Procedimiento para el Acceso a los Programas Fuentes y Datos de Pruebas". La gestión de cambios se canaliza mediante el SUATT estableciendo el responsable del cambio.

En la migración de datos e información, se aplican los procedimientos: "2-03-04-171, Procedimiento para la Elaboración del Plan de Migración de Datos" y "2-03-04-170, Procedimiento para la Migración de Datos de Sistemas de Información".

X.3 Actualización de manuales para la funcionalidad y operatividad de los sistemas

Condición

Se evidencia la ausencia de un control como por ejemplo matriz o reporte para validar la actualización de los manuales técnicos o de base datos para los sistemas de información de información bajo estudio.

Causa

Ausencia de una matriz integral con la versión y fecha de la última actualización requerida para los manuales de los sistemas de información; se debe ingresar a la carpeta de cada sistema y verificar si se encuentran actualizados contra la atención de requerimientos que pudieron presentar un cambio o mejora en el manual respectivo.

Efecto

Posible demora en tiempo en la toma de decisiones para atender cambios, capacitar a líderes técnicos o proveedores, con mayor probabilidad en ausencia del personal responsable por parte del área de TI para atender los requerimientos a los sistemas de información.

Recomendación

Valorar la confección de un reporte o matriz donde con cierta regularidad se actualicen las fechas y versiones de los manuales respectivos.

<u>Cumplimiento:</u>

Parcial alto.

Nivel de riesgo:

Normal.

Evidencia de auditoría

1. Requerimientos de información del proceso.
2. Entrevistas con la Unidad de Tecnologías de Información y Comunicación.
3. Entrevistas con usuarios finales.
4. Cuestionarios aplicados.

3.3 Implementación de infraestructura tecnológica

La organización debe adquirir, instalar y actualizar la infraestructura necesaria para soportar el software de conformidad con los modelos de arquitectura de información e infraestructura tecnológica y demás criterios establecidos. Como parte de ello debe considerar lo que resulte aplicable de la norma 3.1 anterior y los ajustes necesarios a la infraestructura actual.

Situación actual

La adquisición de infraestructura tecnológica se encuentra alineada a los planes estratégicos y las partidas presupuestarias de acuerdo con la alineación al Plan de Infraestructura.

La gestión de contratos con terceros se realiza mediante la Ley de Contratación Administrativa y los procedimientos establecidos en lo interno.

Cumplimiento:

Cumple.

Nivel de riesgo:

Normal.

Evidencia de auditoría

1. Requerimientos de información del proceso.
2. Entrevistas con la Unidad de Tecnologías de Información y Comunicación.
3. Entrevistas con usuarios finales.

3.4 Contratación de terceros para la implementación y mantenimiento de software e infraestructura

La organización debe obtener satisfactoriamente el objeto contratado a terceros en procesos de implementación o mantenimiento de software e infraestructura. Para lo anterior, debe:

a) Observar lo que resulte aplicable de las normas 3.1, 3.2 y 3.3 anteriores.
b) Establecer una política relativa a la contratación de productos de software e infraestructura.
c) Contar con la debida justificación para contratar a terceros la implementación y mantenimiento de software e infraestructura tecnológica.
d) Establecer un procedimiento o guía para la definición de los "términos de referencia" que incluyan las especificaciones y requisitos o condiciones requeridas o aplicables, así como para la evaluación de ofertas.
e) Establecer, verificar y aprobar formalmente los criterios, términos y conjunto de pruebas de aceptación de lo contratado, sean instalaciones, hardware o software.
f) Implementar un proceso de transferencia tecnológica que minimice la dependencia de la organización respecto de terceros contratados para la implementación y mantenimiento de software e infraestructura tecnológica.

Situación actual

En la implementación o mantenimiento de software o infraestructura por terceros se mantiene el control desde el inicio del proyecto. De acuerdo con los procedimientos internos, se gestionan, administran y monitorean los términos de los contratos, y se hacen evaluaciones de la calidad del servicio del proveedor.

La gestión de contratos con terceros se realiza mediante la Ley de Contratación Administrativa y los procedimientos establecidos en lo interno.

Cumplimiento:

Cumple.

Nivel de riesgo:

Normal.

Evidencia de auditoría

1. Requerimientos de información del proceso.
2. Entrevistas con la Unidad de Tecnologías de Información y Comunicación.
3. Entrevistas con usuarios finales.

4.1 Definición y administración de acuerdos de servicio

La organización debe tener claridad respecto de los servicios que requiere y sus atributos, y los prestados por la Función de TI según sus capacidades.

El jerarca y la Función de TI deben acordar los servicios requeridos, los ofrecidos y sus atributos, lo cual deben documentar y considerar como un criterio de evaluación del desempeño. Para ello deben:

a) Tener una comprensión común sobre: exactitud, oportunidad, confidencialidad, autenticidad, integridad y disponibilidad.
b) Contar con una determinación clara y completa de los servicios y sus atributos, y analizar su costo y beneficio.
c) Definir con claridad las responsabilidades de las partes y su sujeción a las condiciones establecidas.
d) Establecer los procedimientos para la formalización de los acuerdos y la incorporación de cambios en ellos.
e) Definir los criterios de evaluación sobre el cumplimiento de los acuerdos.
f) Revisar periódicamente los acuerdos de servicio, incluidos los contratos con terceros.

Situación actual

Se ha definido un catálogo de servicios de Tecnologías de Información y Comunicación y se encuentra definido un responsable por parte de TI y otro por parte de la Institución. Existe un procedimiento “2-03-04-174, Procedimiento para la Definición y Administración de Acuerdos de Servicio” para la formalización en la incorporación de servicios.

La oportunidad de mejora del periodo anterior fue atendida.

Cumplimiento:

Cumple.

Nivel de riesgo:

Normal.

Evidencia de auditoría

1. Requerimientos de información del proceso.
2. Entrevistas con la Unidad de Tecnologías de Información y Comunicación.
3. Entrevistas con usuarios finales.

4.2 Administración y operación de la plataforma tecnológica

La organización debe mantener la plataforma tecnológica en óptimas condiciones y minimizar su riesgo de fallas. Para ello debe:

a) Establecer y documentar los procedimientos y las responsabilidades asociadas con la operación de la plataforma.
b) Vigilar de manera constante la disponibilidad, capacidad, desempeño y uso de la plataforma, asegurar su correcta operación y mantener un registro de sus eventuales fallas.
c) Identificar eventuales requerimientos presentes y futuros, establecer planes para su satisfacción y garantizar la oportuna adquisición de recursos de TI requeridos tomando en cuenta la obsolescencia de la plataforma, contingencias, cargas de trabajo y tendencias tecnológicas.
d) Controlar la composición y cambios de la plataforma y mantener un registro actualizado de sus componentes (hardware y software), custodiar adecuadamente las licencias de software y realizar verificaciones físicas periódicas.
e) Controlar la ejecución de los trabajos mediante su programación, supervisión y registro.
f) Mantener separados y controlados los ambientes de desarrollo y producción.
g) Brindar el soporte requerido a los equipos principales y periféricos.
h) Definir formalmente y efectuar rutinas de respaldo, custodiar los medios de respaldo en ambientes adecuados, controlar el acceso a dichos medios y establecer procedimientos de control para los procesos de restauración.
i) Controlar los servicios e instalaciones externos.

Situación actual

Existe un marco para la administración de la infraestructura definido por el procedimiento "2-03-04-175, Procedimiento para el Monitoreo del Desempeño y la Capacidad de la Infraestructura Tecnológica" donde se indican las pautas sobre controles en el proceso de monitoreo a fin de mantener la plataforma tecnológica en óptimas condiciones y minimizar su riesgo de fallas.

Se han establecido políticas y procedimientos "2-03-04-159, Procedimiento para el Acceso a los Programas Fuentes y Datos de Pruebas"," 2-03-04-164, Procedimiento para Definición de Estándares de los Sistemas de Información de TI" y "2-03-04-175, Procedimiento para el Monitoreo del Desempeño y la Capacidad de la Infraestructura Tecnológica", en donde se definen responsables asociados a la operación de la plataforma.

Por medio del Plan de Infraestructura y Plan de Mantenimiento se da soporte y continuidad del proceso a la Administración y Operación de la Plataforma Tecnológica.

Se aplican procedimientos de respaldo y restauración.

Cumplimiento:

Cumple.

Nivel de riesgo:

Normal.

Evidencia de auditoría

1. Requerimientos de información del proceso.
2. Entrevistas con la Unidad de Tecnologías de Información y Comunicación.
3. Entrevistas con usuarios finales.
4. Cuestionarios aplicados.

4.3 Administración de los datos

La organización debe asegurarse que los datos que son procesados mediante TI corresponden a transacciones válidas y debidamente autorizadas, que son procesados en forma completa, exacta y oportuna, y transmitidos, almacenados y desechados en forma íntegra y segura.

Situación actual

Los datos que se procesan cuentan con seguridad y procedimientos en actividades de respaldo, restauración, licenciamiento, pases como los siguientes:

- ✓ Procedimiento de Generación de Respaldos
- ✓ Procedimiento de Restauración de Respaldos de la Base de Datos
- ✓ Procedimiento para el Control de Licenciamiento
- ✓ Procedimiento para Tramitar Solicitudes de Respaldo de Información
- ✓ Procedimiento de Ejecución de pases en Base de Datos

Existe un proceso de revisión de pistas de auditoría, como mecanismo de aseguramiento y gestión de la integridad, seguridad y autenticidad de los registros procesados.

Existe un procedimiento para la clasificación de la información que no se ha implementado.

Cumplimiento:

Parcial alto.

Nivel de riesgo:

Normal.

Evidencia de auditoría

1. Requerimientos de información del proceso.
2. Entrevistas con la Unidad de Tecnologías de Información y Comunicación.
3. Entrevista con la Auditoría Interna.
4. Entrevistas con usuarios finales.

4.4 Atención de requerimientos de los usuarios de TI

La organización debe hacerle fácil al usuario el proceso para solicitar la atención de los requerimientos que le surjan al utilizar las TI. Asimismo, debe atender tales requerimientos de manera eficaz, eficiente y oportuna; y dicha atención debe constituir un mecanismo de aprendizaje que permita minimizar los costos asociados y la recurrencia.

Situación actual

Se cuenta con una mesa de servicio para recibir las solicitudes de los usuarios, que son priorizados de acuerdo con el recurso y tipo de solicitud para ser atendidas por medio del SUATT.

Existe un procedimiento para la Atención de Solicitudes de los Usuarios a la Unidad de Tecnologías de Información y Comunicación, para la atención y el escalamiento requerido.

Cumplimiento:

Cumple.

Nivel de riesgo:

Normal.

Evidencia de auditoría
1. Requerimientos de información del proceso.
2. Entrevistas con la Unidad de Tecnologías de Información y Comunicación.
3. Entrevistas con usuarios finales.
4. Cuestionarios aplicados.

4.5 Manejo de incidentes

La organización debe identificar, analizar y resolver de manera oportuna los problemas, errores e incidentes significativos que se susciten con las TI. Además, debe darles el seguimiento pertinente, minimizar el riesgo de recurrencia y procurar el aprendizaje necesario.

Situación actual

Existe un proceso y procedimiento definido para el registro, atención y análisis de la Administración de Incidentes de TI por medio de la herramienta SUATT.

Cumplimiento:

Cumple.

Nivel de riesgo:

Normal.

Evidencia de auditoría

1. Requerimientos de información del proceso.
2. Entrevistas con la Unidad de Tecnologías de Información y Comunicación.
3. Entrevistas con usuarios finales.
4. Cuestionarios aplicados.

4.6 Administración de servicios prestados por terceros

La organización debe asegurar que los servicios contratados a terceros satisfagan los requerimientos en forma eficiente. Con ese fin, debe:

a) Establecer los roles y responsabilidades de terceros que le brinden servicios de TI.
b) Establecer y documentar los procedimientos asociados con los servicios e instalaciones contratados a terceros.
c) Vigilar que los servicios contratados sean congruentes con las políticas relativas a calidad, seguridad y seguimiento establecidas por la organización.
d) Minimizar la dependencia de la organización respecto de los servicios contratados a un tercero.
e) Asignar a un responsable con las competencias necesarias que evalúe periódicamente la calidad y cumplimiento oportuno de los servicios contratados.

Situación actual

Existe un proceso que monitorea la prestación del servicio, en donde se valida el cumplimiento de los acuerdos del contrato y acuerdos de niveles de servicios (SLA´s). Se aplican los controles en la contratación administración de servicios, productos y sistemas de información.

Se aplican prácticas de control en la confidencialidad de la información con los terceros que se contratan.

Cumplimiento:

Cumple.

Nivel de riesgo:

Normal.

Evidencia de auditoría

1. Requerimientos de información del proceso.
2. Entrevistas con la Unidad de Tecnologías de Información y Comunicación.
3. Entrevistas con usuarios finales.

5.1 Seguimiento de los procesos de TI

La organización debe asegurar el logro de los objetivos propuestos como parte de la gestión de TI, para lo cual debe establecer un marco de referencia y un proceso de seguimiento en los que defina el alcance, la metodología y los mecanismos para vigilar la gestión de TI. Asimismo, debe determinar las responsabilidades del personal a cargo de dicho proceso.

Situación actual

Se cuenta con un procedimiento de control interno de TI, del cual se confecciona un cronograma de trabajo y se ejecutaron las evaluaciones. Existen planes de acción que atender las autoevaluaciones internas.

En apoyo a la gestión de Tecnologías de Información y Comunicación, existe la Política 5, "Seguimiento y Control Interno" y el procedimiento "2-03-04-180, Procedimiento para el Seguimiento de los Procesos de TI", que establecen un marco de referencia y un proceso de seguimiento como mecanismos para monitorear la gestión de TI.

Se ha definido el personal responsable de la ejecución al plan de trabajo, se ha comunicado la brecha para el cumplimiento con el ente regulador e identificado recomendaciones atendidas y otras en proceso de atención.

Cumplimiento:

Cumple.

Nivel de riesgo:

Normal.

Evidencia de auditoría

1. Requerimientos de información del proceso.
2. Entrevistas con la Unidad de Tecnologías de Información y Comunicación.
3. Entrevistas con usuarios finales.

5.2 Seguimiento y evaluación del control interno en TI

El jerarca debe establecer y mantener el sistema de control interno asociado con la gestión de las TI, evaluar su efectividad y cumplimiento y mantener un registro de las excepciones que se presenten y de las medidas correctivas implementadas.

Situación actual

Se hace seguimiento al control interno de TI, por medio del plan de trabajo establecido a lo interno y las auditorías de TI externas, de las cuales se emiten planes de acción para atender los hallazgos internamente, direccionar al área de atención y reportar a la Unidad de Planificación para el seguimiento.

Por medio de las autoevaluaciones internas y auditorías externas se comunican oportunidades de mejora y observaciones de los procesos de TI, de las cuales se encuentran en proceso de atención.

Cumplimiento:

Cumple.

Nivel de riesgo:

Normal.

Evidencia de auditoría

1. Requerimientos de información del proceso.
2. Entrevistas con la Unidad de Tecnologías de Información y Comunicación.
3. Entrevista con la Auditoría Interna.
4. Entrevistas con usuarios finales.

5.3 Participación de la Auditoría Interna

La actividad de la Auditoría Interna respecto de la gestión de las TI debe orientarse a coadyuvar, de conformidad con sus competencias, a que el control interno en TI de la organización proporcione una garantía razonable del cumplimiento de los objetivos en esa materia.

Situación actual

De acuerdo con su plan de trabajo, la Auditoría Interna ejecuta revisiones e informes a los procesos de gestión de TI y realiza seguimientos periódicos de las recomendaciones en proceso de atención informadas por auditorías internas, externas y ente regulador para el área de TIC.

Cumplimiento:

Cumple.

Nivel de riesgo:

Normal.

Evidencia de auditoría

1. Requerimientos de información del proceso.
2. Entrevistas con la Unidad de TIC.
3. Entrevista con la auditoría interna.
4. Entrevistas con usuarios finales.

XI. Seguimiento de las recomendaciones de periodos anteriores.

Se resume el cumplimiento de las recomendaciones emitidas en informes de periodos anteriores. En el periodo 2017 no se encuentran observaciones en proceso de atención, fueron atendidas en el periodo anterior.

Estado	2015	2016	2018	2019	Total, General
Atendidas	14	13	9	2	38
En Proceso				2	2
Pendientes					-
N/A	1		1		2
Total	**15**	**13**	**10**	**4**	**42**



	Carta	Asunto	Estado		
			Atendido	En proceso	Se mantiene
X.1	**2015**	**4.4.8 Cumplimiento parcial de las políticas de gestión de calidad para los servicios de TI** **Riesgo Normal**	☒	☐	☐

El Sistema de Evaluación de la Calidad del Servicio que ofrece OCO no ha sido implementado, su aplicación está prevista como una de la metas del PAO 2016, específicamente: "Establecer un sistema para la gestión de la calidad del servicio de despacho de recursos para la atención de emergencias", a pesar de que se solicitó el aval para ser aplicado en plan piloto, tampoco se ha planificado, medido y analizado los diferentes servicios y productos que brinda la Unidad de TIC, y por ende no se han definido planes de acción que contribuyan a la mejora continua de dichos servicios, tal y como lo establece la política.

Al no medir, analizar y definir planes de acción relacionados a los servicios que ofrece la Unidad de TIC, podría no garantizarse una calidad suficiente en los servicios y productos de TI, lo que podría provocar fallas, retrabajo e impedimento de la mejora continua.

Recomendaciones

Cumplir lo establecido en las políticas relacionadas a la gestión de calidad, las cuales indican que se debe planificar, y ejecutar el seguimiento, medición, análisis y mejora continua de los servicios y productos de TI.

Gestionar la definición, aprobación y divulgación de una Metodología o Procedimiento de Gestión de Calidad, alineada con las políticas, con el fin de detallar e integrar cómo se llevará a cabo todo el proceso de gestión de calidad de los servicios y productos que ofrece la Unidad de TIC.

Comentario de la auditoría

Por medio de los oficios CBCR-024107-2021-TIB-00566, CBCR-024229-2021-PLB-00145 y las validaciones respectivas se atiende la observación.

	Carta	Asunto	Estado		
			Atendido	En proceso	Se mantiene
X.2	**2016**	**Sistema de Aseguramiento de la Calidad** **Riesgo Normal**	☒	☐	☐

Se requiere de la implementación de un Sistema de Aseguramiento de la Calidad, con el objetivo de evaluar los sistemas de información que son entregados por proveedores para ser implementados, medir y monitorear la calidad, el servicio de soporte técnico y evaluar su desempeño.

Recomendaciones

Valorar y establecer un equipo de trabajo para la implementación y atención de un Sistema de Administración de Calidad para los procesos de gestión de TI y de negocio.

Establecer un proceso de validación de la calidad del software, código fuente, su documentación y cumplimiento de la metodología utilizada en la entrega por parte del proveedor de los desarrollos contratados para posteriormente, pasarlos al plan de pruebas hasta continuar con su aceptación e implementación.

Comentario de la auditoría

Por medio de los oficios CBCR-024107-2021-TIB-00566, CBCR-024229-2021-PLB-00145 y las validaciones respectivas se atiende la observación.

	Carta	Asunto	Estado		
			Atendido	En proceso	Se mantiene
X.3	**2016**	**Ausencia de un plan y estrategia sobre Seguridad de la información** **Riesgo Normal**	☒	☐	☐

En apoyo a las actividades que se realizan es recomendable un plan y estrategia aprobado e implementado para reforzar la gestión de la seguridad de la información institucional.

Recomendación

Implementar un modelo de gestión de la seguridad de la información institucional, junto con una estrategia que refuerce a la organización sobre la integridad, confidencialidad y disponibilidad de la información, la infraestructura de procesamiento y minimice el impacto de vulnerabilidades e incidentes de seguridad.

Comentario de la auditoría

Por medio del oficio CBCR-035127-2021-PLB-00244, la evidencia aportada y la verificación respectiva se da por atendida la observación.

	Carta	Asunto	Estado		
			Atendido	En proceso	Se mantiene
X.4	**2016**	**Desarrollo de Excelsior** **Riesgo Elevado**	☒	☐	☐

No evidenciamos una estrategia referente al control del proyecto, para el monitoreo de su calidad y del retorno de la inversión conforme a las expectativas iniciales pactadas con la alta administración, por medio de una gestión documentada en cada etapa, para la administración de proyectos de esta magnitud.

Durante el desarrollo de esta auditoría no se nos suministró un cronograma detallado de la implementación de los módulos del ERP (Planificación de Recursos Empresariales) Excelsior, que permitiera reflejar la fecha de conclusión, costos, alcance y fechas de entregas de los diversos productos.

Recomendaciones

Establecer un procedimiento de monitoreo de calidad para el control de cumplimiento de objetivos de los contratos de servicios de tecnología adjudicados. De forma que logre el máximo aprovechamiento de los recursos y la implementación oportuna de los productos contratados. Así como su incorporación a los diversos contratos de servicios por outsourcing vigentes.

Establecer un cronograma y un costeo detallado, de finalización de los productos contratados por servicios de terceros, previo a la renovación del contrato en el mes de agosto de 2017.

Crear la Oficina de Administración de Proyectos en TIC para la gestión de todos los proyectos que se desarrollan en la Unidad.

Comentario de la auditoría:

Por medio de los oficios correspondientes: CBCR-028240-2021-TIB-00648 y CBCR-028378-2021-PLB-00174 y las validaciones respectivas se atiende la observación.

	Carta	Asunto	Estado		
			Atendido	En proceso	Se mantiene
X.5	**2018**	**IX.1 Delimitar el ancho de banda para el servicio de internet en las estaciones** **Riesgo Normal**	☒	☐	☐

En la comunicación con la jefatura de soporte técnico de Tecnologías de Información, nos informan que en las estaciones existen entre dos a cuatro equipos de cómputo, sin embargo, se identificaron algunas estaciones visitadas (Tibás, Pavas, Belén, Barrio México y Estación Central) en las que existen más de seis equipos en la red de la estación, llegando en algunos casos a existir hasta quince equipos entre computadoras e impresoras sin contar con otros dispositivos que se encuentran conectados a la red de la estación cómo es equipo personal de los bomberos, equipo de la Red Sismológica Nacional (RSN), y en algunas estaciones se cuentan con salas para realizar reuniones y capacitaciones a la cual los participantes llevan sus equipos personales y se conectan a la red por el WIFI de la estación.

Se conoce por medio del encargado de la Unidad de Servicios Generales que no se cuenta con un único proveedor de Internet para la organización, ya que en algunos casos el ICE (Instituto Costarricense de Electricidad), en algunas zonas el ancho de banda es muy reducido y la estación siente que necesita más por tal motivo, se dieron a la tarea de contratar con otros proveedores.

A nivel general se desconoce si en todas las estaciones el servicio de internet es deficiente porque el ancho de banda contratado con el proveedor no es el óptimo para las estaciones, o la infraestructura de cada estación ya se encuentra colapsada, por el incremento de las herramientas nuevas que la organización ha ido solicitando para la operativa de las estaciones y se ha ido aumentando la cantidad de equipo en las estaciones que en algunos casos supera lo indicado por la jefatura de soporte técnico casi al doble.

Recomendaciones

Definir un plan de trabajo para realizar una revisión a todas las estaciones e identificar la cantidad de equipos, tipo de servicios de internet y causas de caídas.

Realizar los cambios necesarios en las estaciones para el mejoramiento del servicio de internet, si el cambio abarca varias estaciones definir un plan de atención e incorporarlo en los planes operativos anuales.

Comentario de la auditoría:

Por medio de los oficios correspondientes: CBCR-011339-2021-TIB-00255 y CBCR-011947-2021-PLB-00086 y las validaciones respectivas se atiende la observación.

	Carta	Asunto	Estado		
			Atendido	**En proceso**	**Se mantiene**
X.6	**2018**	**IX.2 Seguridad en la red de las estaciones** **Riesgo Elevado**	☒	☐	☐

En entrevistas con la jefatura del área de infraestructura y Soporte Técnico, se identifica que en las estaciones no se cuenta con una infraestructura para el resguardo de la red de la estación y de la Institución. Aunque la cantidad de equipo es pequeño, si tienen conexión con internet para poder utilizar los sistemas que fueron creados para la administración en las estaciones.

Se carece de dispositivos para controlar los ingresos de ataques que provienen vía internet hacia la Institución.

Tener instalado un antivirus en nuestro ordenador es muy importante, pero, al fin y al cabo, los antivirus son solo una herramienta más en un sistema de seguridad que mantiene a salvo". Porque "los virus no son lo único que pone en riesgo nuestra vida digital". Cuando "un ciberdelincuente quiere tener acceso a tu ordenador, tiene multitud de opciones para hacerlo."

Recomendaciones

Aplicar los procedimientos de seguridad y monitoreo en las estaciones.

Realizar campañas de concientización a los colaboradores sobre el uso de equipo personales dentro de las instalaciones de la Institución.

Comentario de la auditoría

Por medio del oficio CBCR-035068-2021-PLB-00243, la evidencia aportada y la verificación respectiva se da por atendida la observación.

	Carta	Asunto	Estado		
			Atendido	**En proceso**	**Se mantiene**
X.7	**2018**	**IX.4 Revisar el proceso para comunicar los cambios** **Riesgo Normal**	☒	☐	☐

En la atención de un cambio en el Sistema de Facturación, se utilizó el canal de correo electrónico para informar de las modificaciones respectivas al Sistema por el problema de operación de este.

No evidenciamos la documentación del cambio, porque se nos indicó que el canal de comunicación para este cambio era vía correo electrónico.

Recomendaciones

Incluir en las licitaciones un apartado que indique una comunicación efectiva cuando se realicen cambios por el proveedor, principalmente cuando son sistemas contratados.

Revisar y valorar la aplicación el procedimiento de cambios de manera general para cualquier cambio o mejora.

Comentario de la auditoría

Por medio del oficio CBCR-030798-2021-PLB-00206, la evidencia aportada y la verificación respectiva se da por atendida la observación.

	Carta	Asunto	Estado		
			Atendido	**En proceso**	**Se mantiene**
X.8	**2018**	**IX.8 Procedimiento para el mantenimiento al cableado estructurado en las estaciones Riesgo Normal**	☒	☐	☐

Se determina que no existe un procedimiento para dar mantenimiento al cableado estructurado de la red de las estaciones, se constató que en las estaciones visitadas (Barrio México, Tibás, Pavas, Belén) no se encuentran bajo el estándar que se debe tener para la instalación de este.

Se carece de un monitoreo de la red en las estaciones y tampoco se encontró un documento que indique cómo se encuentra el ancho de banda en las estaciones o al menos en las que fueron revisadas en sitio y en forma remota.

El cableado estructurado en las estaciones visitadas no cuenta con la seguridad suficiente para evitar cortes, filtración de agua, incendio, ya que se encuentra expuesta o descubierta, carece de canaletas para su protección. Falta etiquetada del cableado.

Recomendaciones

Establecer una estandarización de infraestructura y realizar un estudio para determinar los anchos de banda adecuados según el requerimiento y demanda adecuados para cada estación.

Aplicar un procedimiento de revisión y mantenimiento en las estaciones para que toda la red en las estaciones sea provista de un cableado estructurado estandarizado.

Incorporar en la contratación nueva con el proveedor del servicio del cableado estructurado un diagrama de red para cada estación y la capacidad de dispositivos que soporta la red en el momento que se implemente, para llevar un control si se agrega un dispositivo adicional.

Comentario de la auditoría:

Por medio de los oficios correspondientes: CBCR-011339-2021-TIB-00255 y CBCR-011947-2021-PLB-00086 y las validaciones respectivas se atiende la observación.

	Carta	Asunto	Estado		
			Atendido	En proceso	Se mantiene
X.9	**2019**	**IX.1Actualización y aplicación del proceso de continuidad Riesgo Elevado**	☐	☒	☐

Evidenciamos que los documentos sobre el proceso de Gestión de la Continuidad de Negocio, que fueron diseñados por un tercero y con levantamiento de datos del 2015, 2016 y 2017, no se encuentran actualizados, entre otros los siguientes:

- Documento: "Análisis de impacto y mitigación por dependencia", plantea acciones por trimestre y semestre levantadas desde el 2016 y 2017. Los riesgos y acciones formuladas deben haber cambiado por la dinámica de la organización y del personal.
- Plan de Continuidad de TI: no tienen escenarios planteados, no describe los flujos de proceso con identificación de los equipos o puntos críticos de falla y su redundancia operativa o acción contingente, los documentos actuales generan dependencia del personal y de su reacción a la respuesta.
- Documento sobre los Roles y Responsabilidades para la Continuidad de las Operaciones del Benemérito Cuerpo de Bomberos de Costa Rica con fecha del 06/05/2016.
- Documento: Directriz de Continuidad de las Operaciones del Benemérito Cuerpo de Bomberos de Costa Rica con fecha del 27/08/2015.
- No evidenciamos que las acciones señaladas en el "Plan de Gestión de Continuidad Operativa", se han realizado y estén documentadas.

Llamamos la atención sobre los documentos revisados y que no cuentan con escenarios de riesgos, ni indicadores definidos en la restauración de los servicios y procesos críticos.

El personal de diferentes áreas de la institución no tiene claridad sobre las acciones que debería ejecutar ante un evento de interrupción de servicio, para la mitigación de riesgos y evitar la incertidumbre de las actividades a realizar.

Recomendaciones

Definir los escenarios de pruebas y ensayos que brinden la confianza y madurez sobre los planes y procedimientos para responder, recuperar, reanudar y restaurar el nivel de operación predefinido después de una interrupción en todas las áreas de la Institución.

Actualizar los documentos del proceso y considerar su aplicación.

Capacitar a las partes interesadas sobre la continuidad, basados en buenas prácticas de gestión o ISO 22301, con el objetivo de formar un equipo que lidere las tareas de formulación de pruebas, actualización del marco normativo y planes respectivos, incorporando procedimientos de gestión del cambio y manejo de incidentes como parte del ciclo integral de la continuidad de negocio.

Comentario de la auditoría

La recomendación 1 y 2 se encuentran pendientes, la número 3 se encuentra atendida.

	Carta	Asunto	Estado		
			Atendido	En proceso	Se mantiene
X.10	**2019**	**IX.2 Mejorar la gestión para proyectos con metodologías ágiles (SCRUM)** **Riesgo Normal**	☐	☐	☒

La herramienta aplicada MSProject para la planificación y control del proyecto, así como plantillas y reportes independientes, no brindan una visión integral del proceso aplicado y el desempeño del equipo de proyecto y no se deja documentación de los artefactos y eventos de la metodología SCRUM, para control y auditoría del ciclo de desarrollo.

Se carece de una herramienta integral del ciclo de SCRUM como control interno, que permita una gestión de la productividad y desempeño real del equipo de proyecto y al proveedor para la rendición de cuentas del proyecto contratado, con el objetivo que el área de sistemas y la jefatura de tecnología visualicen la ejecución y desarrollo del proyecto mediante informes y diagramas que concuerden con los reportes del proveedor y sus avances.

Recomendación

Valorar la implementación de una herramienta para el control del desarrollo de software utilizando metodologías ágiles que orienta el control de la planificación, diseño, construcción, ejecución y documentación en forma dinámica, gráfica y adaptativa.

	Carta	Asunto	Estado		
			Atendido	En proceso	Se mantiene
X.11	**2019**	**IX.3 Funcionalidad de WEBSIIS** **Riesgo Normal**	☒	☐	☐

El sistema WEBSIIS no brinda las funcionalidades del registro de entradas y salidas del inventario de los productos médicos al consultorio; a la fecha de este informe se lleva de manera manual y su salida se gestiona mediante un formulario que se llena manualmente al entregarse los medicamentos al funcionario, representando una debilidad de control. Las recetas requieren de un monitoreo alineado a la salida de medicamentos, para evitar el riesgo de pérdida del control de inventario.

Recomendaciones

Valorar por el dueño del sistema la automatización necesaria para evitar descontrol de inventarios y toma de decisiones en oportunidad.

Solicitar el acompañamiento en el levantamiento de los requerimientos funcionales respectivos para el registro y administración de los suministros médicos.

Comentario de la auditoría:

Por medio de los oficios correspondientes: CBCR-017188-2021-TIB-00408, CBCR-017957-2021-PLB-00100 y las validaciones respectivas se atiende la observación.

	Carta	Asunto	Estado		
			Atendido	En proceso	Se mantiene
X.12	**2019**	**IX.4 Acuerdos de niveles de servicio** **Riesgo Normal**	☒	☐	☐

En entrevistas a usuarios de los sistemas EXCELSIOR, EVA, WEBSIIS, SIABO, SIGAE sobre la atención de requerimientos por atender en la herramienta SUATTS, nos comunican que no conocen de los acuerdos de niveles de servicio y el tiempo para la atención del servicio solicitado.

Recomendaciones

Comunicar a todos los usuarios de las áreas de negocio los acuerdos de niveles de servicio con sus tiempos de respuesta.

Establecer un mecanismo de aceptación en tiempo entre las partes para la atención de los servicios solicitados a la mesa de servicio.

Comentario de la auditoría:

Por medio de los oficios correspondientes: CBCR-029779-2021-PLB-00196, CBCR-017459-2021-TIB-00410 y las validaciones respectivas se atiende la observación.

Conclusiones

1. Respecto al cumplimiento del Manual de Normas Técnicas de la Contraloría General de la República, de acuerdo con nuestra evaluación se requieren esfuerzos para cerrar la brecha respecto a los siguientes apartados para cumplir los objetivos de control:

   - ✓ Gestión de la Seguridad.
   - ✓ Gestión de proyectos.
   - ✓ Gestión de continuidad de operaciones de TI.
   - ✓ Implementación de la Infraestructura Tecnológica.

2. Fortalecer los procesos con la valoración interna y los marcos de referencia de buenas prácticas de control para TI para apoyar y entregar un valor al negocio.

3. En seguimiento de la resolución N° R-DC-17-2020 del 17 de marzo del 2020 sobre la derogación de las Normas Técnicas para la Gestión y el Control de las Tecnologías a partir del 1 de enero del 2022, dar seguimiento a los comunicados por el MICIT respecto a la definición de un Marco de Gestión de TI, y prepararse para los estudios de la auditoría de las posibles buenas prácticas que serán consideradas en el marco de gestión (COBIT, ITIL, ISO´s, entre otros).

Cuadro # 1

Cuestionario basado en las Normas Técnicas de la Contraloría General de la República

Capítulo	Sub-capítulo	#	Pregunta	Pts. Totales	Cumplimiento	Puntaje obtenido	Ref
CAPITULO I NORMAS DE APLICACIÓN GENERAL	***1.1 Marco Estratégica de TI***	**1**	¿Cuenta el área de TI con un marco estratégico constituido por políticas organizacionales?	1.47%	SI	1.47%	Se cuenta con un marco de Políticas "Manual de Políticas de Tecnologías V6". El mismo cuenta con las aprobaciones y es divulgado. Existe un plan estratégico institucional 2019-2023 y un plan estratégico de TI para el mismo periodo de tiempo.
		2	¿Se divulga este marco estratégico al personal de la empresa?	1.47%	SI	1.47%	Como mecanismos de divulgación del marco de TIC se ha implementado: • Mediante oficios CBCR-000456-2017-DGB-00004 y CBCR-013718-2017-TIB-00221 se comunica y priorizan contenidos a ser comunicados a nivel institucional. • Se publica en INSIDE (intranet de BCBCR) .Se adjunta "Divulgación" como evidencia. • Se ha implementado a nivel institucional una campaña que se envía por correo llamada "Hablemos de Tecnología" donde se publican contenidos referentes al marco como Normas técnicas de Control CGR, seguridad de información y otros. • Comunicados sobre actualización de procedimientos vigentes dentro de la unidad. Se adjunta "comunicado".
	1.2 Gestión de la Calidad	**3**	¿Se generan productos y servicios de TI de acuerdo con los requerimientos de los usuarios con base en un enfoque que permita alcanzar eficiencia y mejoramiento continuo?	1.47%	SI	1.47%	Existe un procedimiento para atender las solicitudes de los usuarios "2-03-04-178 Procedimiento para la Atención de Solicitudes de los Usuarios a la Unidad de TIC", que se implementa mediante el sistema SUATT. El SUATT es una herramienta automatizada que permite la atención de los requerimientos de TIC a fin de facilitar el proceso de atención, en esta los usuarios pueden mediante una encuesta calificar el grado de atención y satisfacción de los servicios ofrecidos por TIC. Se ha establecido una metodología de proyectos "2-03-04-187 Metodología para Administración de Proyectos" y un estándar de implementación de software y arquitectura "2-03-04-188 Estándar de implementación software e infraestructura de TIC" que incorpora el papel de los usuarios claramente definidos mediante roles y toma en cuenta su aceptación. En complemento el procedimiento "2-03-04-169 Procedimiento para la Administración y Control de Cambios de TI" complementa un plan de apoyo a las operaciones sobre los cambios que realiza TIC. Se envían correos recordatorios sobre uso de esta herramienta "recordatorio". Se requiere cumplir con la política para la Gestión de la Calidad.
	1.3 Gestión de Riesgos	**4**	¿Cuenta la empresa con un sistema de valoración de riesgos institucional que permita responder a las posibles amenazas que afecten la Gestión de TI?	1.47%	SI	1.47%	Con el propósito de alinear la valoración de riesgo a las metas de Bomberos de Costa Rica, existe un marco compuesto por los siguientes instrumentos, los cuales incorporan un ciclo de vida para la mitigación de los riesgos de TI. • Política para la Administración de Riesgos (Política 2 y Capítulo VI Ámbito de la Gestión de Riesgos de las Tecnologías). • Metodología para la administración de los riesgos, "2-03-04-183 Metodología para Administración de Riesgos". • Procedimiento para la administración de riesgos de TI, "2-03-04-156 Procedimiento para la Administración de Riesgos de TI".

Cuestionario basado en las Normas Técnicas de la Contraloría General de la República

Capítulo	Sub-capítulo	#	Pregunta	Pts. Totales	Cumplimiento	Puntaje obtenido	Ref
							• Se han dejado de identificar riesgos en proyectos y desarrollos que se han materializado.
	1.4 Gestión de la Seguridad de la Información	**5**	¿Posee la empresa una política de seguridad de información?	1.47%	SI	1.47%	Se ha definido el Capítulo VII Ámbito de la Gestión de la Seguridad de las Tecnologías y la Información.
		6	¿Cuenta la empresa con procedimientos para la asignación de recursos necesarios para lograr los niveles de seguridad requeridos?	1.47%	PARCIAL ALTO	0.98%	Los procedimientos "2-03-04-160 Procedimiento para el Control y Seguimiento de la Seguridad de la Información", "2-03-04-180 Procedimiento para el Seguimiento de los Procesos de TI", "2-03-04-157 Procedimiento para la Gestión de Identidad de Accesos" establecen los aspectos para definir e implantar las medidas de seguridad de la información. Se identifican recomendaciones de seguridad de la información.
		7	¿Poseen controles de acceso, y planes para la continuación de las operaciones en caso de presentarse una contingencia?	1.47%	PARCIAL BAJO	0.49%	Se adjunta plan de continuidad de TI que se definió bajo el fundamento de apoyar las operaciones de continuidad a los principales servicios de las tecnologías de información y comunicación, cuando un evento o situación de emergencia impacte sus operaciones normales, con el fin de reanudar las operaciones en el menor tiempo posible en forma eficiente. Se está en proceso de atención el plan de acción sobre informe de vulnerabilidades 2019 y la aplicación de la estrategia de seguridad de la información.
	1.4.1 Implementación de un marco de Seguridad de la Información	**8**	¿Se ha establecido un marco metodológico que incluya la clasificación de los recursos de TI?	1.47%	PARCIAL ALTO	0.98%	El marco está constituido por 2-03-04-158 Procedimiento para Clasificación de Activos de Información y 2-03-04-184 Estándar de clasificación de la información, que aún no se realiza.
		9	¿Se mantienen documentadas y actualizadas las responsabilidades del personal de la organización y de terceros relacionados?	1.47%	SI	1.47%	Los responsables se definen en el procedimiento.
	1.4.2 Compromiso del personal con la Seguridad de la Información	**10**	¿Se establecen medidas de seguridad, y se vigila constantemente y se ejecutan actualizaciones?	1.47%	SI	1.47%	Se adjunta evidencia sobre vigilancia de transacción mediante procesos de pistas de auditoria. Realización de planes de pruebas, así como reportes de monitoreo de Infraestructura sobre correo, políticas y componentes.
		11	¿Se capacita al personal sobre sus responsabilidades en materia de seguridad, confidencialidad y riesgos de TI?	1.47%	SI	1.47%	Se generan comunicados sobre la importancia de vigilancia de las transacciones mediante pistas de auditoria. Además, se generan campañas con temas de seguridad de información. La convención colectiva considera cláusulas de confidencialidad; así como los contratos en lo aplicable.

Capítulo	Sub-capítulo	#	Pregunta	Pts. Totales	Cumplimiento	Puntaje obtenido	Ref
		12	¿Existen implementadas medidas de seguridad relacionadas con las operaciones de los recursos de TI?	1.47%	SI	1.47%	El procedimiento 2-03-04-169 Procedimiento para la Administración y Control de Cambios de TI controla la seguridad de las operaciones gestionando que se realicen en un ambiente controlado. Se adjunta evidencia de aviso sobre actualizaciones a sistemas y reportes de monitoreo. Los ambientes de producción y pruebas están separados. Las puestas en producción son en coordinación con los usuarios. Se aplicaron guiones de pruebas que debieron estar mejor confeccionados que provocaron un porcentaje indicado en bitácoras de horas en pruebas.
		13	¿Existen políticas, reglas y procedimientos relacionados con el acceso a la información, al software de base y de aplicación, a las bases de datos y a las terminales y otros recursos de comunicación?	1.47%	SI	1.47%	Se cuenta con los procedimientos: "2-03-04-157 Procedimiento para la Gestión de Identidad de Accesos",2-03-04-193 Creación, actualización o retiro de usuarios de Base de Datos políticas sobre gestión de accesos. Se adjunta controles de matrices de roles en sistemas y gestión de accesos mediante suatts.
		14	¿Se han establecido y comunicado, a los funcionarios pertinentes, los objetivos de la administración y las políticas de TI?	1.47%	SI	1.47%	El cumplimiento de los objetivos de la administración está contemplado en el manual de Políticas fundamentalmente mediante las políticas 3, Administración estratégica de las TI y 4 Ambiente de Control que definen el Marco de control que gestiona la estrategia de TI. Adicionalmente se cuenta con el procedimiento 2-03-04-161 Procedimiento para Decisiones sobre Asuntos Estratégicos de TI como soporte a estas políticas. La planeación de las TIC es implementada mediante planes Estratégicos y Tácticos realistas a largo plazo de TI que reflejan los cambiantes avances tecnológicos y el progreso de la institución.
		15	¿El área de TI cuentan con procedimientos para la definición de perfiles, roles y niveles de privilegio, y para la identificación y autenticación para el acceso a la información, tanto para usuarios como para recursos de TI?	1.47%	SI	1.47%	Mediante el procedimiento "2-03-04-157 Procedimiento para la Gestión de Identidad de Accesos", se gestionan los accesos de los usuarios como a los recursos de TIC. Con esta cada área es la encargada de solicitar a TI la creación de una cuenta, así como la modificación de permisos, además RRHH es el encargado de comunicar a TI cuando un funcionario abandona la Institución. Además, el acceso a otros recursos como bases de datos, redes y carpetas compartidas gestionado mediante 2-03-04-038 Crear, asignar y distribuir las claves de acceso a la red inalámbrica institucional, 2-03-04-019 Crear y asignar políticas de usuarios del Active Directory Institucional,2-03-04-193 Creación, actualización o retiro de usuarios de Base de Datos. Se identifican mejora en la gestión de perfiles.
	1.4.3 Seguridad Física y Ambiental	**16**	¿La ubicación física es segura de los recursos de TI?	1.47%	SI	1.47%	Se he establecido un procedimiento para el control de acceso físico al área de TIC, en resguardo de los recursos, "2-03-04-007 Control de Acceso a las instalaciones de TIC", además de la política sobre Seguridad Física.
		17	¿Se cuentan con políticas y procedimientos para el ingreso y salida de equipos de la organización?	1.47%	SI	1.47%	Mediante procedimiento 2-03-04-075 Solicitar adquisición de accesorios de cómputo radiocomunicación y telefonía se gestiona la salida e ingreso de equipo.

Capítulo	Sub-capítulo	#	Pregunta	Pts. Totales	Cumplimiento	Puntaje obtenido	Ref
		18	¿Los requerimientos de seguridad fueron considerados en la implementación y mantenimiento de software e infraestructura de TI?	1.47%	SI	1.47%	Se cuenta con el estándar "2-03-04-188 Estándar de implementación software e infraestructura de TIC" que define los requerimientos en el mantenimiento y puesta en producción del software e infraestructura. En los contratos se referencia el uso de los estándares de programación. Además, se creó el estándar de Bases de Datos "2-03-04-189 Estándar de Base de Datos" para aseguramiento de la integridad de la información. El procedimiento "2-03-04-159 Procedimiento para el Acceso a los Programas Fuentes y Datos de Pruebas" colabora con el repositorio de fuentes; mediante el versiona miento y control de acceso de equipos de colaboradores a Producción o Pruebas. Se están desarrollando las pruebas de vulnerabilidad.
	1.4.4 Seguridad en las Operaciones y Comunicaciones	**19**	¿Se implementa mecanismos de control que permitan asegurar la autenticidad, la integridad y la confidencialidad de las transacciones y de la transferencia o intercambio de información?	1.47%	PARCIAL ALTO	0.98%	El procedimiento 2-03-04-157 Procedimiento para la Gestión de Identidad de Accesos controla la definición de perfiles, roles y privilegios y para la identificación y autenticación en el acceso a la información tanto para los usuarios como para recursos de TI mediante la autenticidad de usuarios. Además, institucionalmente se gestiona un proceso de implementación y seguimiento de pistas de auditoria que los usuarios gestionan de conformidad con sus requerimientos y en observancia de la información que custodian. Es necesario hacer aplicación de prácticas de ciberseguridad de la información y establecer a nivel institucional Sistema de Gestión de la Seguridad de la Información. Se está en proceso de atención el plan de acción sobre informe de vulnerabilidades 2019.
		20	¿Se cuenta con procedimientos para proteger la información almacenada en cualquier tipo de medio físico?	1.47%	SI	1.47%	Los procedimientos "2-03-04-030 Trasladar y Custodiar los Respaldos Institucionales", 2-03-04-197 Solicitud de respaldos y restauraciones de Base de Datos, 2-03-04-177 Procedimiento de Generación de Respaldos son controles de apoyo a manejo de la información de los usuarios.
		21	¿Se han establecido medidas preventivas, detectivas y correctivas con respecto a software "malicioso" o virus?	1.47%	SI	1.47%	Los procedimientos " 2-03-04-032 Monitorear la Ejecución de Reglas Programadas para Sitios WEB", 2-03-04-041 Revisar y asegurar la ejecución de las políticas del Antivirus Institucional en los equipos de la Institución, 2-03-04-055 Analizar e Investigar Paquetes Maliciosos que puedan afectar la infraestructura tecnológica en la Inst. Se adjunta evidencia de controles sobre correo, políticas y demás.

Capítulo	Sub-capítulo	#	Pregunta	Pts. Totales	Cumplimiento	Puntaje obtenido	Ref
	1.4.5 Control de acceso	**22**	¿Se cuentan con políticas y procedimientos relacionados con el acceso a la información, al software y terminales?	1.47%	SI	1.47%	Se cuenta con los siguientes procedimientos: 2-03-04-038 Crear, asignar y distribuir las claves de acceso a la red inalámbrica institucional, 2-03-04-193 Creación, actualización o retiro de usuarios de Base de Datos, 2-03-04-157 Procedimiento para la Gestión de Identidad de Accesos y el procedimiento 2-03-04-159 Procedimiento para el Acceso a los Programas Fuentes y Datos de Pruebas gestionan el acceso a estos recursos. Además del 2-03-04-184 Estándar de clasificación de la información que condiciona nivel de acceso a la información. Estos controles promueven una planeación y asignación de recursos, en fundamento de la integridad, disponibilidad y confiabilidad de la información, criterios indispensables en la entrega del servicio al usuario.
		23	¿Se ha definido la propiedad, custodia y responsabilidad sobre los recursos de TI?	1.47%	SI	1.47%	Se definido responsables de equipo como servidores y software.
		24	¿Se cuenta con procedimientos para la definición de perfiles, roles y niveles de privilegio para el acceso a la información?	1.47%	SI	1.47%	La creación de roles se ejecuta a luz del marco 2-03-04-187 Metodología para Administración de Proyectos, 2-03-04-188 Estándar de implementación software e infraestructura de TIC que consideran la Matriz de Roles. Sobre el seguimiento se considera el procedimiento 2-03-04-157 Procedimiento para la Gestión de Identidad de Accesos.
		25	¿Se cuenta con controles de acceso a la información impresa, visible en pantallas o almacenada en medios físicos y se protege adecuadamente dichos medios?	1.47%	SI	1.47%	Se ha definido 2-03-04-186 Estándar de clasificación de la documentación. Se debe aplicar el estándar de la clasificación de la información.
		26	¿Se cuenta con mecanismos necesarios (pistas de auditoría) que permitan un adecuado y periódico seguimiento al acceso a las TI?	1.47%	SI	1.47%	Se ha implementado a nivel institucional un proceso continuo de revisión de estas, en respuesta al procedimiento "2-03-04-125 Atender y gestionar la Configuración de Pistas de Auditoría de BD de los SI del BCBCR".
	1.4.6 Seguridad en la Implementación y mantenimiento de software e infraestructura tecnológica	**27**	¿Se controla el acceso a los programas fuente y a los datos de pruebas?	1.47%	SI	1.47%	Mediante el procedimiento "2-03-04-159 Procedimiento para el Acceso a los Programas Fuentes y Datos de Pruebas" se ha implementado el control de un repositorio de fuentes, su acceso y versionamiento.
		28	¿Se cuenta con procedimientos definidos para el mantenimiento y puesta en producción del software?	1.47%	PARCIAL BAJO	0,49%	Mediante la Política 20. Implementación de Software y el procedimiento "2-03-04-178 Procedimiento para la Atención de Solicitudes de los Usuarios a la Unidad de TIC" se implementa el mantenimiento del software. Se identifica 1 oportunidad de mejora sobre normativo para gestión de correos electrónicos.

Capítulo	Sub-capítulo	#	Pregunta	Pts. Totales	Cumplimiento	Puntaje obtenido	Ref
	1.4.7 Continuidad de los servicios de TI	**29**	¿La organización mantiene una continuidad razonable de sus procesos y su interrupción no afecta significativamente a sus usuarios?	1.47%	SI	1.47%	Se cuenta con un plan.
		30	¿Están documentadas y se pone en práctica, de forma efectiva y oportuna, las acciones preventivas y correctivas necesarias con base en los planes de mediano y largo plazo de la organización, la evaluación e impacto de los riesgos y la clasificación de sus recursos de TI según su criticidad?	1.47%	PARCIAL BAJO	0.49%	Falta la aplicación del plan de pruebas luego de la actualización del plan de continuidad de negocio. Hay 1 observación en proceso de atención.
	1.5 Gestión de proyectos	**31**	¿Se administran los proyectos de TI de manera que se logran los objetivos, se satisfacen los requerimientos y se cumple con los términos de calidad, tiempo y presupuesto óptimos prestablecidos por la Organización?	1.47%	PARCIAL ALTO	0.98%	Los proyectos de TIC se encuentran alineados a los objetivos estratégicos establecidos en el PETIC, que esboza su portafolio mediante planes tácticos y que se vuelven operables mediante planes Operativos institucionales que TIC. Los mismos consideran las aspiraciones de la alta Dirección mediante una priorización de estos. En consideración a la política 15 y 16. Se ha definido 2-03-04-187 Metodología para Administración de Proyectos, que contempla gestión de calidad, tiempo y presupuesto mediante controles en el ciclo de vida del proyecto. Se encuentra una observación en proceso de atención.
	1.6 Decisiones sobre asuntos estratégicos de TI	**32**	¿Se cuenta con un equilibrio entre la estrategia institucional y los proyectos de TI?	1.47%	PARCIAL ALTO	0.98%	Se ha definido el procedimiento "2-03-04-161 Procedimiento para Decisiones sobre Asuntos Estratégicos de TI". Los proyectos de TIC se encuentran alineados a los objetivos estratégicos establecidos en el PETIC, que esboza su portafolio mediante planes tácticos y que se vuelven operables mediante planes Operativos institucionales que TIC. Los mismos consideran las aspiraciones de la alta Dirección mediante una priorización de estos, en consideración a las políticas 15 y 16. Seguimiento al cumplimiento de los planes. La continuidad del desarrollo de otros módulos para el Excelsior se encuentra en proceso de contratación externa. En los informes de autoevaluación de control interno están en proceso de atención unas oportunidades de mejora.
	1.7 Cumplimiento de obligaciones relacionadas con la gestión de TI	**33**	¿La organización vela por el cumplimiento del marco jurídico que tiene incidencia sobre la gestión de TI con el propósito de evitar posibles conflictos legales que pudieran ocasionar eventuales perjuicios económicos y de otra naturaleza?	1.47%	PARCIAL ALTO	0.98%	En el marco de políticas de TIC se ha definido la Política 6. Cumplimiento de Obligaciones Relacionadas con la Gestión de TI; así mismo se ha establecido el procedimiento "2-03-04-162 Procedimiento para el Cumplimiento de las Obligaciones Relacionadas con la Gestión de TI". Se adjunta evidencia de medición de planes y actas presentadas al comité de TIC

Capítulo	Sub-capítulo	#	Pregunta	Pts. Totales	Cumplimiento	Puntaje obtenido	Ref
CAPÍTULO II PLANIFICACIÓN Y ORGANIZACIÓN	***2.1 Planificación de las Tecnologías de Información***	**34**	¿El proceso de planificación logra un balance óptimo entre los requerimientos, capacidad presupuestaria y las oportunidades que brindan las tecnologías existentes y emergentes?	1.47%	SI	1.47%	La planificación definida en el PETIC logra su operación mediante metas específicas en el PAO donde se justifican los requerimientos presupuestarios contemplados en este proceso. El PAO es evaluado por la alta dirección para asegurar el cumplimiento de objetivos y la inversión.
	2.2 Modelo de Arquitectura de Información	**35**	¿La empresa posee un modelo de arquitectura de información que identifique, capture y comunique, en forma completa, exacta y oportuna, sólo la información requerida por los procesos?	1.47%	SI	1.47%	El modelo de arquitectura de información está compuesto por: Política 17. Definición del Modelo de Arquitectura y Estandarización de TI. 2-03-04-164 Procedimiento para Definición de Estándares de los Sistemas de Información de TI. 2-03-04-188 Estándar de implementación software e infraestructura de TIC. 2-03-04-185 Estándares de Seguridad en la Información. 2-03-04-186 Estándar de clasificación de la documentación. 2-03-04-189 Estándar de Base de Datos. 2-03-04-200 Estándar de Programación. El mismo es divulgado para su cumplimiento por la alta dirección: CBCR-012892-2017-DOB-00264
	2.3 Infraestructura Tecnológica	**36**	¿La organización mantiene una perspectiva clara de su dirección y condiciones en materia tecnológica, así como de la tendencia de las TI para que, conforme a ello, optimice el uso de su infraestructura tecnológica, manteniendo el equilibrio que debe existir entre sus requerimientos y la dinámica y evolución de las TI?	1.47%	SI	1.47%	La perspectiva sobre la dirección es enmarcada en el PETIC y en consideraciones a tendencias para optimizar la infraestructura se define el Plan de Infraestructura como instrumento de apoyo en la planificación equilibrada en la infraestructura.
	2.4 Independencia y Recurso Humano de la Función de TI	**37**	¿TI es independiente respecto de las áreas usuarias, pero mantiene la coordinación y comunicación con las demás dependencias tanto internas y como externas?	1.47%	SI	1.47%	La estructura de TI; está definida para facilitar la especialización de servicios vinculados con requerimientos de la organización mediante planes como PETIC y Tácticos. De forma que pueda trabajar con independencia pero que colabore intrínsecamente con las áreas del negocio a las que sirve mediante servicios. Se ha establecido un Plan de Gestión de Recurso humano en TIC con consideración de capacitación, sucesión y demás. En apoyo a ello se cuenta con el 2-03-04-167 Procedimiento para la Administración del Recurso Humano de TI

Capítulo	Sub-capítulo	#	Pregunta	Pts. Totales	Cumplimiento	Puntaje obtenido	Ref
		38	¿Cuenta el área de TI con una fuerza de trabajo motivada, suficiente, competente y a la que se le haya definido, de manera clara y formal, su responsabilidad, autoridad y funciones?	1.47%	SI	1.47%	Se ha implementado un plan de capacitación de conformidad con los requerimientos de las diferentes áreas. Además, se considera un plan de sucesión para facilitar independencia funcional. Es necesario reforzar el tema de capacitación en la metodología de desarrollo Scrum a todos los funcionarios inmersos en la atención de requerimientos internos y externos con los proveedores.
	2.5 Administración de Recursos Financieros	**39**	¿Se controlan en forma efectiva los recursos financieros observando el marco jurídico que al efecto le resulte aplicable?	1.47%	SI	1.47%	El presupuesto de TIC está justificado mediante metas organizacionales en el PAO. Al mismo se le da seguimiento a nivel organizacional con evaluaciones de PAO y en TIC internamente se lleva un control de presupuesto consumido y disponible en colaboración a la efectividad de mismo, además se informa al COMITE de TIC. Se cuenta con el procedimiento en apoyo 2-03-04-168 Procedimiento para la Administración de Recursos Financieros TIC.
CAPITULO III IMPLEMENTACIÓN DE TECNOLOGIAS DE INFORMACION	***3.1 Consideraciones Generales de la Implementación de TI***	**40**	¿La Organización implementa y mantiene las TI requeridas y en concordancia con el marco estratégico y de planeación, así como con la arquitectura de información e infraestructura tecnológica?	1.47%	PARCIAL BAJO	0.49%	Se cuenta con un estándar de implementación de software e infraestructura (2-03-04-188 Estándar de implementación software e infraestructura de TIC) que establece pautas en concordancia a los requerimientos vigentes en materia de infraestructura y software. Se encuentra en proceso de atención observación del periodo 2019.
		41	¿Existen políticas sobre la justificación, autorización y documentación de solicitudes de implementación o mantenimiento de TI?	1.47%	SI	1.47%	La metodología de proyectos y la de infraestructura especifican los niveles y responsables de los procesos en la implementación y en proyectos. En la implementación se considera el visto bueno del usuario respecto a los cambios implementados.
		42	¿Se encuentra establecido el respaldo claro y explícito para los proyectos de TI tanto del jerarca como de las áreas usuarias?	1.47%	SI	1.47%	Los proyectos son respaldados por un comité de dirección multidisciplinarios donde participan las diferentes áreas, la alta dirección y TIC que se reúne y toman consideraciones sobre el proyecto.
		43	¿Se asignan líderes responsables a cada proyecto de TI?	1.47%	SI	1.47%	Los líderes de proyectos; así como los diferentes roles están definidos mediante la metodología de proyectos en la etapa de Formulación de Proyecto.
	3.2 Implementación de Software	**44**	¿Se ha desarrollado y aplicado un marco metodológico que guie los procesos de implementación y consideré la definición de requerimientos, los estudios de factibilidad, la elaboración de diseños, la programación y pruebas?	1.47%	PARCIAL ALTO	0.98%	El marco considera en primera instancia el Capítulo IV. Ámbito de la Gestión de la Implementación de las Tecnologías, respecto a ello se ha definido el estándar de implementación de software e infraestructura de TI "2-03-04-188 Estándar de implementación software e infraestructura de TIC" donde se establecen los lineamientos en la implementación así como: levantamiento de Requerimientos, Condiciones Generales de Desarrollo de Sistemas de Información, Estudio de Factibilidad, Especificación de Casos de uso, Formato Plan de Pruebas, Resultado de pruebas de usuario, capacitación y demás.

Capítulo	Sub-capítulo	#	Pregunta	Pts. Totales	Cumplimiento	Puntaje obtenido	Ref
							Adicionalmente este marco considera el procedimiento "2-03-04-164 Procedimiento para Definición de Estándares de los Sistemas de Información de TI". Se debe reforzar aspectos de QA del software y estudios de factibilidad y la atención de la observación IX.3
		45	¿Se establecen los controles y asignan las funciones, responsabilidades y permisos de acceso al personal a cargo de las labores de implementación y mantenimiento de software?	1.47%	SI	1.47%	El procedimiento "2-03-04-164 Procedimiento para Definición de Estándares de los Sistemas de Información de TI", colabora con este control. En el Plan de mantenimiento de Infraestructura se establecen responsables del mantenimiento de la infraestructura. También a nivel de software se establecen responsables de repositorio "2-03-04-159 Procedimiento para el Acceso a los Programas Fuentes y Datos de Pruebas". En la implementación de cambios mediante el SUATT se establece el responsable del cambio.
		46	¿Se controla la implementación de software en el ambiente de producción y se garantiza la integridad de datos y programas en los procesos de conversión y migración?	1.47%	SI	1.47%	Se cuenta con documentación detallada para efectuar migraciones de datos e información, se adjuntan procedimientos: "2-03-04-171 Procedimiento para la Elaboración del Plan de Migración de Datos", "2-03-04-170 Procedimiento para la Migración de Datos de Sistemas de Información"
		47	¿Se controla las distintas versiones de los programas que se generan como parte de su mantenimiento?	1.47%	SI	1.47%	Se cuenta con un procedimiento "2-03-04-159 Procedimiento para el Acceso a los Programas Fuentes y Datos de Pruebas" que gestiona el proceso de versiona miento.
	3.3 Implementación de la Infraestructura Tecnológica	**48**	¿Se adquiere, instala y actualiza la infraestructura necesaria para el buen funcionamiento del software?	1.47%	SI	1.47%	El plan de infraestructura y el plan de mantenimiento de infraestructura gestionan los requerimientos necesarios para una plataforma estable de software.
	3.4 Contratación de terceros para la implementación y mantenimiento de software e infraestructura	**49**	¿Se utiliza contratos a terceros en procesos de implementación o mantenimiento de software e infraestructura?	1.47%	SI	1.47%	Si, existen contratos a terceros. Estos se gestionan formalmente mediante la Ley de Contratación administrativa. En apoyo a la implementación se ha definido la política Administración de contratación por tercero y el procedimiento 2-03-04-173 Procedimiento para la Definición de Términos de Referencia con consideraciones de contratación. Es necesario incluir en todos los contratos la transferencia de conocimiento y la revisión por medio de informes de evaluaciones a los proveedores, adicional a la revisión del cumplimiento de los SLA´s.

Capítulo	Sub-capítulo	#	Pregunta	Pts. Totales	Cumplimiento	Puntaje obtenido	Ref
CAPITULO IV PRESTACIÓN DE SERVICIOS Y MANTENIMIENTO	***4.1 Definición y Administración de Acuerdos de Servicio***	**50**	¿La organización tiene claridad respecto a los servicios que requiere?	1.47%	SI	1.47%	Se ha establecido una lista que compone el catálogo de servicios de TIC. Los mismos han sido acordados entre la gerencia y TIC de conformidad a los requerimientos de la organización y a cuya función responde TIC con las distintas áreas. En dichos acuerdos se ha establecido un responsable por parte de TIC y uno por parte de la organización. Observación en proceso de atención.
		51	Se ha definido los procedimientos para la formalización de los acuerdos y la incorporación de cambios en ellos, así como los criterios de evaluación sobre el cumplimiento de los acuerdos.	1.47%	SI	1.47%	Se ha definido el "2-03-04-174 Procedimiento para la Definición y Administración de Acuerdos de Servicio" que considera la formalización en la incorporación de servicios. Se han definido SLA que consideran requerimientos de cumplimiento como acuerdos.
		52	¿Se revisan periódicamente los acuerdos de servicios incluyendo los contratos a terceros?	1.47%	SI	1.47%	Los requerimientos de servicio son revisados cada vez que se factura a proveedores mediante KPI´s que se documentan.
	4.2 Administración y operación de la plataforma tecnológica	**53**	¿La organización ha establecido y documentado los procedimientos y las responsabilidades asociados con la operación de la plataforma?	1.47%	SI	1.47%	Se han establecido políticas y procedimientos "2-03-04-159 Procedimiento para el Acceso a los Programas Fuentes y Datos de Pruebas"," 2-03-04-164 Procedimiento para Definición de Estándares de los Sistemas de Información de TI" y "2-03-04-175 Procedimiento para el Monitoreo del Desempeño y la Capacidad de la Infraestructura Tecnológica" donde se definen responsables asociados de la operación de la plataforma.
		54	¿Se vigila de manera constante la disponibilidad, capacidad, desempeño y uso de la plataforma, asegurar su correcta operación y mantener un registro de sus eventuales fallas?	1.47%	SI	1.47%	Se cuenta con procedimiento "2-03-04-175 Procedimiento para el Monitoreo del Desempeño y la Capacidad de la Infraestructura Tecnológica" que desprende un reporte mensual en observancia y reporte de fallas sobre la operación de la plataforma. Se adjuntan reportes mensuales.
		55	¿Existen controles sobre la composición y cambios de la plataforma y se mantiene un registro actualizado de sus componentes (hardware y software), custodiando adecuadamente las licencias de software y realizando verificaciones físicas periódicas?	1.47%	SI	1.47%	Se mantienen controles de cambios mediante bitácoras técnicas en el SUATT. Se mantiene un control del licenciamiento, así como el versionamiento del software.
		56	¿Se brinda el soporte adecuado a los equipos tanto principales como periféricos?	1.47%	SI	1.47%	Se adjunta evidencia sobre actividades de soporte a equipos de infraestructura y periféricos. El manteniendo de infraestructura se gestiona mediante el Plan de Mantenimiento de Infraestructura donde se calendarizan las tareas de soporte a realizarse en forma preventiva.

Cuestionario basado en las Normas Técnicas de la Contraloría General de la República

Capítulo	Sub-capítulo	#	Pregunta	Pts. Totales	Cumplimiento	Puntaje obtenido	Ref
		57	¿Poseen rutinas de respaldos, se controlan los procesos de restauración?	1.47%	SI	1.47%	El proceso de respaldos y restauraciones ha sido acogido mediante la planeación mediante el Plan de Mantenimiento. Además, que cuenta con los procedimientos "2-03-04-177 Procedimiento de Generación de Respaldos", "2-03-04-195 Restauración de respaldos de la Base de Datos", "2-03-04-197 Solicitud de respaldos y restauraciones de Base de Datos" como sustento a la ejecución.
		58	¿Existen parámetros definidos para las pruebas de sistemas (tales como de entrada, valores mínimos y máximos, etc.)?	1.47%	SI	1.47%	Se establecen planes de pruebas en la implementación donde se establecen parámetros esperados en el comportamiento del componente a validar.
	4.3 Administración de los datos	**59**	¿La administración se asegura de que los datos que son procesados por TI correspondan a transacciones válidas y debidamente autorizadas y que sean procesados de forma completa, exacta y oportuna?	1.47%	PARCIAL ALTO	0.98%	Se ha establecido a nivel institucional un proceso continuo de revisión de pistas de auditoria, como mecanismo se aseguramiento sobre integridad de información y autenticidad de transacciones. Falta un plan y estrategia de las prácticas de seguridad. Existe un procedimiento para la clasificación de la información que no se ha implementado.
	4.4 Atención de requerimientos de los usuarios de TI	**60**	¿El proceso para solicitar la atención de los requerimientos por parte del usuario es de manera fácil?	1.47%	SI	1.47%	Se cuenta con un procedimiento para la atención de requerimientos "2-03-04-178 Procedimiento para la Atención de Solicitudes de los Usuarios a la Unidad de TIC", el mismo es gestionado mediante la herramienta SUATT para facilitar el proceso al usuario.
	4.5 Manejo de incidentes	**61**	¿La organización identifica, analiza y resuelve de manera oportuna los problemas, errores e incidentes significativos que se susciten con las TI. Además, debe darles el seguimiento pertinente, ¿minimizar el riesgo de recurrencia y procurar el aprendizaje necesario?	1.47%	SI	1.47%	Mediante el procedimiento "2-03-04-178 Procedimiento para la Atención de Solicitudes de los Usuarios a la Unidad de TIC", se bitácoras incidentes, los mismos son gestionados mediante el SUATT. Se procura la gestión y aprendizaje de problemas.
	4.6 Administración de servicios prestados por terceros	**62**	¿La administración minimiza la dependencia de la organización respecto de los servicios contratados a un tercero?	1.47%	SI	1.47%	La contratación a terceros se realiza mediante contratos donde se consideran criterios de apego a contratos de desarrollo, transferencia de conocimiento entre otros para minimizar la dependencia. Estos términos son referidos mediante "2-03-04-173 Procedimiento para la Definición de Términos de Referencia".

Cuestionario basado en las Normas Técnicas de la Contraloría General de la República

Capítulo	Sub-capítulo	#	Pregunta	Pts. Totales	Cumplimiento	Puntaje obtenido	Ref
CAPITULO V SEGUIMIENTO	***5.1 Seguimiento de los procesos de TI***	**63**	¿La organización se encarga de asegurar el logro de los objetivos propuestos como parte de la gestión de TI?	1.47%	SI	1.47%	El cumplimiento de los objetivos de la administración está contemplado en el manual de Políticas fundamentalmente mediante las políticas 3, Administración estratégica de las TI y 4 Ambiente de Control que definen el Marco de control que gestiona la estrategia de TI. La planeación de las TIC es implementada mediante planes Estratégicos y Tácticos realistas a largo plazo de TI que reflejan los cambiantes avances tecnológicos y el progreso de la institución. Adicionalmente en apoyo a esta gestión internamente en TIC, se ha establecido un proceso referenciado por la Política 5. Seguimiento y Control Interno y el procedimiento "2-03-04-180 Procedimiento para el Seguimiento de los Procesos de TI" que establecen un marco de referencia y un proceso de seguimiento como mecanismos para vigilar la gestión de TI.
		64	Existe un marco de referencia que defina el alcance, la metodología y los mecanismos para vigilar la gestión de TI.	1.47%	SI	1.47%	Se ha establecido la Política 5. Seguimiento y Control Interno y el procedimiento "2-03-04-180 Procedimiento para el Seguimiento de los Procesos de TI" establece un marco de control para evaluar y dar seguimiento a la gestión de las tecnologías de información.
		65	¿Se determinan las responsabilidades del personal a cargo del seguimiento de los procesos de TI?	1.47%	SI	1.47%	Se han establecido responsables del proceso de seguimiento de los procesos de TIC, mediante el programa de Normativa y Control.
	5.2 Seguimiento y evaluación del control interno	**66**	¿Existe establecido un sistema de control interno asociado con la gestión de las TI?	1.47%	SI	1.47%	El control interno hacia TIC se realiza mediante Auditorías externas.
		67	¿Este sistema de control interno evalúa la efectividad y cumplimiento de las excepciones que se presenten y de las medidas correctivas implementadas?	1.47%	SI	1.47%	Producto de las auditorías externas, se realizan informes donde se emiten hallazgos, la administración emite planes de acción a los cuales se les da seguimiento internamente en TIC y las diferentes direcciones según corresponda y se reporta a la Unidad de Planificación quien es la encarga de dar seguimiento por parte de institución. Es necesario cumplir con el procedimiento para el seguimiento de los procesos de TI, existen autoevaluaciones con recomendaciones de periodos anteriores sin atender, existen recomendaciones de área de negocio que se indicaron en informes de TI.
	5.3 Participación de la auditoria interna	**68**	¿La Auditoría Interna coadyuva, de conformidad con sus competencias, a que el control interno en TI de la organización proporcione una garantía razonable del cumplimiento de los objetivos en Gestión de TI?	1.47%	SI	1.47%	La auditoría interna participa mediante Auditorías Externas a TIC.
ESTADO GENERAL:						92.16%	