Benemérito Cuerpo de Bomberos de
Costa Rica

Informe de auditoría externa de sistemas de información del Benemérito Cuerpo de Bomberos de Costa Rica

Al 31 de diciembre de 2021

Crowe Horwath CR, S.A.

Benemérito Cuerpo de Bomberos de Costa Rica

Informe de auditoría externa de sistemas de información del Benemérito Cuerpo de Bomberos de Costa Rica

Al 31 de diciembre de 2021

Benemérito Cuerpo de Bomberos de Costa Rica

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 - 6 -
III. Responsabilidad de los auditores y marco normativo - 6 -
IV. Alcance - 7 -
V. Procedimientos - 8 -
VI. Delimitaciones - 8 -
VII. Metodología de evaluación - 9 -
VIII. Resultados del periodo 2021 - 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 - 16 -
XI. Seguimiento de las recomendaciones de periodos anteriores - 48 -

Conclusiones - 52 -
Anexo # 1 - 53 -
Anexo # 2 - 55 -
Cuadro # 1 - 57 -

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

30 de setiembre de 2022

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.

Atentamente,

FABIAN ZAMORA AZOFEIFA (FIRMA)

Firmado digitalmente por FABIAN ZAMORA AZOFEIFA (FIRMA)
Fecha: 2022.11.25 10:40:31 -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.

Cuadro A: Sistemas Informáticos [1]:

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.
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.

[1] Se copia textualmente la tabla de sistemas según el cartel CBCR-018522-2021-PRB-00778, 10 de mayo de 2021.

N°	Nombre del sistema	Función
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.

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.

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 2021 no es efectivo en relación con las normas y procedimientos vigentes de 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, 1.4.1, 1.4.3, 1.4.4, 1.4.6, 1.4.7, 4.2 y 4.3.

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 este informe de auditoría externa de los sistemas de información al 31 de diciembre de 2021 se extiende hasta el 30 de setiembre de 2022. La fecha de este informe 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.

FABIAN ZAMORA AZOFEIFA (FIRMA)

Firmado digitalmente por FABIAN ZAMORA AZOFEIFA (FIRMA)
Fecha: 2022.11.25 10:41:15 -06'00'

Dictamen firmado por
Fabián Zamora Azofeifa N° 2186
Pol. 0116 FIG 7 V.30-9-2023
Timbre Ley 6663 ¢1.000
Adherido al original

Nombre del CPA: FABIAN ZAMORA AZOFEIFA
Carné: 2186
Cédula: 302870450
Nombre del Cliente: Benemérito Cuerpo de Bomberos de Costa Rica
Identificación del cliente: 3007547060
Dirigido a: Benemérito Cuerpo de Bomberos de Costa Rica
Fecha: 25-11-2022 08:16:14 AM
Tipo de trabajo: INFORME DE AUDITORÍA EXTERNA SOBRE LOS SISTEMAS DE INFORMACIÓN

Timbre de ¢1000 de la Ley 6663 adherido y cancelado en el original.

FABIAN ZAMORA AZOFEIFA
Contador Público Autorizado
No. 2186
COSTA RICA

COSTA RICA TIMBRE
1000 COLONES 1000

Código de Timbre: CPA-1000-1860

Anexo A

Benemérito Cuerpo de Bomberos de Costa Rica

Informe de auditoría externa de sistemas de información del Benemérito Cuerpo de Bomberos de Costa Rica

Al 31 de diciembre de 2021

I. Resumen ejecutivo

De acuerdo con lo indicado en la contratación de los servicios de auditoría externa de Tecnología de Información, se planifica y realiza la auditoría.

Durante el plazo de la revisión se van compartiendo resultados y avance con la Auditoría Interna, que es quien hace la contratación de los servicios.

Para el estudio de la revisión de los sistemas de información del periodo 2021, se basó en los criterios que establece las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE) emitida por la Contraloría General y marco normativo de la Institución.

En el alcance se consideró la visita a 10 estaciones de bomberos, con el objetivo de validar controles en seguridad física y lógica en las computadoras y tabletas que permitieron identificar oportunidades de mejora que se detallan en el informe.

Adicionalmente, se realizaron evaluaciones a los sistemas, entre ellos al sistema Excelsior en módulos tales como Planificación y Presupuesto, Gestión de Activos, Compras, Aprovisionamiento, SIGAE. Así mismo, el seguimiento a las recomendaciones del informe del periodo 2020.

Se presenta un resumen de lo comunicado en el estudio:

Oportunidades de mejora 2021:

Ref.	Oportunidades de mejora	Nivel de cumplimiento	Impacto	Frecuencia	Categoría de riesgo
X.1	Debilidades de cableado y dispositivos de acceso inalámbrico en estaciones	Cumplimiento parcial bajo	Serio	Frecuente	Elevado
X.2	Servicios de internet y seguridad de la información	Cumplimiento parcial bajo	Serio	Frecuente	Elevado
X.3	Inconsistencias en sistemas de información	Cumplimiento parcial bajo	Serio	Frecuente	Elevado

Seguimiento de recomendaciones de periodos anteriores

Año	Ref.	Oportunidades de mejora	Nivel de cumplimiento	Impacto	Frecuencia	Categoría de riesgo
2020	XI.2	X.2 Saltos en los consecutivos y duplicados en SICOF (1.4.6)	Cumplimiento parcial bajo	Serio	Frecuente	Elevado
2019	XI.3	IX.1 Actualización y aplicación del proceso de continuidad (1.4.7)	Cumplimiento parcial bajo	Serio	Frecuente	Elevado

II. 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 en proceso de atención de los años 2019 y 2020 sobre este mismo tema.

III. Responsabilidad de la Administración

La administración del BCBCR 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.

IV. 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. Los procedimientos seleccionados dependen del juicio del auditor.

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

V. 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.

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.

VI. 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.

VII. 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 Contralor emitió la resolución No. R-DC-17-2020 en la cual notifica la derogatoria de las Normas Técnicas de Tecnologías de Información y Comunicación con un transitorio de vigencia hasta el 31 de diciembre del 2021:

…" Artículo No. 1 Derogar las Normas Técnicas para la Gestión y Control de las Tecnologías de Información (N-2-2007-CO-DFOE), resolución No. R-CO.26-2007 del 07 de junio del 2007, a partir del 1° de enero del 2022 …"

Actualmente las Normas vigentes y de acatamiento fueron emitidas por la Dirección de Gobernanza Digital del MICITT (Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones), conforme oficio No. MICITT–DGD-OF-215-2021, (oficio de formalización de las nuevas normas técnicas de Tecnologías de Información, las cuales están vigentes a partir del 1 de enero del 2022).

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.

El informe corresponde a la evaluación del periodo 2021, con la presentación de evidencia al 30 de setiembre de 2022.

VIII. 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 valida 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[2]:

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.

[2] 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.

Se identifica una lista actualizada de los sistemas de información que fue aportada a la auditoría interna para la actualización en el contrato por los servicios de la contratación CBCR-018522-2021-PRB-00779, Licitación Abreviada 2021LA-000012-0012800001, para el servicio de auditoría externa en los Sistemas de Información del BCBCR. Ver Anexo # 1.

Los resultados fueron tabulados, analizados y se presenta en el informe oportunidades de mejora 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.

C. Seguimiento a las recomendaciones anteriores

Se ejecutaron las siguientes acciones:

a) Revisar el informe de seguimiento de auditoría de sistemas de información externo al 28 de febrero de 2022.

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.

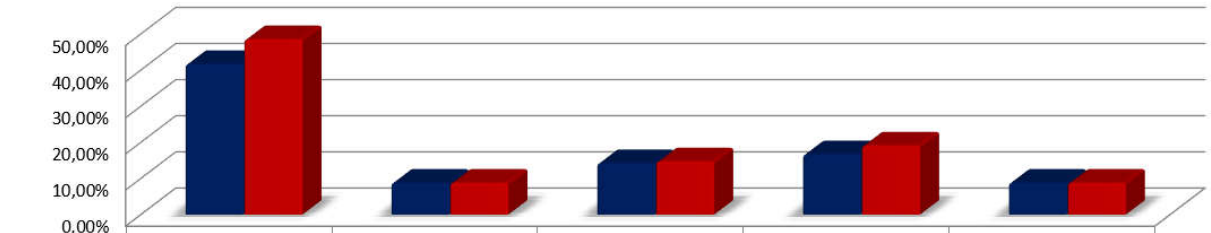
IX. Resultados del periodo 2021 con oportunidades de mejora y en proceso de atención de los apartados de las Normas Técnicas de la Contraloría General de la República

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 alto	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	Cumplimiento parcial bajo	Elevado
1.4.4	Seguridad en las operaciones y comunicaciones	Cumplimiento parcial bajo	Elevado
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	Cumple	Normal
1.6	Decisiones sobre asuntos estratégicos de TI	Cumple	Normal
1.7	Cumplimiento de obligaciones relacionadas con la gestión de TI	Cumple	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	Cumple	Normal
3.2	Implementación de Software	Cumple	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	Cumplimiento parcial bajo	Elevado
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	41,67%	48,53%
II	PLANIFICACIÓN Y ORGANIZACIÓN	8,82%	8,82%
III	IMPLEMENTACIÓN DE TECNOLOGIAS DE INFORMACION	14,22%	14,71%
IV	PRESTACION DE SERVICIOS Y MANTENIMIENTO	16,67%	19,12%
V	SEGUIMIENTO	8,82%	8,82%
ESTADO GENERAL		90,20%	100,00%



	I	II	III	IV	V
Estado	41,67%	8,82%	14,22%	16,67%	8,82%
Cumplimiento	48,53%	8,82%	14,71%	19,12%	8,82%

Capítulo I Normas de aplicación general

Ref.	Oportunidades de mejora	Nivel de cumplimiento	Impacto	Frecuencia	Categoría de riesgo
X.1	Debilidades de cableado y dispositivos de acceso inalámbrico en estaciones	Cumplimiento parcial bajo	Serio	Frecuente	Elevado
X.2	Servicios de internet y seguridad de la información	Cumplimiento parcial bajo	Serio	Frecuente	Elevado

Capítulo IV Prestación de servicios y mantenimiento

Ref.	Oportunidades de mejora	Nivel de cumplimiento	Impacto	Frecuencia	Categoría de riesgo
X.3	Inconsistencias en sistemas de información	Cumplimiento parcial bajo	Serio	Frecuente	Elevado

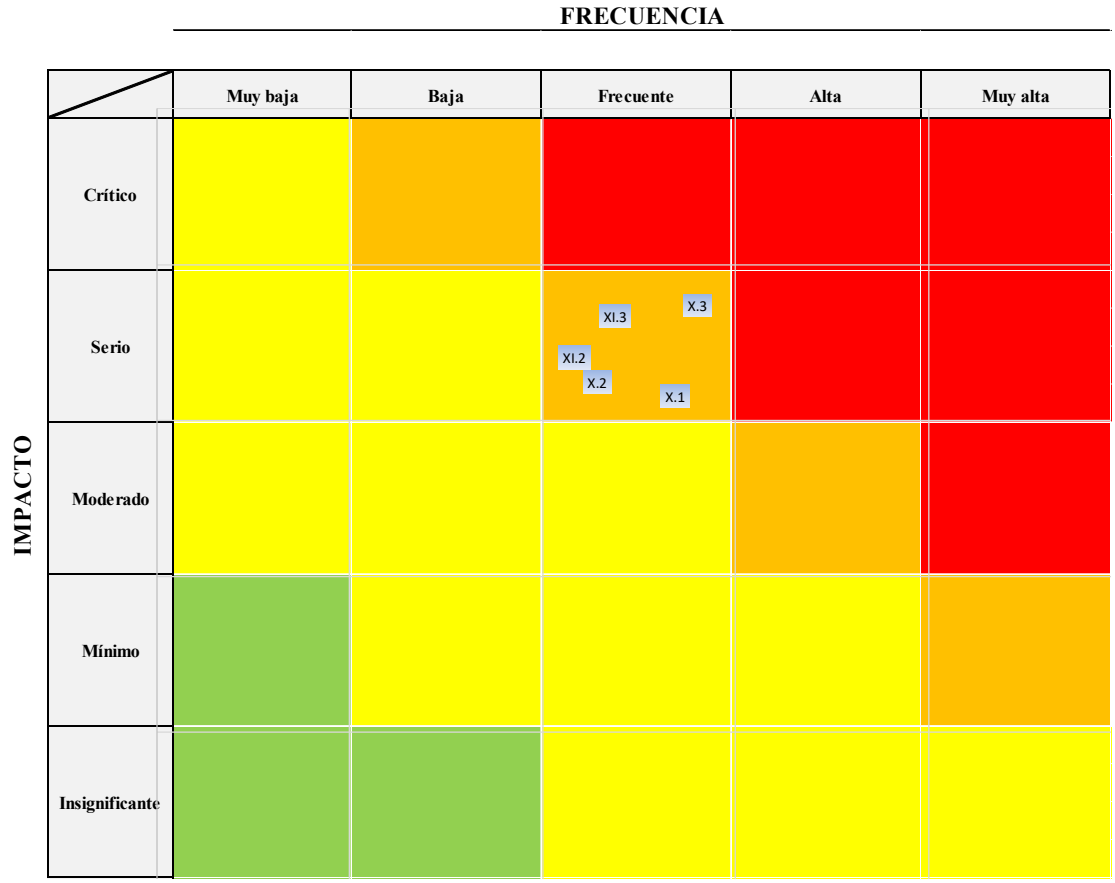
Seguimiento de las recomendaciones de periodo anteriores

Se encuentran en proceso de atención los siguientes 2 hallazgos:

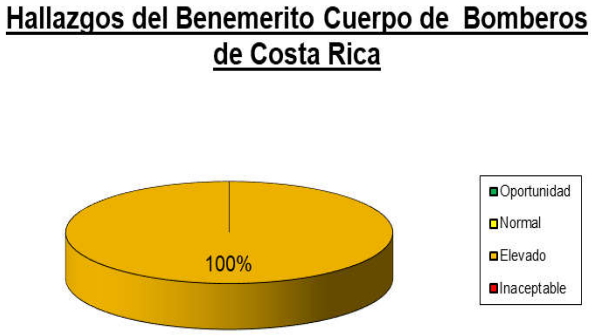
Año	Ref.	Oportunidades de mejora	Nivel de cumplimiento	Impacto	Frecuencia	Categoría de riesgo
2020	XI.2	X.2 Saltos en los consecutivos y duplicados en SICOF (1.4.6)	Cumplimiento parcial bajo	Serio	Frecuente	Elevado
2019	XI.3	IX.1 Actualización y aplicación del proceso de continuidad (1.4.7)	Cumplimiento parcial bajo	Serio	Frecuente	Elevado

X. 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 2021.



Como resultado del periodo 2021 y las observaciones de seguimiento, se identifican 5 observaciones, se distribuyen en un riesgo elevado:

- 5 de riesgo elevado

XI. 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 marco estratégico constituido por políticas, procedimientos, manuales, entre otros.

Se dio cumplimiento de los objetivos del PAO 2021.

Se está en proceso de implementación de las normas técnicas del MICITT, por medio de un cronograma que se ha ido cumplimiento en tiempo las actividades programadas.

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 marco normativo para el cumplimiento de la Gestión de la Calidad y cumplir las necesidades de los usuarios y cumplir con los planes de trabajo y los objetivos y metas institucionales.

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

Existe un sistema de valoración de riesgos institucional que permita responder a las posibles amenazas que afecten la Gestión de TI y la Gestión de Gobierno.

Se realizan ejercicios y evaluaciones de acuerdo con los procedimientos internos.

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 y técnicos.

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 para la gestión de seguridad. Se está conformando el Comité de Seguridad de la Información. Se atienden las alertas técnicas aportadas por el MICITT y la Contraloría.

Aun no se ha gestionado la clasificación de la información. Se atiende el plan de acción sobre los estudios de vulnerabilidades presentados en el mes de diciembre de 2021.

Se debe fortalecer la supervisión y administración de la seguridad del sistema de información a través de herramientas que correlacionen eventos e intervención remota, como parte de la implementación de las prácticas de seguridad.

Cumplimiento:

Parcial alto.

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. Informes de vulnerabilidades externas.
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

Existe un marco regulatorio aprobado.

Se hacen revisiones de seguridad y monitores internos y externos de acuerdo con los planes de trabajo.

Existen oportunidades de mejora para reforzar la clasificación de los activos de la información y el cierre de brechas de las evaluaciones de vulnerabilidades.

Se trabaja en la socialización y evaluación de la Política de Gestión de Seguridad de la Información y Ciberseguridad del Grupo INS, disposiciones complementarias a la Política de Gestión de Seguridad de la Información y Ciberseguridad del Grupo INS y Política de Comunicaciones y Reputación del Grupo INS.

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.

1.4.2 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

Se aplica el cumplimiento de un plan de capacitación del periodo 2021 y 2022.

Se encuentran medidas de seguridad implementadas relacionadas con las operaciones de los recursos de TI.

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. Entrevistas con usuarios técnicos y dueños de los sistemas de información.

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

Existen mecanismos de seguridad física y ambientales para las instalaciones administrativas y oficinas.

Se mantiene control para el ingreso y salida de equipo. El data center mantiene controles razonables.

Se cuenta con brigadas y procedimientos para simulacros y evacuaciones respectivas.

X.1 Debilidades de cableado y equipos de acceso inalámbrico en estaciones

En el anexo # 2 de este informe se presenta un resumen de los resultados a las 10 estaciones seleccionadas para validar los controles de seguridad física, lógica, infraestructura, operativos y de continuidad de los servicios.

Condición

Se identifican problemas de cableado estructurado para comunicaciones, telefonía y electricidad y uso de UPS y regletas en las siguientes estaciones:

- ✓ Guadalupe
- ✓ Santo Domingo

Los access point revisados en las estaciones, presentaron pérdida de señal para los equipos a los cuales se encuentran relacionados, en:

- ✓ Tibás
- ✓ Belén
- ✓ Metropolitana Norte

Causa

En el plan de mantenimiento les corresponde la atención del cableado a estas estaciones en el último trimestre del 2022 y en el 2023.

Se debe informar al área responsable sobre la pérdida de señal de los equipos de acceso inalámbrico.

Efecto

Problemas en tiempo de conectividad más allá de la disponibilidad mínima requerida por pérdida de señal.

Recomendaciones

Valorar incorporar otras acciones de coadyuven en brindar un seguimiento para el mantenimiento preventivo de equipos de manera presencial o virtual según la atención o actividad que se deba desarrollar.

Recordar y reforzar a los usuarios el objetivo de las baterías (UPS) y el uso de las regletas para un uso efectivo por parte del personal en las estaciones y del cumplimiento del marco de normativo.

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. Visita a estaciones de bomberos.

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

Se han implementado mecanismos de control que permitan asegurar la autenticidad, la integridad y la confidencialidad de las transacciones y de la transferencia o intercambio de información por medio de firewalls, evaluaciones de vulnerabilidades, accesos por VPN, aplicación del doble factor de autenticación, gestión de contraseñas.

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

Se atiende el plan de acción sobre la evaluación de vulnerabilidades, las alertas del MICITT y el plan de implementación de las normas del MICITT.

X.2 Servicio de internet y seguridad de la información

En el anexo # 2 de este informe se presenta un resumen de los resultados a las 10 estaciones seleccionadas para validar los controles de seguridad física, lógica, infraestructura, operativos y de continuidad de los servicios.

Condición

a) Servicio de internet de 10 GB, genera lentitud para acceso a los sistemas de información y la operativa diaria en las siguientes estaciones:

- ✓ Tibás
- ✓ Belén
- ✓ Santo Domingo
- ✓ San Ramón

b) Las tabletas que son usadas en las estaciones no contienen antivirus.

c) Se evidencia 2 equipos con antivirus desactualizado, uno en cada estación:

- ✓ Metro Sur (ESCENTRAL-RECEPT)
- ✓ Guadalupe, ver recorte:

d) Uso de USB no cuenta con supervisión de seguridad. No se encuentran encriptados los dispositivos. La práctica se da en las 10 estaciones evaluadas.

e) En las carpetas de "Escritorio, Papelera de Reciclaje y en Descargas" hay una amplia cantidad de informes, archivos, fotos entre otros documentos, que no se eliminan ni desechan en las 10 estaciones revisadas.

Causa

a) Posible falta de capacidad del proveedor.
b) No se había incorporado al presupuesto esa inversión para la seguridad en las tabletas.
c) Equipo guardado sin uso, el cual es vulnerable al utilizarlo.
d) Falta de monitoreo de los dispositivos.
e) Falta reforzar y evaluar prácticas de seguridad para la operativa y funcionalidad de los equipos y sistemas de información.

Efecto

Posible demora en tiempo para conectividad a los sistemas y pérdida de señal.

Exposición a vulnerabilidades que puedan ocasionar perdida de información.

Recomendaciones

Reconsiderar de acuerdo con la capacidad y ubicación de las estaciones una ampliación del internet de acuerdo con lo normado y la ampliación en el uso de los sistemas por la operativa diaria, valorar alternativas en los casos más necesarios.

Dar seguimiento a la implementación de los antivirus en las tabletas.

Entregar equipo que no se encuentra en uso al área responsable por la exposición al ser encendido y no estar actualizado el antivirus.

Ampliar y reforzar el programa de capacitación de seguridad por medio de evaluaciones y la aplicación de controles de seguridad entorno a los USB, carpetas con información que puede ser desechada, la importancia y funcionamiento de los antivirus.

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. Visita a estaciones.

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

Existen políticas y procedimientos relacionados con el acceso a la información, al software y terminales de trabajo.

Se cuenta con procedimientos para la definición de perfiles, roles y niveles de privilegio para el acceso a la información.

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.

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

Se cuenta con procedimientos definidos para el mantenimiento y puesta en producción del software.

Se utiliza el sistema "SUAT" como parte de los servicios de la mesa de ayuda.

Se cuenta con un plan de infraestructura tecnológica para el periodo 2021.

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

Se encuentra en proceso de atención observación sobre los saltos en los consecutivos y duplicados en SICOF.

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. 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.

Situación actual

Existe un marco normativo aprobado y de conocimiento institucional.

Se aplican procedimientos de redundancia, respaldos y pruebas de restauración de datos.

Se deben aplicar los escenarios de pruebas para la continuidad de operaciones. En la sección de seguimiento se encuentra observación 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 y procedimientos aprobados para la gestión de proyectos.

Se identifica a nivel institucional un recurso que llevara las tareas como "Gestor de Proyectos" a partir de agosto de 2022.

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.

1.6 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

El plan estratégico de TI se encuentra alineado al plan estratégico institucional.

Existe un Comité de Tecnología formalmente establecido y se mantiene actas de las reuniones ejecutadas.
Los canales de comunicación se encuentran formalizados.

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.

1.7 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 un perfil tecnológico para la Gestión de Tecnologías de información de acuerdo con la implementación de las normas del MICITT.

Se cuenta con un cronograma de trabajo para la implementación del nuevo Marco de Gestión.

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.

2.1 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 de trabajo.

Se han atendido temas de ciberseguridad y seguridad de la información en acatamiento con el MICITT y el fortalecimiento de los procesos y servicios de TI.

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 estándares, política y prácticas de control y gestión.

La oficialización del Modelo de arquitectura de información se dio mediante oficio CBCR-012892-2017-DOB-00264.

Existen oportunidades de mejora que se encuentran en proceso de atención de acuerdo con las nuevas normas del MICITT.

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 de acuerdo con las proyecciones de presupuesto, se aplican tareas de control para verificar el uso de los recursos de la manera más eficiente.

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. Funcionalidad de los sistemas.

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 trabaja en función del PAO y los planes tácticos para cumplir con el Plan Estratégico de Tecnologías de Información y Comunicación, en caso de existir desviación o cambio se hace la debida comunicación a los Órganos de Dirección.

Se han aplicado capacitaciones al recurso humano de TI, se han realizado las evaluaciones sobre el desempeño de los puestos de trabajo. Existe un plan de sucesión.

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.

2.5 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.

Se hace rendimiento de cuenta sobre el presupuesto asignado y aplicado de acuerdo con los procedimientos internos de control.

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 desarrollo de software, por medio del sistema SUATT los usuarios detallan sus necesidades y requerimientos.

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

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.

3.2 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.

Se han confeccionado una serie de procedimientos respecto al ciclo de vida 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. Entrevistas con usuarios finales.

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

De acuerdo con el PAO y el plan de infraestructura tecnológica se adquiere la compra de equipo, software, licencias y otros activos de TI.

La gestión de contratos cumple con los procedimientos establecidos a lo interno y la Ley de Contratación Administrativa.

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 y 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.

Se aplica el procedimiento para la “Definición y Administración de Acuerdos de Servicio” para la formalización de servicios.

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 normativo para la administración y operación de la plataforma tecnológica.

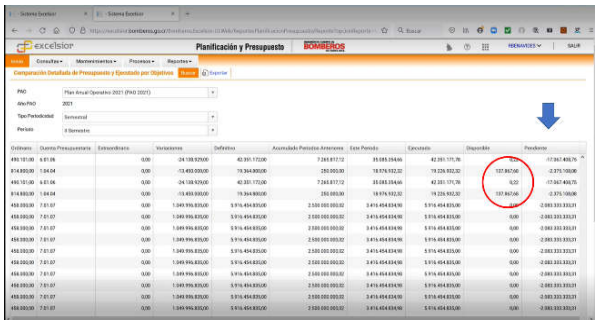
Se aplica un plan de infraestructura tecnológica. Existen prácticas de control para la gestión de respaldos y restauración.

X.3 Inconsistencias en sistemas de información

Condiciones

a. <u>En la evaluación del sistema Excelsior se identifica:</u>

- ✓ En el módulo de Planificación y Presupuesto se muestran unos saldos que no corresponden de acuerdo con los datos de Enterprise.



Causa

Diferencia en la generación del reporte cuando se despliega la pantalla en los registros entre las partidas.

Efecto

Podría incurrir en errores en la toma de decisiones sobre los datos mostrados en el sistema.

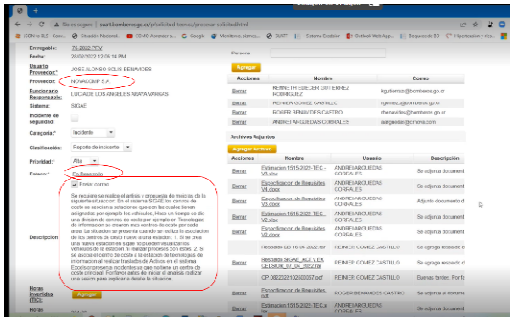
Recomendación

Considerar la mejora en el reporte para efectos de visualización de los mismos datos en el módulo de Planificación y Presupuesto.

b. <u>El módulo de Gestión de Activos</u>

- ✓ Presenta errores que están siendo valorados por el proveedor sobre asociación de centros de costos nuevo a una estación desde el sistema SIGAE. Presentándose una asociación no correcta.

  Se identifica un suatt para la atención de lo identificado. De acuerdo con la evidencia revisada se encuentran en pruebas técnicas. Ver recorte:



Causa

Se hizo evaluación de lo identificado por el área y se atiende por medio del suatt indicado.

Efecto

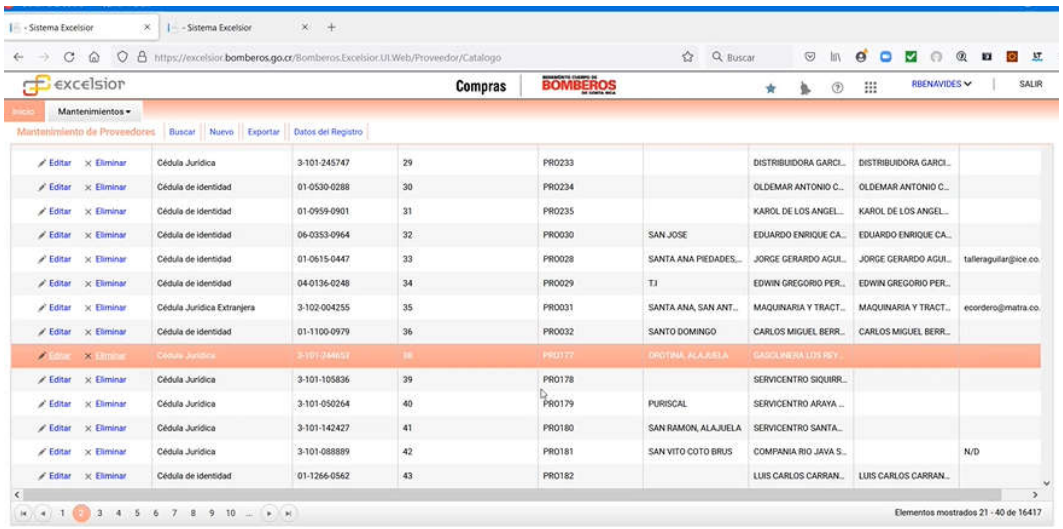
Podría existir activos que no se logren asignar a centros de costos o que no se logren identificar oportunamente.

Recomendación

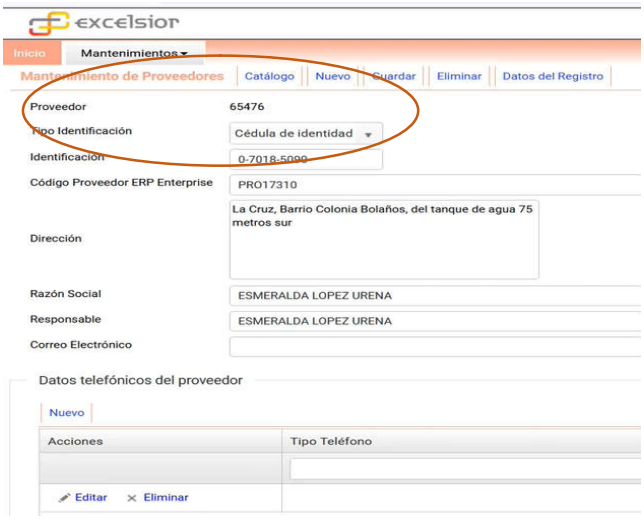
Al finalizar el proceso de corrección por parte del proveedor y las pruebas correspondientes, el área usuaria deberá revisar si quedara alguna inconsistencia en los registros o datos generados.

c. <u>El módulo de Compras</u>

✓ Se encontraron registros de proveedores faltantes por ejemplo el número 37 (datos de Excelsior). No hay pista de auditoría para la eliminación de registros.



✓ Se identifica error en el registro del número de identidad (cédula del proveedor).



Causa

Requerimientos de activación de las bitácoras, que no han solicitado el área usuaria y no se han generado corrección de errores en el registro de números de cédula PRO17310.

Efecto

La ausencia de bitácoras, en el caso de eliminación de proveedores, dificultaría el poder dar seguimiento y reconocer las responsabilidades de dicha situación.

Recomendación

Considerar la ausencia de las pistas de auditoría en el módulo de compras y dato erróneo en el registro de cédula de identidad identificado.

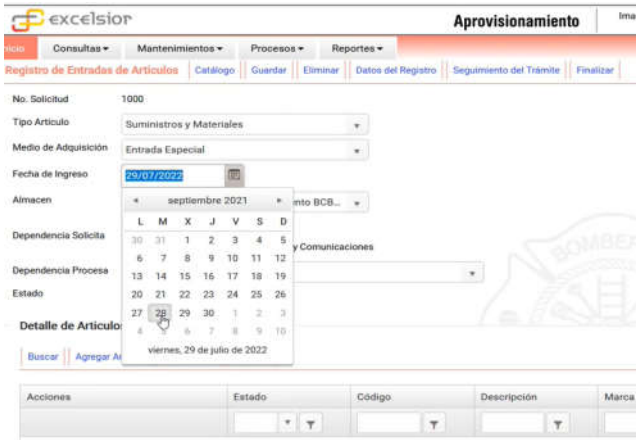
d. <u>El módulo de Aprovisionamiento</u>

✓ En el módulo de Aprovisionamiento, el sistema permite registrar el costo con valores negativos y al final genero un error de cálculo en el sistema (Overflow), tal como se muestra en la siguiente pantalla:

El valor del costo en el pedido permite valores negativos, al finalizar el cálculo da el error. Error de overflow:

"ExeAdmErr0019: ha ocurrido un error en la aplicación. Detalle tecnico: Arithmetic overflow erro converting numeric to data type numeric. The statement has beeb terminated".

✓ En el módulo de Aprovisionamiento, el sistema permite registrar entradas de artículos con fechas anteriores del periodo actual tal como el 28-set-21 cuyo registro fue afectado exitosamente, tal como se muestra en la siguiente pantalla:



✓ El sistema permite indicar la fecha de ingreso a una fecha anterior como fue el caso revisado:

Causa

Falta de alertas o control relativas al manejo de fechas de ingreso para la solicitud de ingreso de artículos.

Efecto

Podría generar información incorrecta en la solicitud de entrada de artículos.

Recomendaciones

Valorar cambiar el mensaje de error del overflow al idioma español, siendo comprensible la lectura al usuario o validador del sistema.

Considerar la flexibilidad de rango de fechas en el registro de la fecha de ingreso por parte del área usuaria y considerar una disminución del plazo de las fechas o alerta de control para rectificar en los casos necesarios.

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. Revisión de sistemas de información.

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, gestión de cambios y desarrollo de sistemas.

Se está en proceso de aplicar el procedimiento sobre 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 controles en la contratación administración de servicios, productos y sistemas de información.

Por medio de los contratos se hace la fiscalización del cumplimiento de las cláusulas.

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

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.

En el Comité de TI y los Órganos de Dirección se hace presentación de los resultados del cumplimiento del PAO, los procesos de TI y la atención a los servicios de información que se otorgan.

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, direccionar al área de atención y reportar a la Unidad de Planificación para el seguimiento.

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.

XII. Seguimiento de las recomendaciones de periodos anteriores

Se resume el cumplimiento de las recomendaciones emitidas en informes de periodos anteriores. En el periodo 2019 y 2020 se identifican 2 observaciones en proceso de atención, para los años anteriores fueron atendidas.

Año / Estado	Atendidas	En Proceso	Pendientes	N/A	**Total General**
2019	3	1			4
2020	2	1			3
Total	**5**	**2**			**7**

	Carta	Asunto	Estado		
			Atendido	En proceso	Se mantiene
XI.1	**2020**	**IX.1 Normativa sobre reglas en las direcciones de correo electrónico** **Riesgo Elevado**	☒	☐	☐

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.

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.

Comentario de la administración

- Inicialmente la Jefatura de TIC instruyo al encargado de correo la redacción de la política requerida para la mejora planteada.

Se desarrollo una Política para asignación y uso del correo electrónico. Además, se ajustó el procedimiento 4-03-03-027 "Gestión de Usuarios de Correo Electrónico" para que sea coherente con la política.

Comentario de la auditoría

Por medio del oficio CBCR-011230-2022-PLB-00062, del 24 de marzo de 2022, se da por atendidas la recomendación.

	Carta	Asunto	Estado		
			Atendido	En proceso	Se mantiene
XI.2	**2020**	**IX.2 Saltos en los consecutivos y duplicados en SICOF (1.4.6)** **Riesgo Elevado**	☐	☒	☐

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.

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

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

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

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

- La jefatura de TIC remite oficio CBCR-040709-2021-TIB-00935 “Propuesta de migración de tecnología del Sistema de Correspondencia Oficial - SICOF”.
- Actualmente mediante SUATT 4351-2021-TEC se le está dando tratamiento a la propuesta de desarrollo planteada.

Comentario de la auditoría

Se valida oficio CBCR-020763-2022-PLB-00094, para solicitar ampliación en el plazo de atención al 31/12/2022.

Se cuenta con un cronograma de trabajo que indica fecha de finalización para diciembre 2022.

	Carta	Asunto	Estado		
			Atendido	En proceso	Se mantiene
XI.3	**2019**	**IX.1Actualización y aplicación del proceso de continuidad (1.4.7)** **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 administración

- La jefatura de TIC remite oficio CBCR-040709-2021-TIB-00935 "Propuesta de migración de tecnología del Sistema de Correspondencia Oficial - SICOF".
- Actualmente mediante SUATT 4351-2021-TEC se le está dando tratamiento a la propuesta de desarrollo planteada.

Comentario de la auditoría

Por medio del oficio CBCR-025736-2022-PLB-00110, se solicitó ampliación para el cumplimiento del plan de acción al 31/12/2022.

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

Conclusiones

1. Se deben seguir aportando recursos para atender la implementación de las normas de acatamiento del MICITT que le corresponde al BCBCR.

2. Se deben revisar las necesidades y cierre de brechas para cubrir temas de ciberseguridad y continuidad con posibles estrategias de Grupo, que por recorte de presupuesto no puedan ser atendidas directamente por BCBCR.

3. Se requiere que áreas de negocio y la Auditoría Interna conozcan, participen y se involucren en la implementación de las normas del MICITT de acuerdo con las responsabilidades de cada área.

4. 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 brechas y serán de fortalecimiento a las normas del MICITT respecto a:

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

Anexo # 1
Herramientas informáticas

Herramientas informáticas que utiliza el Cuerpo de Bomberos de Costa Rica 2021-2022								
N°	**Identificador**	**Nombre**	**Desarrollo a medida**	**Comprado y adaptado**	**Alquilado a un tercero**	**APP**	**VISOR***	**BackEND****
1	SICOF	Sistema Institucional de Correo Formal	X					
2	SIGSA	Sistema Integrado para la Gestión de Seguridad y Accesos	X					
3	SIGAE	Sistema de Información Geográfica para la Atención de Emergencias	X					
4	SIBA	Sistema Integrado de Bitácoras	X					
5	SUATT	Sistema Único de Atención a Trámites de Tecnologías	X					
6	SIABO	Sistema de la Academia de Bomberos	X					
7	MIF	Módulo Integrado de Facturación	X					
8	Evolution	Sistema de Flotilla vehicular		X				
9	Enterprise	Sistema Financiero administrativo - ERP		X				
10	Excelsior	Sistema Administrativo Financiero	X					
11	MPE	Módulo de Personal Externo	X					
12	PASE	Plataforma de Atención y Servicio de la Academia	X					
13	SPEIHS	Sistema para el estudio integral de hidrantes	X					
14	SIMAV	Sistema Integrado de Mantenimiento Vehicular	X					
15	SWS	Sistema de Factura electrónica			X			
16	CGP	Consola SINPE - Sistema de transferencias SINPE			X			
17	VITAL-E	Sistema de Expediente electrónico médico			X			
18	MIDAS	Sistema de pistas de auditoría		X				
19	ACADEMICO	Administración de un Centro Académico			X			
20	GVT	Sistema de Gestión Virtual del Talento			X			
21	Moodle	Aula virtual de la Academia			X			
22	Entrega de Servicio	Entrega de servicio	X					
23	BITAB	Bitácora de Bomberos				X		

Herramientas informáticas que utiliza el Cuerpo de Bomberos de Costa Rica 2021-2022								
N°	**Identificador**	**Nombre**	**Desarrollo a medida**	**Comprado y adaptado**	**Alquilado a un tercero**	**APP**	**VISOR***	**BackEND****
24	DTR	Backend DTR						X
25	DTR	Datos en Tiempo Real				X		
26	Marcas	Registro de entrada y salidas de las estaciones				X		
27	BIVUB	Backend BIVUB						X
28	BIVUB	Bitácora de Vuelo de Bomberos				X		
29	CCBICA	Backend CCBICA						X
30	CCBICA	App Realidad Aumentada CCBICA				X		
31	F5	BackEnd BomberosCR-F5						X
32	F5	Consulta de Unidades				X		
33	BomberosCR	Bomberos Costa Rica				X		
34	INSIDE	Bomberos INSIDE					X	
35	SIAA	Servidor de Archivos					X	
36	OWA	Outlook Web					X	
37	IDEB	Infraestructura de Datos Espaciales de Bomberos					X	
38	SIDEB	Sistema de Infraestructura de Datos Espaciales de Bomberos					X	
39	SPADA	Sistema para direcciones de apoyo					X	

*Corresponde a herramientas que solo permiten la consulta de información.

**Son herramientas para la configuración de datos y/o parámetros de algunas APP y a las que solo tienen acceso los dueños y Administradores de las APP.

Anexo # 2

Resultados de la inspección in situ de estaciones de BCBCR

Validación de prácticas de seguridad para la gestión de equipos e infraestructura tecnológica

Estación	Resultados
Estación Metropolitana Sur	1. Se identifica equipo sin antivirus ubicado en la recepción, nombre de equipo "ESCENTRAL-RECEP" 2. No se evidencio visitas periódicas para mantenimiento preventivo a los equipos y dispositivos 3. Tabletas sin antivirus 4. Se permite el uso de dispositivos USB, son personales y no están encriptados
Estación Metropolitana Norte	1. Se permite el uso de dispositivos USB, son personales y no están encriptados 2. Caídas regulares de los sistemas por débil conexión de las redes 3. Equipo access point ubicado en sitio que genera pérdida de señal 4. En la vista de descarga, escritorio y papelera se identificó bastantes archivos que pueden estar expuestos a seguridad por no estar eliminados o en subcarpetas dentro de la unidad del disco 5. No se evidencio visitas periódicas para mantenimiento preventivo a los equipos y dispositivos 6. Tabletas sin antivirus 7. Equipo tiene Office 365 por ser parte del Fideicomiso
Estación de Desamparados	1. Se permite el uso de dispositivos USB 2. Servicio de internet adquirido por los colaboradores 3. No se evidencio visitas periódicas para mantenimiento preventivo a los equipos y dispositivos 4. Tableta sin antivirus
Estación de Guadalupe	1. Se permite el uso de dispositivos USB 2. Equipo sin antivirus (HP) y con windows 7 profesional para uso de voluntarios. (Versión desactualizada) 3. Cableado estructurado no cumple las buenas prácticas de control para comunicaciones, telefonía y electricidad 4. No se evidencio visitas periódicas para mantenimiento preventivo a los equipos y dispositivos 5. Tabletas sin antivirus
Estación de Tibás	1. Se permite el uso de dispositivos USB, son personales y no están encriptados 2. Servicio de internet es de 10 GB 3. Equipo access point ubicado es sitio que genera pérdida de señal 4. En la vista de descarga, escritorio y papelera se identificó archivos que pueden estar expuestos a seguridad por no estar eliminados o en subcarpetas dentro de la unidad del disco. 5. No se evidencio visitas periódicas para mantenimiento preventivo a los equipos y dispositivos 6. Tabletas sin antivirus
Estación de San Ramón	1. Se permite el uso de dispositivos USB 2. Servicio de internet es de 10 GB y por cable 3. No se evidencio visitas periódicas para mantenimiento preventivo a los equipos y dispositivos 4. Tableta sin antivirus
Estación de Belén	1. Se permite el uso de dispositivos USB, son personales y no están encriptados 2. Servicio de internet es de 10 GB 3. Equipo access point ubicado es sitio que presenta pérdida de señal 4. En la vista de descarga, escritorio y papelera se identificó archivos que pueden estar expuestos a seguridad por no estar eliminados o en subcarpetas dentro de la unidad del disco 5. No se evidencio visitas periódicas para mantenimiento preventivo a los equipos y dispositivos 6. Tableta sin antivirus

Resultados de la inspección in situ de estaciones de BCBCR	
Validación de prácticas de seguridad para la gestión de equipos e infraestructura tecnológica	
Estación	**Resultados**
Estación de Santo Domingo	1. Se permite el uso de dispositivos USB, son personales y no están encriptados 2. Servicio de internet es de 10 GB 3. Regleta conecta a la computadora, impresora, radios de comunicación, cargadores de celulares, parlantes, entre otros 4. En la vista de descarga, escritorio y papelera se identificó archivos que pueden estar expuestos a seguridad por no estar eliminados o en subcarpetas dentro de la unidad del disco 5. Cableado estructurado no cumple las buenas prácticas de control para comunicaciones, telefonía y electricidad 6. No se evidencio visitas periódicas para mantenimiento preventivo a los equipos y dispositivos 7. Tabletas sin antivirus
Estación de San Pedro de Poas	1. Se permite el uso de dispositivos USB 2. No se evidencio visitas periódicas para mantenimiento preventivo a los equipos y dispositivos 3. Tabletas sin antivirus
Estación de Grecia	1. Se permite el uso de dispositivos USB 2. No se evidencio visitas periódicas para mantenimiento preventivo a los equipos y dispositivos 3. Tableta sin antivirus 4, Equipo principal estaba en F5 para revisión, motivo por el cual no se hace la validación de controles al equipo mencionado

Cuadro # 1

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

Capítulo	Sub-capítulo	#	Pregunta	Pts. Totales	Cumplimiento	Puntaje obtenido	Comentario por el no cumplimiento
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%	
		2	¿Se divulga este marco estratégico al personal de la empresa?	1.47%	SI	1.47%	
	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%	
	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%	
	1.4 Gestión de la Seguridad de la Información	**5**	¿Posee la empresa una política de seguridad de información?	1.47%	SI	1.47%	
		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%	Falta fortalecer el sistema de monitoreo de la seguridad de forma continua. Se debe aplicar la clasificación de los activos de información.
		7	¿Poseen controles de acceso, y planes para la continuación de las operaciones en caso de presentarse una contingencia?	1.47%	PARCIAL ALTO	0.98%	Falta la aplicación de pruebas de continuidad. Se está en proceso de atención el plan de acción sobre informe de vulnerabilidades.
	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%	Se está en proceso de la aplicación práctica de la clasificación de la información.
		9	¿Se mantienen documentadas y actualizadas las responsabilidades del personal de la organización y de terceros relacionados?	1.47%	SI	1.47%	
	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%	
		11	¿Se capacita al personal sobre sus responsabilidades en materia de seguridad, confidencialidad y riesgos de TI?	1.47%	SI	1.47%	

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

Capítulo	Sub-capítulo	#	Pregunta	Pts. Totales	Cumplimiento	Puntaje obtenido	Comentario por el no cumplimiento
		12	¿Existen implementadas medidas de seguridad relacionadas con las operaciones de los recursos de TI?	1.47%	SI	1.47%	
		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%	
		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%	
		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%	
	1.4.3 Seguridad Física y Ambiental	**16**	¿La ubicación física es segura de los recursos de TI?	1.47%	PARCIAL BAJO	0.49%	Se identifica observación debilidades de seguridad física en visita a estaciones
		17	¿Se cuentan con políticas y procedimientos para el ingreso y salida de equipos de la organización?	1.47%	SI	1.47%	
		18	¿Los requerimientos de seguridad fueron considerados en la implementación y mantenimiento de software e infraestructura de TI?	1.47%	PARCIAL BAJO	0.49%	Se identifica observación sobre seguridad en la infraestructura de comunicaciones en visita a las estaciones
	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%	Se está en proceso de atención el plan de acción sobre informe de vulnerabilidades
		20	¿Se cuenta con procedimientos para proteger la información almacenada en cualquier tipo de medio físico?	1.47%	PARCIAL BAJO	0.49%	Se identifica observación sobre seguridad en la infraestructura de comunicaciones en visita a las estaciones
		21	¿Se han establecido medidas preventivas, detectivas y correctivas con respecto a software "malicioso" o virus?	1.47%	PARCIAL ALTO	0.98%	Se identifica observación sobre seguridad en la infraestructura de comunicaciones en visita a las estaciones

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%	
		23	¿Se ha definido la propiedad, custodia y responsabilidad sobre los recursos de TI?	1.47%	SI	1.47%	
		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%	
		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%	
		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%	
	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%	
		28	¿Se cuenta con procedimientos definidos para el mantenimiento y puesta en producción del software?	1.47%	PARCIAL BAJO	0.49%	Se encuentra observación del SICOF en proceso de atención.
	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%	
		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. Se identifica oportunidad del periodo en evaluación sobre redundancia y enlaces por continuidad de negocio.
	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%	SI	1.47%	
	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%	SI	1.47%	
	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%	SI	1.47%	

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%	
	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%	
	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%	
	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%	
		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%	
	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%	
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%	SI	1.47%	
		41	¿Existen políticas sobre la justificación, autorización y documentación de solicitudes de implementación o mantenimiento de TI?	1.47%	SI	1.47%	
		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%	
		43	¿Se asignan líderes responsables a cada proyecto de TI?	1.47%	SI	1.47%	

Capítulo	Sub-capítulo	#	Pregunta	Pts. Totales	Cumplimiento	Puntaje obtenido	Ref
	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%	SI	1.47%	
		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%	
		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%	
		47	¿Se controla las distintas versiones de los programas que se generan como parte de su mantenimiento?	1.47%	SI	1.47%	
	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%	
	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%	
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%	
		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%	
		52	¿Se revisan periódicamente los acuerdos de servicios incluyendo los contratos a terceros?	1.47%	SI	1.47%	
	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%	
		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%	PARCIAL BAJO	0.49%	Se identifica observación inconsistencias en registro de datos en sistemas de información
		55	¿Existen controles sobre la composición y	1.47%	SI	1.47%	

Capítulo	Sub-capítulo	#	Pregunta	Pts. Totales	Cumplimiento	Puntaje obtenido	Ref
			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?				
		56	¿Se brinda el soporte adecuado a los equipos tanto principales como periféricos?	1.47%	PARCIAL BAJO	0.49%	Se identifica observación inconsistencias en registro de datos en sistemas de información
	4.3 Administración de los datos	**57**	¿Poseen rutinas de respaldos, se controlan los procesos de restauración?	1.47%	SI	1.47%	
		58	¿Existen parámetros definidos para las pruebas de sistemas (tales como de entrada, valores mínimos y máximos, etc.)?	1.47%	SI	1.47%	
		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%	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%	
	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%	
	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%	

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%	
		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%	
		65	¿Se determinan las responsabilidades del personal a cargo del seguimiento de los procesos de TI?	1.47%	SI	1.47%	
	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%	
		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%	
	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%	
ESTADO GENERAL:						90.19%	