Benemérito Cuerpo de Bomberos de Costa Rica
(BCBCR)

Informe de auditoría externa de Sistemas de Información del Benemérito Cuerpo de Bomberos de Costa Rica

Al 31de diciembre de 2022

Benemérito Cuerpo de Bomberos de Costa Rica
(BCBCR)

Índice de contenido

	Página
Anexo A	- 6 -
I. Resumen ejecutivo	- 6 -
II. Delimitaciones	- 7 -
III. Limitaciones	- 8 -
IV. Metodología de evaluación	- 8 -
V. Conclusiones generales del periodo 2022	- 11 -
VI. Mapa de calor de los riesgos evidenciados al cierre de este informe	- 12 -
VII. Actividades evaluadas	- 13 -
A. Gestión de Tecnologías de Información	- 13 -
B. Gestión de prácticas de seguridad de la información	- 14 -
C. Gestión de sistemas la información	- 18 -
D. Gestión de la continuidad de operaciones	- 25 -
E. Seguimiento a recomendaciones anteriores	- 25 -
F. Conclusiones	- 34 -

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 2023

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

ASUNTO: INFORME DE AUDITORÍA EXTERNA SOBRE LOS SISTEMAS DE INFORMACIÓN

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

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

Nuestra responsabilidad sobre este informe de la auditoría externa sobre los sistemas de información al 30 de setiembre de 2023 se extiende hasta el 30 de setiembre de 2023. 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.

Atentamente,

FABIAN ZAMORA AZOFEIFA (FIRMA)

Firmado digitalmente por FABIAN ZAMORA AZOFEIFA (FIRMA)
Fecha: 2023.10.12 10:56:49 -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 que no son auditoría ni revisión de información financiera histórica, sobre la eficacia y efectividad de las políticas, procedimientos y controles 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. 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 se 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, por el año terminado el 31 de diciembre de 2022, con el fin de emitir una opinión de auditoría sobre 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.

Nuestra responsabilidad es expresar opinión sobre 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 MICITT (Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones), siendo las Normas Técnicas para la gestión y el control de las tecnologías de la información con base en el resultado del Anexo A.

En el Anexo A se detallan las conclusiones de control interno y exposición al riesgo con el fin de validar el cumplimiento de las medidas de control sobre el acatamiento de las normas.

Se realizó el trabajo de acuerdo con la Norma Internacional de Encargos de Aseguramiento, (NIEA) 3000 (Revisada), "Encargos de aseguramiento distintos de la auditoría o de la revisión de información financiera histórica" y con base en la Circular 32-2022 "Lineamientos para Realizar un Encargo de Aseguramiento distinto de la Auditoría o de la Revisión de la Información Financiera Histórica según la NIEA 3000" del Colegio de Contadores Públicos de Costa Rica.

Dicha norma requiere 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:

Herramientas informáticas que utiliza el Cuerpo de Bomberos de Costa Rica 2022-2023								
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					

Herramientas informáticas que utiliza el Cuerpo de Bomberos de Costa Rica 2022-2023								
N°	**Identificador**	**Nombre**	**Desarrollo a medida**	**Comprado y adaptado**	**Alquilado a un tercero**	**APP**	**VISOR***	**BackEND****
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		
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.

B. Expresar una opinión sobre el cumplimiento de la normativa aplicable a los sistemas de Información del BCBCR.

C. Evaluar y obtener entendimiento de la estructura de control interno de los Sistemas de Información,

D. 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.

E. 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.

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

G. 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.

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

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

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

K. 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 valoración.

En consecuencia, y en nuestra opinión, los procedimientos y controles de acuerdo con las Normas, son eficaces y efectivos sobre 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 2022, en todos los aspectos importantes, excepto por lo indicado en los factores evaluados en B.1, B.2, C.1, C.2, C.3, E.1 y E.2.

"Manifiesto que estoy facultado(a) de conformidad con el artículo 4 de la Ley N.º 1038 para emitir este informe y declaro que soy independiente al cumplir con lo estipulado en el artículo 9 de la Ley N° 1038, los artículos 20 y 21 del Reglamento de la misma Ley, y los requerimientos de independencia y demás requerimientos de ética establecidos en el Código de Ética Profesional emitido por el Colegio de Contadores Públicos de Costa Rica".

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

Restricción del uso del informe y su contenido

Este reporte del contador público independiente sobre compromisos de seguridad que no son auditoría ni revisión de información financiera histórica, sobre la evaluación de la eficacia y efectividad de los sistemas de información, ha sido preparado únicamente para el uso de la Administración de Benemérito Cuerpo de Bomberos de Costa Rica (BCBCR) únicamente para el cumplimiento de la contratación y no para ningún otro propósito ni contexto.

Nuestro informe no deberá ser considerado apto para ser utilizado o mencionado por alguna parte que desee adquirir derechos frente a nosotros, salvo el Benemérito Cuerpo de Bomberos de Costa Rica (BCBCR), para cualquier propósito o contexto. Cualquier parte, salvo Benemérito Cuerpo de Bomberos de Costa Rica (BCBCR) que obtenga acceso a nuestro informe o a una copia de este y decida mencionar nuestro informe (o una parte de este) lo hará bajo su propia responsabilidad. Dentro del alcance máximo permitido por la ley, no aceptamos ni asumimos responsabilidad alguna y negamos cualquier obligación frente a terceros, salvo Benemérito Cuerpo de Bomberos de Costa Rica (BCBCR), en relación con el trabajo efectuado, con el presente reporte del contador público independiente sobre compromisos de seguridad o con las conclusiones emitidas.

Liberamos nuestro informe a Benemérito Cuerpo de Bomberos de Costa Rica (BCBCR) en el entendido de que no podrá copiarse, referirse ni revelarse una parte o la totalidad del informe, excepto para los efectos internos de Benemérito Cuerpo de Bomberos de Costa Rica (BCBCR) sin nuestro consentimiento previo y por escrito.

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.

FABIAN ZAMORA AZOFEIFA (FIRMA)

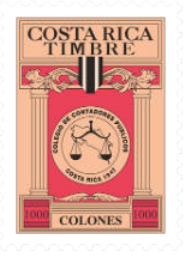
Firmado digitalmente por FABIAN ZAMORA AZOFEIFA (FIRMA)
Fecha: 2023.10.12 10:57:34 -06'00'

Dictamen firmado por
Fabián Zamora Azofeifa N° 2186
Pol. 0116 FIG 7 V.30-9-2024
Timbre Ley 6663 ¢1.000
Adherido al original

Nombre del CPA: FABIAN ZAMORA AZOFEIFA
Carné: 2186
Cédula: 3008?0450
Nombre del Cliente: Benemérito Cuerpo de Bomberos de Costa Rica
Identificación del cliente: 3007547060
Dirigido a: Benemérito Cuerpo de Bomberos de Costa Rica
Fecha: 12-10-2023 10:45:18 AM
Tipo de trabajo: Informe de auditoria externa de 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



Código de Timbre: CPA-1000-7604

Anexo A

Benemérito Cuerpo de Bomberos de Costa Rica
(BCBCR)

Informe de auditoría externa sobre la eficacia y efectividad de sistemas de información del Benemérito Cuerpo de Bomberos de Costa Rica

Al 31 de diciembre de 2022

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 avances con la Auditoría Interna, que es quien hace la contratación de los servicios.

La Contraloría General de la República 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 de 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 de 2007, a partir del 1° de enero de 2022 …"

Actualmente las Normas Técnicas para la gestión y el control de las tecnologías de la información 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 de 2022), las cuales están en proceso de implementación y en tiempo hasta el 31 de diciembre de 2023, por medio de CBCR-038272-2022-DOB-00679, con fecha del 28/09/2022 se presenta la propuesta del Marco de gestión para la seguridad de la información del Cuerpo de Bomberos.

En alcance consideró la visita a 8 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.

Se realizaron evaluaciones a sistemas, aplicativos y herramientas informáticas que son detalladas en el alcance de la auditoría. Así mismo, el seguimiento a las recomendaciones del informe del periodo 2021.

Se presenta un resumen de lo comunicado en el estudio:

Recomendaciones 2022:

Año	Ref.	Recomendaciones	Nivel de cumplimiento	Impacto	Frecuencia	Categoría de riesgo
2022	B.1	Debilidades de seguridad física en equipos de las estaciones	Cumplimiento parcial bajo	Serio	Frecuente	Normal
2022	B.2	Debilidades de seguridad de la información en equipos de las estaciones	Cumplimiento parcial bajo	Serio	Frecuente	Normal
2022	C.1	Manuales de usuarios desactualizados y carentes de validaciones	Cumplimiento parcial bajo	Serio	Frecuente	Elevado
2022	C.2	Adjuntar archivos en el sistema SUATT	Cumplimiento parcial alto	Moderado	Frecuente	Normal
2022	C.3	Solicitudes en el sistema SPEIHS	Cumplimiento parcial alto	Moderado	Frecuente	Normal
2022	C.4	Cantidad de intentos fallidos para el ingreso de contraseñas	Cumplimiento parcial bajo	Moderado	Alta	Elevado

Seguimiento de recomendaciones de periodos anteriores

Año	Ref.	Recomendaciones	Nivel de cumplimiento	Impacto	Frecuencia	Categoría de riesgo
2021	E.1	X.3 Inconsistencias en sistemas de información (4.2)	Cumplimiento parcial bajo	Serio	Frecuente	Elevado
2019	E.2	IX.1 Actualización y aplicación del proceso de continuidad (1.4.7)	Cumplimiento parcial bajo	Serio	Frecuente	Elevado

De acuerdo con el cuadro anterior para las recomendaciones han presentado las siguientes prórrogas:

X.3 Inconsistencias en sistemas de información (4.2), una prórroga con vencimiento al 31 de diciembre de 2023.

IX.1 Actualización y aplicación del proceso de continuidad (1.4.7), vencimiento al 31 de diciembre de 2023. Se han presentado 3 prórrogas con vencimiento al 31/12/2022, 30/09/2023 y al 31/12/2023.

II. Delimitaciones

Actualmente la norma vigente 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) y en proceso de implementación hasta el 31 de diciembre de 2023, llamadas las Normas Técnicas para la gestión y el control de las tecnologías de la información.

El nivel de cumplimiento y capacidad de COBIT no se encuentra evaluado en sus 40 procesos, al no estar implementado en la gestión de procesos de tecnología por lo que en esta auditoría se podrían utilizar 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 2022, con la presentación de evidencia al 30 de setiembre de 2023.

III. Limitaciones

Durante el proceso de la auditoría se identifica esta información de los sistemas que no logre ser revisada a la fecha del informe.

SUATT:

1. Reporte de usuarios que utilizan la mesa de ayuda.

SIMAV:

2. Pantallas sobre la funcionalidad del sistema SIMAV desde la perspectiva de un usuario.

DTR:

3. Listado del personal que utiliza el sistema.

La auditoría se llevó a cabo de acuerdo con las normas y principios de auditoría aplicables y hemos obtenido suficiente evidencia por medio de las pruebas de auditoría.

IV. Metodología de evaluación

La auditoría se ejecuta en cumplimiento de la Norma Internacional de Auditoría 315 "Identificación y valoración de los riesgos de incorrección material mediante el conocimiento de la entidad y su entorno", la Norma Internacional de Auditoría 330 "Procedimientos del auditor en respuesta a los riesgos evaluados", al estar derogadas las Normas Técnicas de la Contraloría General de la República y la norma del MICITT vigente en proceso de implementación.

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

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

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

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

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.

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

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

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 2023.
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).

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				
		Muy baja	**Baja**	**Frecuente**	**Alta**	**Muy alta**
Impacto	**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.

V. Conclusiones generales del periodo 2022

En cumplimiento con la NIA 260, “Comunicaciones de asuntos de auditoría con los encargados del gobierno corporativo”, el auditor tiene la responsabilidad de comunicar en una auditoría de estados financieros los hechos observados relacionados con los riesgos de TI y negocio que gestiona actualmente la administración y que son significativos y relevantes en relación con la responsabilidad de supervisión del proceso de información financiera.

Recomendaciones 2022

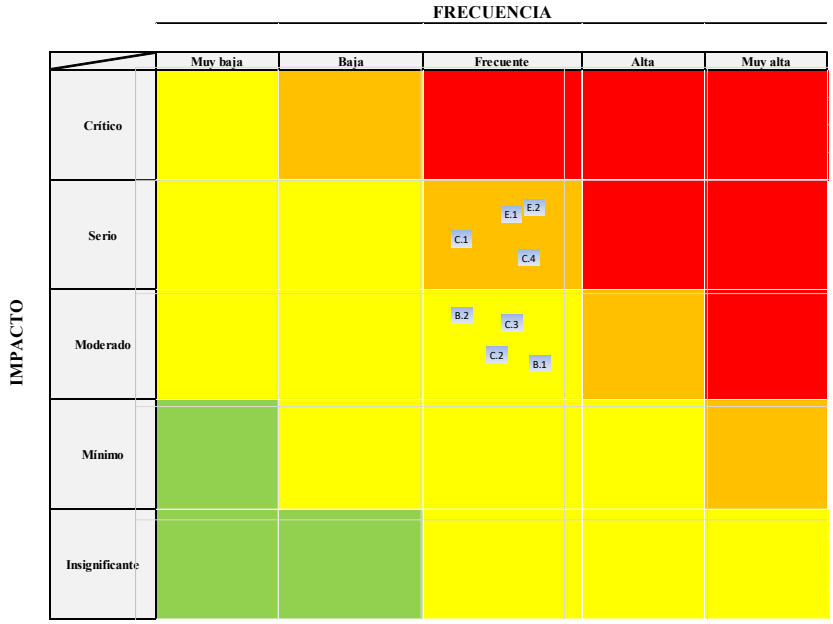
Año	Ref.	Recomendaciones	Nivel de cumplimiento	Impacto	Frecuencia	Categoría de riesgo
2022	B.1	Debilidades de seguridad física en equipos de las estaciones	Cumplimiento parcial bajo	Serio	Frecuente	Normal
2022	B.2	Debilidades de seguridad de la información en equipos de las estaciones	Cumplimiento parcial bajo	Serio	Frecuente	Normal
2022	C.1	Manuales de usuarios desactualizados y carentes de validaciones	Cumplimiento parcial bajo	Serio	Frecuente	Elevado
2022	C.2	Adjuntar archivos en el sistema SUATT	Cumplimiento parcial alto	Moderado	Frecuente	Normal
2022	C.3	Solicitudes en el sistema SPEIHS	Cumplimiento parcial alto	Moderado	Frecuente	Normal
2022	C.4	Cantidad de intentos fallidos para el ingreso de contraseñas	Cumplimiento parcial bajo	Moderado	Alta	Elevado

Seguimiento de las recomendaciones del periodo 2021 y 2019

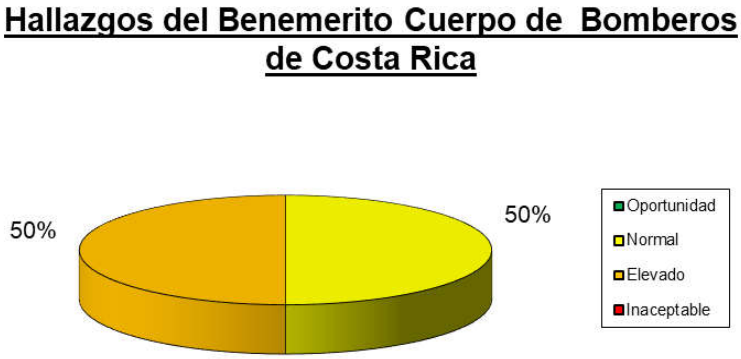
Año	Ref.	Recomendaciones	Nivel de cumplimiento	Impacto	Frecuencia	Categoría de riesgo
2021	E.1	X.3 Inconsistencias en sistemas de información (4.2)	Cumplimiento parcial bajo	Serio	Frecuente	Elevado
2019	E.2	IX.1 Actualización y aplicación del proceso de continuidad (1.4.7)	Cumplimiento parcial bajo	Serio	Frecuente	Elevado

VI. 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 observaciones sobre la auditoría de sistemas de información.



Como resultado de la revisión se comunican 8 oportunidades de mejora que son clasificadas en dos categorías de riesgo ubicadas en las áreas revisadas en la siguiente forma:

- 4 de riesgo elevado
- 4 de riesgo normal

VII. Actividades evaluadas

A. Gestión de Tecnologías de Información

En la revisión de estas actividades se verificó lo siguiente:

1. Plan estratégico de TI.
2. Plan operativo de TI.
3. Estructura organizacional de TI.
4. Administración de proyectos.
5. Contratos de servicios de TI.
6. Acuerdos de niveles de servicios entre las áreas de servicio y proveedores.
7. Monitoreo y evaluación del control interno de TI.
8. Planes de capacitación.
9. Informes de labores sobre la gestión de TI.
10. Actas del Comité de TI.
11. Administración de riesgos institucionales y TI.
12. Cumplimiento del marco regulatorio interno o externo.
13. Gestión de proveedores.
14. Plan de infraestructura.
15. Implementación de las normas técnicas de tecnología de información.

De acuerdo con el resultado de las pruebas realizadas no evidenciamos situaciones que nos hagan creer que no se cumple con los requerimientos de seguridad y control.

B. Gestión de prácticas de seguridad de la información

En la revisión de estas actividades se verificó lo siguiente:

1. Políticas, procedimientos, herramientas y metodologías en la administración de la seguridad de la información.
2. Evaluaciones internas a la seguridad de la información de acuerdo con el plan de trabajo.
3. Aplicación de procedimientos de encriptación de la información.
4. Gestión de roles y perfiles de acceso.
5. Aplicación de pruebas de vulnerabilidad.
6. Planes de acción para la implementación de mejoras o debilidades de seguridad.
7. Gestión en la atención de incidentes.
8. Revisiones sobre seguridad de la información.
9. Revisión e implementación de las alertas técnicas del MICITT.
10. Seguridad física y lógica a Estaciones de Bomberos.

Se identifican las siguientes observaciones de mejora:

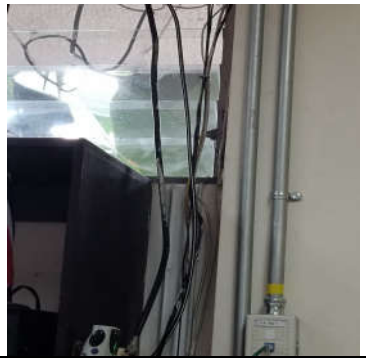
B.1 Debilidades de seguridad física en equipos de las estaciones

Normal

Condición

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

- Desamparados
- Guadalupe
- Santo Domingo
- Tres Ríos

Resultados de la inspección in situ de estaciones de BCBCR	
Validación de prácticas de seguridad física a equipos e infraestructura tecnológica	
Estación	**Resultados**
1. Estación de Desamparados	1. Saturación del cableado eléctrico externo al tomacorriente, donde se conectan los equipos electrónicos.
2. Estación de Guadalupe	1. En el mes de octubre del 2022 la estación recibe mantenimiento y mejora en el cableado de voz y datos, no obstante, el tendido de cable para comunicaciones, telefonía y electricidad de ingreso al edificio de la estación no se encuentra de acuerdo con las buenas prácticas de seguridad.  
3. Estación de Santo Domingo	1. En el mes de julio de 2023, la estación recibe por parte de la empresa NETCOM actividades de mantenimiento, en donde se ordenó el cableado de voz y datos, además mejoras en la red. En la visita in situ se identifican puntos de saturación del cableado eléctrico externo a la toma, donde se conectan los equipos electrónicos. 

Criterio

Las Normas Técnicas para la gestión y el control de las tecnologías de la información, en el proceso 11, Seguridad y Ciberseguridad, menciona:

"La Institución debe propiciar un ambiente seguro, considerando la seguridad física, lógica y ambiental como un componente básico en el esquema de protección requerido para prevenir el acceso físico no autorizado, daños e interferencia a la información y los activos de información de la institución".

Causa

Debilidades en las medidas de seguridad físicas para la instalación de los equipos electrónicos.

Efecto

Exposición a un corto circuito y daño en equipos.

Recomendación

Establecer un plan de visitas anual para verificar las condiciones físicas relativas a las instalaciones eléctricas, con el objetivo de velar por las medidas de seguridad integrales de los equipos e instalaciones.

B.2 Debilidades de seguridad de la información en equipos de las estaciones

Normal

Condición

Se identifican las siguientes debilidades:

Antivirus sin instalar y desactualizado en tabletas en las siguientes estaciones:

- Metro Sur.
- Tibás.

Equipos con versiones de Windows sin soporte:

- Metro Sur, equipo con Windows 7.

Equipos lentos y equipos con obsolescencia tecnológica:

- Metro Sur.
- Tres Ríos.
- Guadalupe.

Resultados de la inspección in situ de estaciones de BCBCR	
Validación de prácticas de seguridad de equipos e infraestructura tecnológica	
Estación	**Resultados**
1. Estación Metropolitana Sur	1. Tablet no tiene instalado el antivirus. 2. Equipo de con Windows 7. 3. Equipo portátil en los Rill con un nivel de obsolescencia tecnológica.
2. Estación de Guadalupe	1. Problemas de equipo de Jefatura, tienen trabajo atrasado de 2 semanas. 2. Clave adherida al equipo.
3. Estación de Tibás	1. Tablet no tiene actualizado el antivirus.
4. Estación de Tres Ríos	1. Equipo muy lento de la Jefatura de la Estación y no tiene tóner para las impresoras por lo que tienen que imprimir en la biblioteca de la comunidad.

Criterio

Las buenas prácticas para la gestión y el control de las tecnologías de la información, menciona:

"Los equipos de usuario final y portátiles utilizados en la organización deben contar con medidas de protección activas, como software antivirus actualizado y en funcionamiento, con el objetivo de prevenir y detectar amenazas de malware, virus y otras vulnerabilidades de seguridad".

Causas

Manipulación por los usuarios y la no confección de tiquetes para la atención expedita de los equipos.

Efecto

Pérdida de información y vulnerabilidades de seguridad.

Recomendaciones

Recordar el uso en la confección de tiquetes en las estaciones para la atención de los equipos en oportunidad de tiempo, para minimizar los riesgos en el deterioro de los equipos y exposición de vulnerabilidades.

Monitorear el estado de los equipos de usuarios final con regularidad para conocer el nivel de protección de los equipos y las debilidades encontradas sean informadas a la Administración para las medidas requeridas.

C. Gestión de sistemas la información

En la revisión de estas actividades se verificó lo siguiente:

1. Aplicación de políticas y metodologías para el desarrollo del ciclo de vida de sistemas.
2. Gestión en la atención de requerimientos de información.
3. Verificación de software licenciado.
4. Administración de cambios.
5. Automatización de sistemas de información.
6. Diagrama sobre la integración de sistemas.
7. Inventarios de equipos de cómputo.
8. Verificación del mantenimiento y desempeño de las bases de datos.
9. Contrato de mantenimiento a la base de datos.
10. Pistas de auditoría.
11. Validación de la funcionalidad de los sistemas y herramientas tecnológicas.
12. Gestión de activos de información.
13. Manuales técnicos y de usuario de las herramientas informáticas.
14. Obsolescencia tecnológica.

Se identifican las siguientes observaciones de mejora:

C.1 Manuales de usuarios desactualizados y carentes de validaciones

Elevado

Condición

Con respecto a los manuales de usuarios de las 39 herramientas tecnológicas, se recibieron 21 manuales.

Se ha evidenciado que los manuales de usuarios correspondientes a los sistemas implementados algunos presentan desactualización. Se observa la carencia de un formato uniforme para dichos manuales, así como la ausencia de una aprobación formal por parte del departamento de tecnologías de información, de acuerdo con el cumplimiento al “Instructivo para la Elaboración de Documentación en el BCBCR”.

Se detalla lista:

N°	Identificador	Nombre	Manual de Usuario	Aprobación/ Revisión	Actualización	Última actualización	Formato
1	**SICOF**	Sistema Institucional de Correo Formal	SI	**No tiene**	Kerling Lara	22/08/2023	SI
2	**SIGSA**	Sistema Integrado para la Gestión de Seguridad y Accesos	SI	Kattya Morales	Karol Mariela Espinoza Rojas	10/08/2023	SI
3	**SIGAE**	Sistema de Información Geográfica para la Atención de Emergencias	SI	Iveth Bolaños González	Karol Mariela Espinoza Rojas	11/08/2023	SI
4	**SIBA**	Sistema Integrado de Bitácoras	SI	**No tiene**	**NO**	14/06/2022	SI
5	**SUATT**	Sistema Único de Atención a Trámites de Tecnologías	SI	Iveth Bolaños González	Luis Alejandro Madrigal	10/08/2023	SI
6	**SIABO**	Sistema de la Academia de Bomberos	SI	**No tiene**	Luis Alejandro Madrigal	18/08/2023	SI
7	**MIF**	Módulo Integrado de Facturación	SI	**No tiene**	**NO**	2021	SI
8	**Evolution**	Sistema de Flotilla vehicular	SI	**No tiene**	**NO**	NO	**NO**
9	**Enterprise**	Sistema Financiero administrativo - ERP	SI	**No tiene**	**¿?**	NO	**NO**
10	**Excelsior**	Sistema Administrativo Financiero	SI	Planificación y Presupuesto esta realizado en el 2016 pero sin la revisión ni la aprobación correspondiente	Roger Benavides Castro	2015-2019	**SI**
11	**MPE**	Módulo de Personal Externo	SI	Rodolfo Alejandro Agüero Chaves	Iveth Bolaños González	11/09/2017	SI
12	**PASE**	Plataforma de Atención y Servicio de la Academia	SI	Alejandro Agüero Chaves y Daniel Redondo Zúñiga	Luis Alejandro Madrigal	16/08/2023	SI
13	**SPEIHS**	Sistema para el estudio integral de hidrantes	SI	Novacomp	Novacomp	06/04/2022	SI
14	**SIMAV**	Sistema Integrado de Mantenimiento Vehicular	SI	José Alonso Solís Benavides	José Alonso Solís Benavides	31/10/2018	SI
15	**SWS**	Sistema de Factura electrónica	SI	-	-	-	NO
16	**CGP**	Consola SINPE - Sistema de transferencias SINPE	SI	-	-	2019	NO
17	**VITAL-E**	Sistema de Expediente electrónico médico	-	-	-	-	-
18	**MIDAS**	Sistema de pistas de auditoría	SI	-	Novacomp	13/07/2022	SI
19	**ACADEMICO**	Administración de un Centro Académico	-	-	-	-	-
20	**GVT**	Sistema de Gestión Virtual del Talento	-	-	-	-	-
21	**Moodle**	Aula virtual de la Academia	-	-	-	-	-
22	**Entrega de Servicio**	Entrega de servicio	-	-	-	-	-

N°	Identificador	Nombre	Manual de Usuario	Aprobación/ Revisión	Actualización	Última actualización	Formato
23	**BITAB**	Bitácora de Bomberos	-	-	-	-	-
24	**DTR**	Backend DTR	-	-	-	-	-
25	**DTR**	Datos en Tiempo Real	-	-	-	-	-
26	**Marcas**	Registro de entrada y salidas de las estaciones	-	-	-	-	-
27	**BIVUB**	Backend BIVUB	-	-	-	-	-
28	**BIVUB**	Bitácora de Vuelo de Bomberos	-	-	-	-	-
29	**CCBICA**	Backend CCBICA	-	-	-	-	-
30	**CCBICA**	App Realidad Aumentada CCBICA	-	-	-	-	-
31	**F5**	BackEnd BomberosCR-F5	-	-	-	-	-
32	**F5**	Consulta de Unidades	-	-	-	-	-
33	**BomberosCR**	Bomberos Costa Rica	-	-	-	-	-
34	**INSIDE**	Bomberos INSIDE	SI	-	-	-	SI
35	**SIAA**	Servidor de Archivos	-	-	-	-	-
36	**OWA**	Outlook Web	-	-	-	-	-
37	**IDEB**	Infraestructura de Datos Espaciales de Bomberos	-	-	-	-	-
38	**SIDEB**	Sistema de Infraestructura de Datos Espaciales de Bomberos	-	-	-	-	-
39	**SPADA**	Sistema para direcciones de apoyo	-	-	-	-	-

Criterio

Las Normas Técnicas para la gestión y el control de las tecnologías de la información, en el proceso 10, Desarrollo, implementación y mantenimiento de sistemas de información, menciona:

"La Unidad de TI debe asegurar la disponibilidad de estándares para programación, gestión de la calidad del software en desarrollo o mantenimiento, cambios por excepción y/o emergencia, llevando un adecuado control de cambios y versiones."

Causa

La desactualización de los manuales y la falta de uniformidad podrían ser resultado de una falta de procesos claros para la revisión y actualización de la documentación. Asimismo, la carencia de una aprobación formal podría deberse a la falta de una estructura organizativa que apruebe la documentación antes de su distribución.

Efecto

La presencia de manuales de usuarios desactualizados y carentes de formato uniforme, así como la falta de aprobación formal, puede tener múltiples efectos negativos. Los usuarios podrían enfrentar dificultades al utilizar los sistemas de manera eficiente, lo que afectaría la productividad y eficacia en sus tareas y errores en la operación de los sistemas.

Recomendaciones

Implementar un proceso de revisión y actualización periódica de los manuales de usuarios, asegurando que se mantengan al día con los cambios en los sistemas y las mejores prácticas.

Cumplir con lo indicado "6-01-03-003 Instructivo para la Elaboración de Documentación en el BCBCR", respecto a la confección, actualización y validaciones respectivas para los manuales de usuario a las herramientas tecnológicas. Estas medidas contribuirán a mejorar la eficiencia operativa, reducir la posibilidad de errores y garantizar la calidad y confiabilidad de la documentación de sistemas.

C.2 Adjuntar archivos en el sistema SUATT

Normal

Condición

Se ha identificado en el sistema SUATT que, al crear una nueva solicitud de servicio, en la sección de adjuntar evidencia, no se ha implementado una restricción de tamaño para los archivos adjuntos, de igual forma se le consultó al usuario experto sobre el tema indicando que no se tiene marco normativo para el tamaño de los adjuntos.

Se está en la contratación del nuevo servicio *"Solicitud de gestión para la adquisición del Servicio de "Migración a la nube de Aranda Inventory y adquisición de Service Desk" -según demanda-,* el cual estará reemplazando el sistema SUATT.

Criterio

Las Normas Técnicas para la gestión y el control de las tecnologías de la información, en el proceso 5, Arquitectura Empresarial, menciona:

"La Institución debe disponer de prácticas formales que permitan gestionar la arquitectura empresarial orientada la gestión de los procesos institucionales para promover la implementación de la estrategia organizacional, en el que se establezca la identificación formal de la estructura de datos clasificada según su nivel de criticidad y uso, la asociación de los procesos institucionales, de acuerdo con el uso de recursos tecnológicos (sistemas de información e infraestructura) para acceder, procesar y almacenar los datos e información".

Causa

La ausencia de restricciones de tamaño en los archivos adjuntos se ha dado un requerimiento de configuraciones para proveedores externos, a pesar de ser inadecuadas es necesaria para la funcionalidad de adjuntar evidencia.

Efecto

La falta de restricciones de tamaño en los archivos adjuntos puede llevar a un crecimiento descontrolado de la base de datos de los diferentes sistemas. Esto podría afectar negativamente el rendimiento general del sistema, ralentizar las consultas y búsquedas, y agotar el espacio de almacenamiento disponible. La falta de espacio de almacenamiento podría eventualmente resultar en la necesidad de una inversión adicional en recursos de hardware, lo que podría impactar en el presupuesto y en la escalabilidad del sistema.

Recomendaciones

Documentar o justificar lo correspondiente de tamaño para los archivos adjuntos en los diferentes sistemas a ser desarrollados o adquiridos; estos al adjuntar archivos en los diferentes procesos que se requieran.

Considerar que la configuración de límites de tamaño para los archivos adjuntos y la implementación de mecanismos para la gestión y purga periódica de archivos no necesarios es una medida pertinente para el manejo adecuando de las bases de datos. Al establecer estas restricciones, se controlará el crecimiento de la base de datos, se preservará el rendimiento del sistema y se garantizará un uso eficiente del espacio de almacenamiento disponible.

C.3 Solicitudes en el sistema SPEIHS

Normal

Condición

Al momento de efectuar la auditoría de los sistemas, se encuentra que, en el sistema de solicitudes para la revisión de Hidrantes, SPEIHS, se ha identificado una limitación significativa, ya que no permite la búsqueda de solicitudes a través del número único asignado a cada solicitud de revisión de hidrantes.

Se nos informa sobre una solicitud para la atención de lo indicado que se encuentra a la fecha de este informe pendiente de ser revisado en los ambientes de prueba para luego pasar a producción.

Criterio

Las Normas Técnicas para la gestión y el control de las tecnologías de la información, en el proceso 10, Desarrollo, implementación y mantenimiento de sistemas de información, menciona:

"La Unidad de TI debe aplicar prácticas formales que permitan ejecutar un proceso consistente para la definición de requerimientos, diseño, adquisición y/o desarrollo, realización de pruebas, migración de datos e información, aprobación, integración de conocimiento e inteligencia de negocios y puesta en marcha de las soluciones, con el fin de asegurar que la institución cuente con sistemas de información y aplicaciones que permitan gestionar adecuadamente la información requerida".

Causa

La carencia de la funcionalidad de búsqueda podría estar relacionada con deficiencias en el diseño o la implementación del sistema, una omisión en los requisitos iniciales del sistema o de problemas técnicos que impiden la implementación adecuada de la función de búsqueda por número único.

Efecto

Como resultado de esta limitación, los usuarios del sistema SPEIHS enfrentan dificultades al intentar localizar solicitudes específicas de revisión de hidrantes, si bien es cierto lo pueden realizar por un rango de fechas establecidas, el no realizarla con el número de la solicitud podría atrasar el trabajo diario. Esto puede afectar negativamente la eficiencia operativa del proceso de revisión de hidrantes y, potencialmente, comprometer la seguridad en caso de emergencias.

Recomendación

Tomar las medidas necesarias para corregir esta deficiencia y garantizar que el sistema permita a los usuarios buscar y acceder de manera efectiva a las solicitudes de revisión de hidrantes utilizando el número único asignado. Esto mejorará la eficiencia operativa, la trazabilidad de las revisiones y, en última instancia, contribuirá a un proceso de revisión de hidrantes más seguro y eficiente.

C.4 Cantidad de intentos fallidos para el ingreso de contraseñas

Elevado

Condición

En la validación de los sistemas y herramientas tecnológicas se identificó que cuando se requiere ingresar a los sistemas se tiene hasta un máximo de 10 intentos para ingresar erróneamente la contraseña, se solicitó al departamento de TI la documentación de dicha política y al día del desarrollo del presente informe no se nos proporcionó información documentada sobre el proceso de recuperación de contraseñas en los sistemas desarrollados.

Criterio

Las Normas Técnicas para la gestión y el control de las tecnologías de la información, en el proceso 11, Seguridad y Ciberseguridad, menciona:

"La Institución debe establecer mecanismos efectivos para prevenir, detectar, impedir, valorar, evaluar y corregir transgresiones a la seguridad que pudieran generarse al nivel de acceso a sistemas, infraestructura e instalaciones en las que se almacena, procesa y transmite información, previendo que el personal y los proveedores tengan accesos mínimos necesarios para la ejecución de sus funciones; se apliquen controles para proteger la confidencialidad, autenticidad, privacidad e integridad de la información".

Como buena práctica a seguir "el Reglamento de Central Directo del Banco Central de Costa Rica, menciona:

"d) Por razones de seguridad, después de tres intentos consecutivos de ingreso fallidos que realice el participante en Central Directo, su clave auxiliar quedará bloqueada permanentemente".

Causa

La falta de documentación y detalles sobre el proceso de recuperación de contraseñas se da por debilidades en la formalización de políticas y procedimientos de seguridad de la información o a una falta de comunicación entre los responsables de la auditoría y los encargados del sistema. Esto ha resultado en la ausencia de información específica sobre la cantidad de intentos permitidos en el proceso de recuperación de contraseñas.

Efecto

La falta de documentación detallada y la ausencia de información sobre los límites de intentos para la recuperación de contraseñas pueden tener un impacto negativo en la seguridad de los sistemas desarrollados. Sin una política clara y restricciones adecuadas, existe un riesgo potencial de abuso o intentos maliciosos de acceso no autorizado a cuentas de usuario.

Recomendación

Documentar y formalizar un proceso de recuperación de contraseñas que cumpla con las mejores prácticas de seguridad de la información. Este proceso debe incluir un procedimiento que establezca un límite razonable en la cantidad de 3 intentos permitidos para la recuperación de contraseñas, con el objetivo de mitigar riesgos de seguridad.

D. Gestión de la continuidad de operaciones

En la revisión de estas actividades se verificó lo siguiente:

1. Aplicación del marco de continuidad de negocio.
2. Existencia del plan de continuidad de TI.
3. Análisis de Impacto.
4. Plan de continuidad de negocio.
5. Capacitación a los colaboradores en continuidad de negocio.
6. Pruebas de validación a los respaldos.

En la sesión de seguimiento de este informe se identifica 1 observación en proceso de atención para la gestión de la continuidad de negocio.

E. Seguimiento a recomendaciones anteriores

Se presenta a continuación la matriz de seguimiento de recomendaciones que se han incorporado en informes sobre tecnología de información de los periodos 2019 y 2021.

La matriz incluye el año de corte del informe, el nombre del hallazgo y el nivel de riesgo indicado en el año del informe, el estado actual de cumplimiento, la descripción de la observación, la(s) recomendación (es) y comentario de la administración.

Se resume el cumplimiento de las recomendaciones emitidas en informes de periodos anteriores. En el periodo 2019 y 2021 se identifican 2 observaciones en proceso de atención, para los años anteriores fueron atendidas.

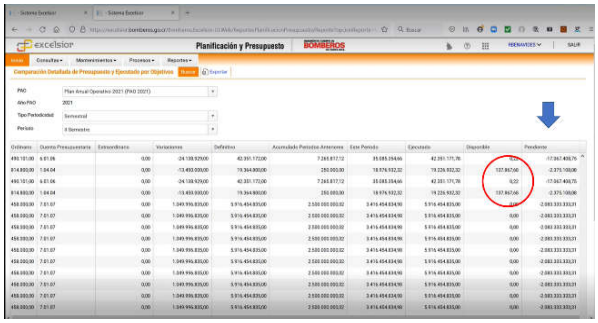
Año / Estado	Total, General	Atendidas	Pendientes	N/A	En Proceso
2019	4	3	-	-	1
2021	3	2	-	-	1
Total	**7**	**5**	**-**	**-**	**2**



	Carta	Asunto	Estado		
			Atendido	En proceso	Se mantiene
E.1	**2021**	**X.3 Inconsistencias en sistemas de información (4.2)** **Riesgo Elevado**	☐	☒	☐

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.



Recomendación

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

<u>Plan de acción</u>

Se consultará al Dueño del Módulo la conveniencia del cambio sugerido por la Auditoría.
Fecha: 01/07/2023.

Fecha vencimientos: 01/07/2023, según CBCR-043283-2022-DGB-01429 del 01/11/2022.

<u>Actividades realizadas</u>

Con fecha 09 de enero de 2023 se envía a la unidad usuaria el oficio número CBCR-000633-2023-TIB-00003, con consulta referente a la recomendación de auditoría. Al día nos mantenemos a la espera de la respuesta.

Mediante SUATT número 3696-2023, se está atendiendo la mejora planteada por la auditoría.

Comentario de la administración CBCR-023069-2023-PLB-00091 con fecha 4 de julio de 2023, se hace solicitud de prórroga al 31 de diciembre del 2023.

<u>Comentario de la administración</u>

Por medio de CBCR-023069-2023-PLB-00091 con fecha 4 de julio de 2023, se hace solicitud de prórroga al 31 de diciembre del 2023.

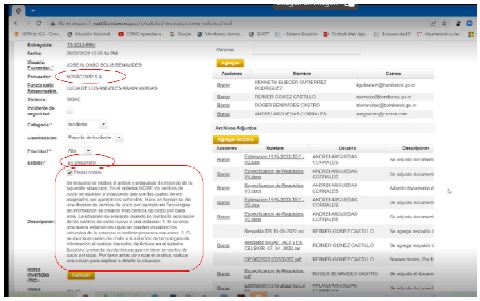
<u>Comentario de la auditoría</u>

En proceso.

b. El módulo de Gestión de Activos

- 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:



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.

Plan de acción

Una vez realizado el ajuste en desarrollo, se solicitará el área usuaria revisar si queda alguna inconsistencia en los registros o datos generados.

Fecha vencimientos: 01/07/2023, según CBCR-043283-2022-DGB-01429 del 01/11/2022.

Actividades realizadas

El día 27/10/2022 se realiza el pase al ambiente de producción del entregable 75-2022-PRV correspondiente al proceso de Gestión de activos, mismo que atiende la recomendación.

Se informa a la unidad usuaria mediante el oficio número CBCR-042753-2022-TIB-00258.

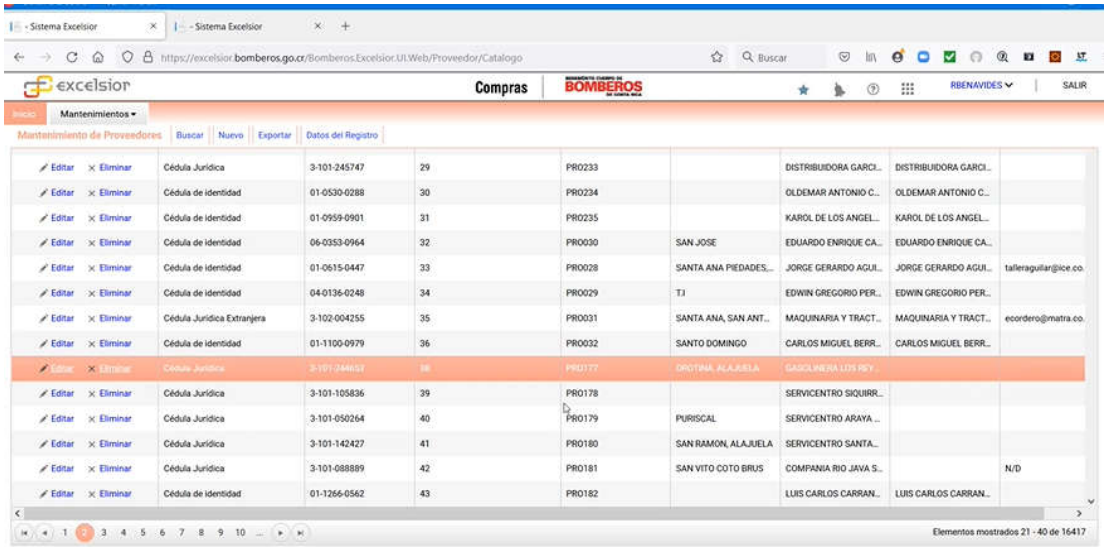
La mejora planteada se atendió mediante entregable número 75-2022- PRV, el mismo se encuentra en producción y fue atendida.

Comentario de la auditoría

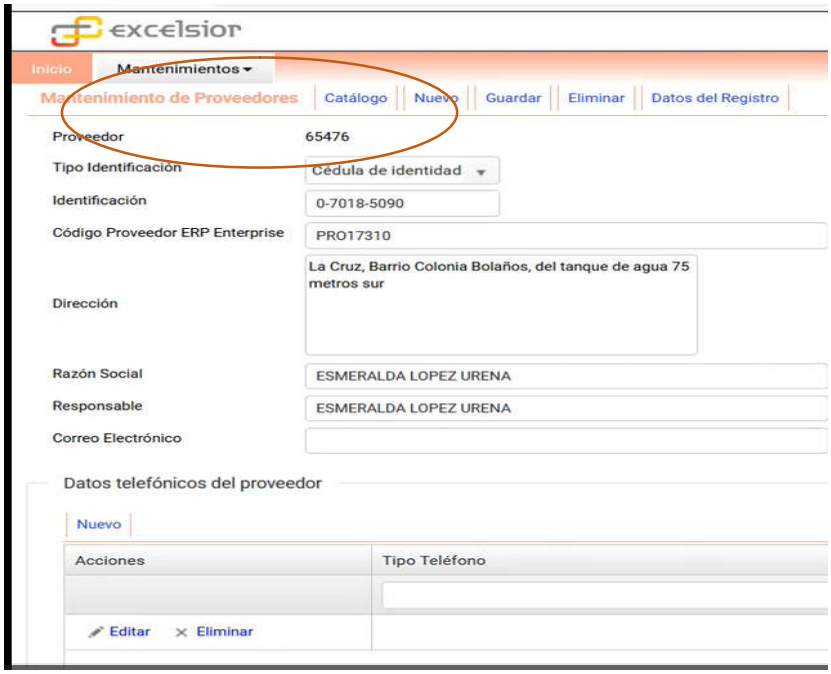
Atendida.

c. El módulo de Compras

- 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).



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.

Plan de acción

Se consultará al Dueño del Módulo de Compras si requiere las pistas sugeridas por la Auditoría.

Se recordará al Usuario el formato de las cédulas en el sistema y se solicitará la revisión de la data correspondiente.

Fecha vencimientos: 01/07/2023, según CBCR-043283-2022-DGB-01429 del 01/11/2022.

Actividades realizadas

Mediante oficio CBCR-000634-2023-TIB-00004 se consulta a la unidad usuaria en relación con la atención de la recomendación, como respuesta se recibe el oficio CBCR-010555-2023-SOA-00116, donde se indica que se estará atendiendo con el desarrollo de la primera parte del módulo de compras de Excelsior, mismo que se encuentra en proceso, con fecha estimada de implementación, para el mes de octubre de 2023, según cronograma general del proyecto.

Mediante oficio CBCR-033733-2022-DGB-01079, se propone el desarrollo del requerimiento: "Registro y actualización de proveedores", que atiende el registro de proveedores como único en el Excelsior.

En forma complementaria, mediante oficio CBCR-010555-2023-SOA-00116, se considera la atención de pistas de auditoría en el desarrollo del nuevo módulo de compras, para los procesos de proveedores.

Comentario de la administración

Por medio de CBCR-023069-2023-PLB-00091 con fecha 4 de julio de 2023, se hace solicitud de prórroga al 31 de diciembre del 2023.

Comentario de la auditoría

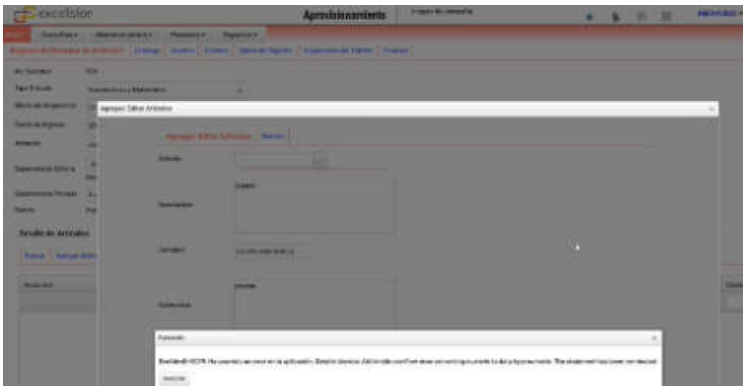
En proceso.

d. El módulo de Aprovisionamiento

- 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".
Plan de acción

Se validará el ingreso de datos negativos para evitar el error.

Actividades realizadas

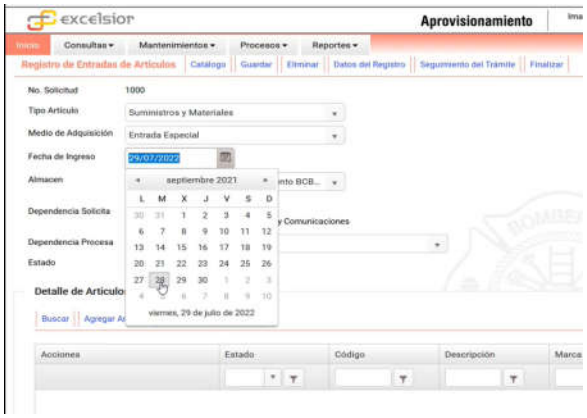
Fecha vencimientos: 01/07/2023, según CBCR-043283-2022-DGB-01429 del 01/11/2022.

Mediante SUATT número 8737-2022-TEC, se atendió la recomendación planteada por la auditoría.

Comentario de la auditoría

Atendida.

- 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:



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.

Plan de acción

Se consultará al Dueño del Módulo la conveniencia del cambio sugerido por la Auditoría.

Fecha vencimientos: 01/07/2023, según CBCR-043283-2022-DGB-01429 del 01/11/2022.

Actividades realizadas

Se atiende mediante el SUATT número 53-2023, mismo que se encuentra en pruebas de usuario.

Comentario de la auditoría

Atendida.

	Carta	Asunto	Estado		
			Atendido	En proceso	Se mantiene
E.2	**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.

Plan de acción

Se actualizarán los documentos que sean necesarios para contar con un Plan de Continuidad que considere los nuevos riesgos en función del negocio de la institución.

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.

Por medio CBCR-012726-2023-PLB-00041, con fecha 13 de abril de 2023 se comenta:

El año anterior, posterior al análisis del documento preliminar del Plan de Continuidad del Negocio del Benemérito Cuerpo de Bomberos, se consideró necesario actualizar las estrategias definidas en dicho plan, con el objetivo de integrar en la definición de variables del modelo, aspectos esenciales que garanticen la continuidad del servicio ofrecido por la Institución.

Así las cosas, nos dimos a la tarea de realizar una investigación de las normas referentes a continuidad de negocios, identificando la existencia de la INTE/ISO 22301:2020 "Seguridad y resiliencia - Sistemas de gestión de continuidad del negocio – Requisitos". Estudiando su alcance, se detecta que tiene un enfoque para empresas y organizaciones de ámbito privado, para la obtención de una ventaja competitiva.

En virtud de lo anterior y dado a que mediante oficio CBCR-012396-2023-DGB-00433 del martes 11 de abril del presente año, se comunicó al Área de Planificación, la asignación del Plan de Continuidad como parte de sus funciones, se solicita la extensión del plazo de atención de la recomendación de referencia, al 30 de setiembre de 2023.

Por medio CBCR-029156-2023-PLB-00154, se comenta sobre los cambios relacionados al Plan de Continuidad del Negocio y establecimiento de los escenarios de interrupción, con fecha 22 de agosto de 2023:

De conformidad con el proceso de continuidad a cargo de este despacho, agradecemos dejar sin efecto el CBCR- 016153-2023-PLB-00055 del 9 de mayo de 2023.

Lo anterior, se debe a que el enfoque del plan de continuidad del negocio fue modificado, con el fin de lograr el alineamiento con el gobierno corporativo y la estrategia de continuidad del negocio, que este persigue. Aspecto que permite, robustecer los cimientos del plan de referencia, para que contribuyan al cumplimiento de la misión y del plan estratégico institucional y se reduzcan las exposiciones negativas, que eventualmente puedan presentarse a nivel de imagen y costos.

Comentario de la Administración

Por medio del oficio CBCR-025736-2022-PLB-00110 del 30 de junio de 2022, se solicita ampliación para el cumplimiento del plan de acción al 31 de diciembre de 2022.

Por medio del oficio CBCR-012726-2023-PLB-00041 del 13 de abril de 2023, se solicita la extensión del plazo de atención de la recomendación, al 30 de setiembre de 2023.

Por medio del oficio CBCR-034170-2023-PLB-00247 del 29 de setiembre de 2023, se solicita ampliación al 31 de mayo de 2024.

Comentario de la auditoría

En proceso.

F. Conclusiones

1. Se deben seguir aportando recursos para atender la implementación de las normas de acatamiento del MICITT que le corresponde al BCBCR. La madurez en la gestión de TI es un proceso evolutivo, y es crucial abordar de manera adecuada tanto la infraestructura tecnológica como la capacidad organizativa para alcanzar un nivel óptimo de cumplimiento de las normativas y garantizar la eficacia en la gestión de la información y la ciberseguridad.

2. Se deben revisar las necesidades y cierre de brechas para cubrir temas de ciberseguridad y continuidad con posibles estrategias de Grupo, para ser atendidas directamente por BCBCR.

3. Importante recordar que, dado la realidad actual de un entorno de crecientes amenazas cibernéticas y desafíos en la seguridad de la información de las instituciones públicas, la importancia de mantener actualizado y efectivo un plan de continuidad y disponibilidad es más crítico que nunca. La capacidad de una organización para mantener sus operaciones, proteger sus datos y responder a amenazas, especialmente después de los ataques recientes que han afectado a instituciones públicas, depende en gran medida de la preparación y la agilidad del plan. Actualizar y comunicar el plan de manera efectiva, así como probarlo regularmente, no solo garantiza que la organización esté bien preparada para enfrentar cualquier interrupción, sino que también envía un mensaje claro de compromiso con la protección de la información sensible y la continuidad del servicio a los ciudadanos y las partes interesadas. La inversión en la robustez de estos planes es una inversión en la seguridad, la confianza y la capacidad de respuesta de la organización en un mundo digitalmente interconectado y en constante evolución.

4. Mantener una coordinación entre la auditoría interna y TI para la identificación, construcción y monitoreo de las pistas de auditoria con el objetivo de fortalecer la supervisión interna, mejorar la detección de problemas y contribuir a la seguridad integral de los sistemas, aplicativos y herramientas de la institución.