Benemérito Cuerpo de Bomberos de Costa Rica
(BCBCR)

Informe sobre el seguimiento a las recomendaciones de la auditoría externa de sistemas de información del BCBCR

Al 28 de febrero de 2023

Crowe Horwath CR, S.A.

Benemérito Cuerpo de Bomberos de Costa Rica
(BCBCR)

Informe sobre el seguimiento a las recomendaciones de la auditoría externa de sistemas de información del BCBCR

Al 28 de febrero de 2023

Benemérito Cuerpo de Bomberos de Costa Rica
(BCBCR)

Índice de contenido

		Página
I.	Objetivo	- 2 -
II.	Responsabilidad de la Administración	- 2 -
III.	Responsabilidad de los auditores y marco normativo	- 2 -
IV.	Alcance	- 2 -
V.	Procedimientos	- 3 -
VI.	Metodología de evaluación	- 3 -
VII.	Seguimiento de las recomendaciones de periodo anteriores	- 5 -
VIII.	Mapa de calor de los riesgos evidenciados al cierre de este informe	- 5 -
IX.	Estado de las recomendaciones al 28 de febrero de 2023.	- 6 -

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

31 de marzo de 2023

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

ASUNTO: INFORME DE SEGUIMIENTO A LAS OBSERVACIONES DE LA 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 dar seguimiento a las recomendaciones emitidas en el informe del periodo 2021, así como las de periodos anteriores que se encuentran pendientes de ejecutar por la Administración.

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 seguimiento a las observaciones de la auditoría externa sobre los sistemas de información al 28 de febrero de 2023 se extiende hasta el día 31 de marzo 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: 2023.05.04 08:30:42 -06'00'

Fabian Zamora Azofeifa
Socio

Benemérito Cuerpo de Bomberos de Costa Rica
(BCBCR)

Informe sobre el seguimiento a las recomendaciones de la auditoría externa de sistemas de información del BCBCR

Al 28 de febrero de 2023

I. Objetivo

Expresar según los términos del Cartel de Contratación, un seguimiento a las recomendaciones en proceso de atención del informe de auditoría externa sobre los Sistemas de Información del periodo 2021, así como las de periodos anteriores que se encuentran pendientes de ejecutar por la Administración. sobre el cumplimiento de las "Normas Técnicas para la Gestión y el Control de las Tecnologías de Información" emitidas por la Contraloría General de la República.

El seguimiento es sobre recomendaciones realizadas en los años 2019, 2020 y 2021.

II. 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. La responsabilidad de la administración de los Sistemas de Información que se encuentren en funcionamiento incluye establecer los mecanismos y procedimientos necesarios para garantizar razonablemente la confiabilidad, pertinencia, relevancia y oportunidad de la información que se produce de las operaciones del BCBCR, para salvaguardar los activos y que sirva de apoyo en la toma de decisiones y en la rendición de cuentas.

III. Responsabilidad de los auditores y marco normativo

Nuestra responsabilidad consiste en revisar y evaluar la atención de las recomendaciones comunicadas en el informe de auditoría externa del periodo 2021, incluye periodos anteriores, sobre la emisión de 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).

IV. Alcance

Dar el debido seguimiento a las recomendaciones emitidas en el periodo 2021 y en periodos anteriores que se encuentren pendientes de ejecutar por la Administración, según último informe emitido por la auditoría externa en Sistemas de Información del BCBCR del periodo 2021.

V. Procedimientos

Seguimiento a las recomendaciones anteriores

Se ejecutaron las siguientes acciones:

a) Revisar el informe de auditoría de sistemas de información externo del periodo 2021.
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.

VI. Metodología de evaluación

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.

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

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

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

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:

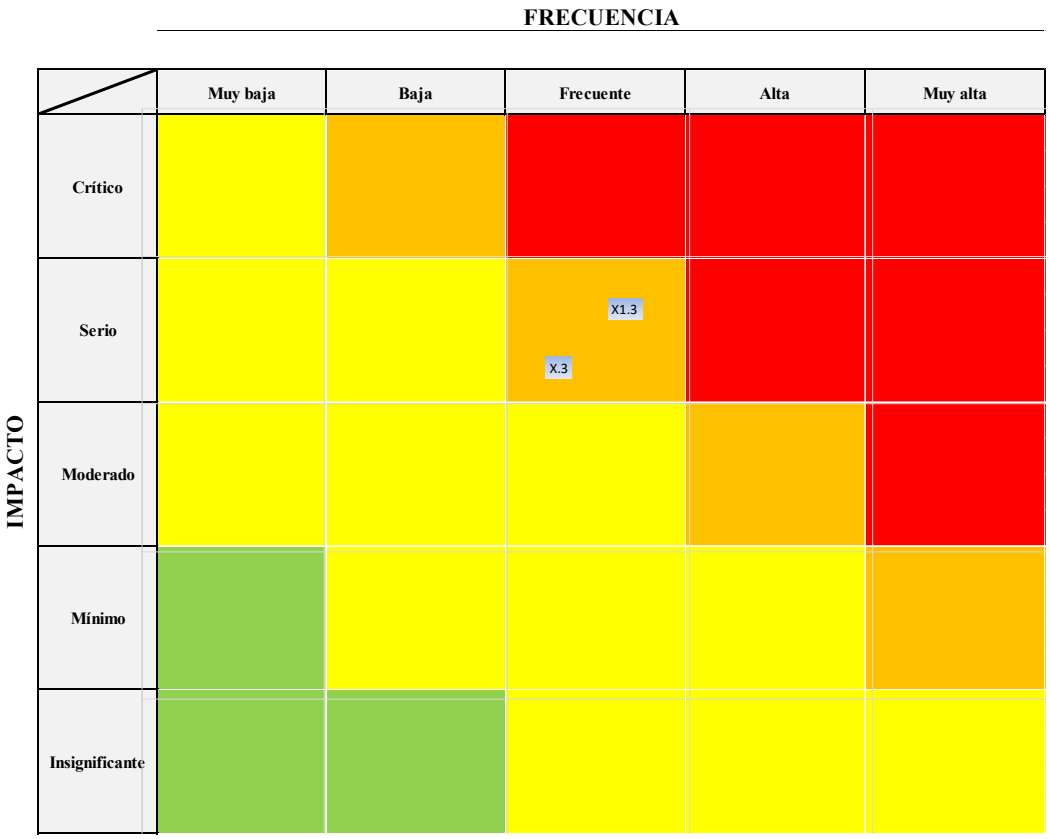
De 1 a 2: El nivel de riesgo es de oportunidad.
De 3 a 9: El nivel de riesgo es normal.
De 10 a 12: El nivel de riesgo es elevado.
De 15 a 25: El nivel de riesgo es inaceptable.

VII. Seguimiento de las recomendaciones de periodo anteriores

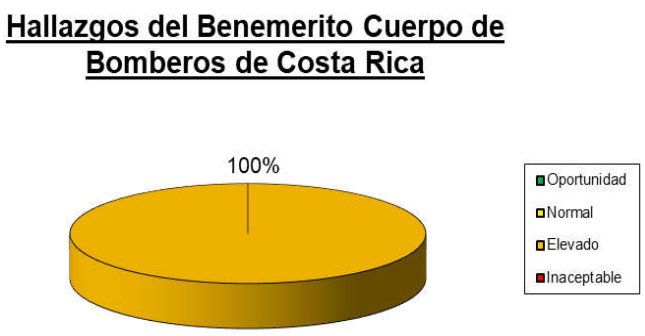
Año	Ref.	Oportunidades de mejora	Nivel de cumplimiento	Impacto	Frecuencia	Categoría de riesgo
2021	X.3	X.3 Inconsistencias en sistemas de información (4.2)	Cumplimiento parcial bajo	Serio	Frecuente	Elevado
2019	XI.3	IX.1 Actualización y aplicación del proceso de continuidad (1.4.7)	Cumplimiento parcial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

VIII. 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 2 observaciones en proceso de atención del periodo 2021 y 2019.



Como resultado de las observaciones de seguimiento, se identifican 2 observaciones en proceso de atención las cuales se distribuye en un 100% de riesgo elevado:

- 2 de riesgo elevado

IX. Estado de las recomendaciones del informe de auditoría externa sobre el cumplimento de los apartados de la Normas Técnicas de Gestión y Control de las Tecnologías de Información al 28 de febrero de 2023.

	Carta	Asunto	Estado		
			Atendido	En proceso	Se mantiene
X.1	**2021**	**X.1 Debilidades de cableado y dispositivos de acceso inalámbrico en estaciones (1.4.3)** **Riesgo Elevado**	☒	☐	☐

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

Criterio

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.

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.

Plan de acción

1. Incorporar 2 funcionarios en el proceso de atención de los servicios de soporte técnico.

2. Enviar comunicado a usuarios recordando uso correcto de UPS y regletas eléctricas.

Fecha vencimientos: 31/10/2022, según CBCR-043283-2022-DGB-01429 del 01/11/2022.

Comentario de la administración

Por medio del oficio CBCR-043550-2022-DOB-00776, con fecha 3/11/2022, se envía comunicado sobre el uso de las UPS y regletas eléctricas.

Se realiza una licitación según demanda 2019LN-000005-0012800001 "Contratación de Servicios Tercerizados (outsourcing)" - Orden de Pedido - Unidad de Tecnologías de Información - Soporte en Componentes Electrónicos.

Este servicio de soporte en componentes electrónicos ayudará a realizar y apoyará en las siguientes actividades por medio de 2 personas:

- *Realizar actividades de mantenimiento preventivo, diagnóstico de fallas y mantenimiento correctivo (reparaciones físicas y/o lógicas) en equipo electrónico tales como equipo de cómputo (de escritorio y portátil), dispositivos móviles (tabletas, teléfonos inteligentes), equipos de impresión de diverso formato, equipo multimedia (proyección, audio y vídeo), equipo de radiocomunicación, equipo telefónico, GPS, Drones, cámaras digitales, simuladores y todas aquellas soluciones que integren equipo informático y de procesamiento. Estas actividades se deben realizar tanto a nivel de hardware como de software.*

- *Realizar actividades de instalación, actualización y configuración en equipos electrónicos tales como los descritos en el ítem anteriormente indicado, estas actividades deben realizarse tanto a nivel local como dentro de una red de datos, también deben realizarse de manera presencial como vía remota.*

- *Instalar, configurar y actualizar software de todo tipo brindado por la Organización, en los equipos de la institución que así lo requieran.*

- *Realizar visitas (giras) a cualquier parte del país donde se requiera de un servicio de soporte y/o asistencia técnica en equipos electrónicos, cableado, diagnóstico, instalación y mantenimiento de cualquier tipo, en instalaciones y actividades del BCBCR.*

- *Realizar otras labores afines al puesto, cuando situaciones especiales lo requieran, todo según lo indicado en el pliego de condiciones de la Licitación Pública 2019LN-000005-0012800001.*

Por medio del oficio CBCR-045918-2022-PLB-00230 se comunica:

"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"

Se informa que, de acuerdo con el Plan de Acción propuesto por la administración, se ejecutaron las siguientes actividades:

1. Se incorporaron dos funcionarios en el proceso de atención de los servicios de soporte técnico. Oficio adjunto CBCR-037964-2022-DHB-01066.

2. Se envió mediante comunicado un recordatorio a las Estaciones de Bomberos el uso correcto de UPS y Regletas eléctricas.

Comentario de la auditoría

En la auditoría del para 2022 se estaría realizando la visita a la estación para la atención de cableado estructurado para comunicaciones, telefonía y electricidad de la estación de Santo Domingo.

	Carta	Asunto	Estado		
			Atendido	En proceso	Se mantiene
X.2	**2021**	**X.2 Servicios de internet y seguridad de la información (1.4.4) Riesgo Elevado**	☒	☐	☐

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.

Criterio

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.

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.

Plan de acción

1. Instalación de Antivirus en Tabletas.

2. Solicitar estudio para aumento de capacidad en el servicio de Internet en todas las Estaciones de Bomberos, acorde con la demanda actual de los sistemas informáticos institucionales.

Fecha vencimientos: 15/11/2022, según CBCR-043283-2022-DGB-01429 del 01/11/2022.

Comentario de la administración

Por medio del oficio CBCR-009959-2023-PLB-00035, con fecha 22 de marzo de 2023.

Se detalla:

Instalación de Antivirus en Tabletas.

1. Se planifico mediante un calendario la visita a las estaciones para actualización de antivirus. Adicionalmente se aprovechó la mejora planteada para instalar también el antivirus en todos los celulares institucionales.

   Se adjunta evidencia en archivos: Instalación antivirus Mcafee Mvisio.rar e Informe mensual de actividades de octubre.msg

Solicitar estudio para aumento de capacidad en el servicio de Internet en todas las Estaciones de Bomberos.

1. Se planteo mediante oficio C BC R-040488-2022-TIB-00245 la solicitud a Servicios Generales sobre las provisiones de capacidades de internet contratadas por estación.

2. Se realizo un análisis, investigación y valoración de los servicios vigentes y sus capacidades; teniendo en cuenta las necesidades planteadas mediante Suatts y las mejoras en el servicio ofrecido por el proveedor actual e incluso validación de alternativas en otros proveedores.

3. Implementación de mejoras planteadas en resolución a los requerimientos planteados.

Comentario de la auditoría

Por medio de la validación de los planes de acción se atienden las recomendaciones indicadas.

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

Criterio

4.2 Administración y operación de la plataforma tecnológica

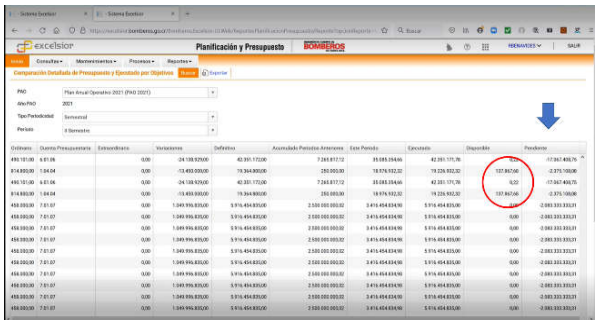
La organización debe mantener la plataforma tecnológica en óptimas condiciones y minimizar su riesgo de fallas. Para ello debe:

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.

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.

Plan de acción

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.

Actividades realizadas

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.

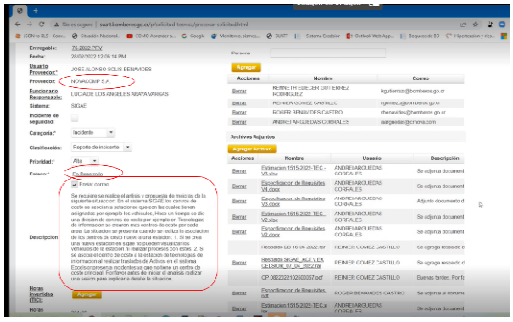
Comentario de la auditoría

Se estaría validando el avance o cumplimiento de la recomendación para la auditoría del periodo 2022.

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:



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.

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.

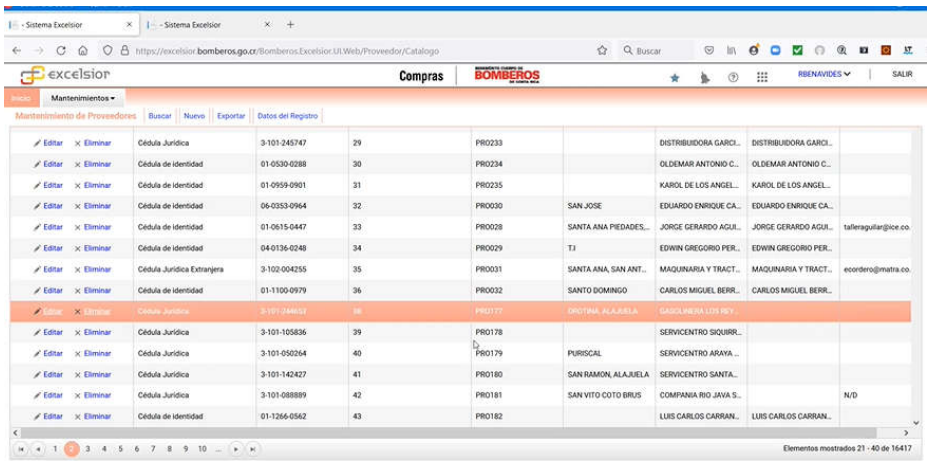
Se informa a la unidad usuaria mediante el oficio número CBCR-042753-2022-TIB-00258.

Comentario de la auditoría

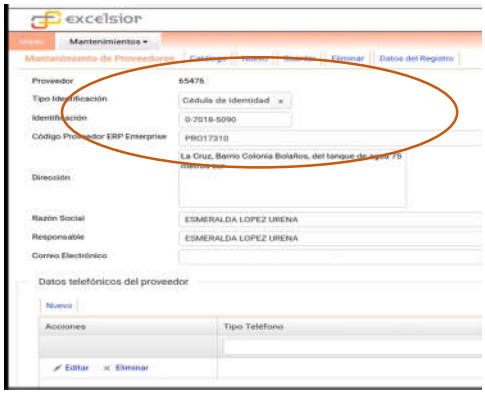
Se estaría validando el avance o cumplimiento de la recomendación para la auditoría del periodo 2022.

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.

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.

Comentario de la auditoría

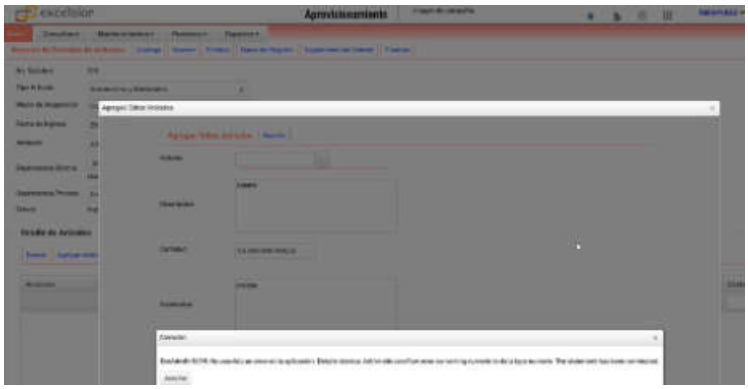
Se estaría validando el avance o cumplimiento de la recomendación para la auditoría del periodo 2022.

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.

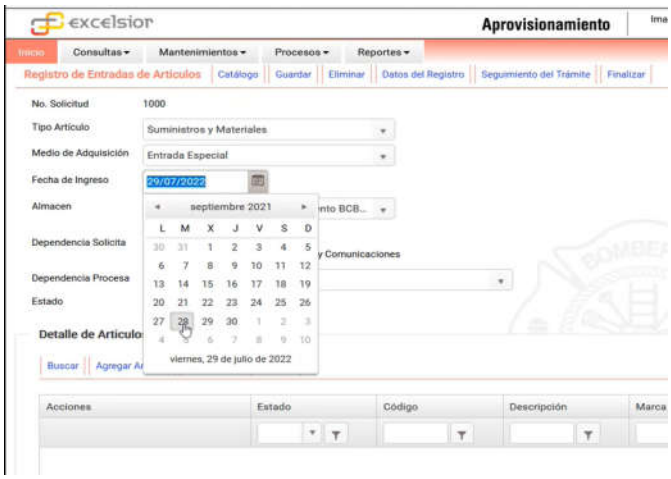
Actividades realizadas

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

Comentario de la auditoría

Pendiente oficio de atención de la recomendación.

✓ 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.

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

Pendiente oficio de atención de la recomendación.

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

Condición

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

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

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

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).

Criterio

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.

Causas

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

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

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

Efectos

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

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

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

Pérdida de credibilidad en la asignación numérica automatizada.

Recomendaciones

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

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

Plan de acción

Migrar el sistema SICOF a una tecnología más actualizada y compatible con los componentes actuales de la infraestructura que lo soporta.

Fecha vencimiento: 31/12/2022, según CBCR-041679-2021-DGB-01317 del 07/10/2021 y CBCR-020763-2022-PLB-00094 del 27/05/2022.

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.

- Se hace el 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.

- Por medio del oficio CBCR-043498-2022-TIB-00260, con fecha 02/11/2022 se da la puesta en producción de la nueva versión del Sistema Correspondencia Formal SICOFv3

Comentario de la auditoría

Se hace revisión de los controles en el sistema SICOF, con un resultado razonable de las mejoras y cambios realizados.

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

Condición

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.

Criterio

Según la Norma ISO 22301 SGCN, Sistema de Gestión para la continuidad del Negocio, se señala en el apartado 3.6, Plan de Continuidad del Negocio, los "Procedimientos documentados que conducen a las organizaciones a responder, recuperar, reanudar y restaurar el nivel de operación predefinido después de una interrupción." Normalmente este plan cubre los recursos, los servicios y las actividades que se requieren para asegurar la continuidad de las funciones del negocio.

Según la Norma ISO 22301 SGCN Sistema de Gestión para la continuidad del Negocio, se señala en el apartado 9.1.2, Evaluación de los procedimientos del negocio, inciso a) "La organización debe realizar evaluaciones de sus procedimientos y capacidades de continuidad del negocio, con objeto de verificar que continúen siendo idóneos, adecuados y eficaces." En el inciso b) se señala que "Estas evaluaciones deben de realizarse de manera periódicas, pruebas, ensayos, informes posteriores a los incidentes y evaluaciones del rendimiento. Los cambios importantes que se produzcan se deben reflejar oportunamente en los procedimientos."

Causas

Ausencia de un perfil profesional para llevar a cabo el ciclo del proceso: actualización, aplicación y monitoreo.

Los tomadores de decisiones no se han visto afectados en la interrupción de los servicios que les haga opinar sobre la materialización de riesgos. Insumos documentales sin probarse ni actualizarse para actuar de forma preventiva.

Efectos

Toma de decisiones con procedimientos y datos desactualizados, que podrían ocasionar un impacto al negocio en su operación e imagen.

Falta de sincronización para atender un evento crítico en el menor tiempo, aplicando los protocolos y los procedimientos de manera correcta.

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.

Fecha vencimiento: 30/09/2023, según CBCR-012726-2023-PLB-00041 del 13/04/2023.

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

Comentario de la auditoría

En la auditoría de TI del periodo 2022 se estaría revisando el cumplimiento de las 3 recomendaciones comunicadas.