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 2022

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 2022

Benemérito Cuerpo de Bomberos de Costa Rica
(BCBCR)

Índice de contenido

Página

21 de marzo de 2021

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 2020, 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.

Atentamente,

Fabian Zamora Azofeifa
Socio

cc.: Comité de Auditoría

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 2022

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 2020, 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 y 2020.

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 2020, 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 2020 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 2020.

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 2020.
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:

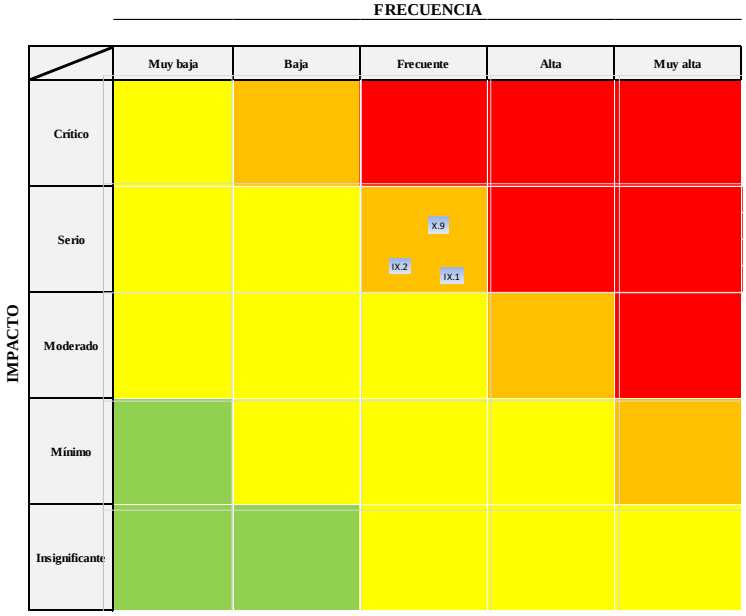
De 1 a 2:	El nivel de riesgo es de oportunidad.
De 3 a 9:	El nivel de riesgo es normal.
De 10 a 12:	El nivel de riesgo es elevado.
De 15 a 25:	El nivel de riesgo es inaceptable.

VII. Seguimiento de las recomendaciones de periodo anteriores

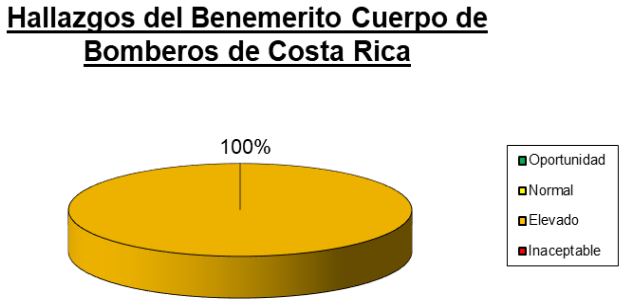
Año	Ref.	Oportunidades de mejora	Nivel de cumplimiento	Impacto	Frecuencia	Categoría de riesgo
2020	IX.1	X.1 Normativa sobre reglas en las direcciones de correo electrónico	Cumplimiento parcial alto	Serio	Frecuente	Elevado
2020	IX.2	X.2 Saltos en los consecutivos y duplicados en SICOF	Cumplimiento parcial bajo	Serio	Frecuente	Elevado
2019	X.9	IX.1 Actualización y aplicación del proceso de continuidad	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 las 3 recomendaciones en proceso de atención para la Unidad de TIC de periodos anteriores y 2020.



Como resultado de las observaciones de seguimiento, se identifican 3 observaciones en proceso de atención las cuales se distribuye en un 100% de riesgo elevado:

- 3 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 2022.

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

Condición

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

Se identifica el siguiente evento:

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

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

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.

Causa

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

Efecto

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

Recomendación

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

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

Comentario de la administración

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

- Se ha venido desarrollando una Política para asignación y uso del correo electrónico. El encargado de correo electrónico desarrollo una propuesta inicial que ha venido ajustando con la jefatura de TIC y que en este momento se encuentra en revisión final por parte de la Jefatura.

	Carta	Asunto	Estado		
			Atendido	**En proceso**	**Se mantiene**
IX.2	**2020**	**X.2 Saltos en los consecutivos y duplicados en SICOF** **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:

b) Definir previamente los requerimientos de seguridad que deben ser considerados en la implementación y mantenimiento de software e infraestructura.
c) 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.

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.

	Carta	Asunto	Estado		
			Atendido	**En proceso**	**Se mantiene**
X.3	**2020**	**Actualización de manuales para la funcionalidad y operatividad de los sistemas** **Riesgo Normal**	☒	☐	☐

Condición

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

Criterio

3.2 Implementación de software

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

a) Establecer los controles y asignar las funciones, responsabilidades y permisos de acceso al personal a cargo de las labores de implementación y mantenimiento de software.
b) Controlar las distintas versiones de los programas que se generen, como parte de su mantenimiento.

Causa

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

Efecto

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

Recomendación

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

Comentario de la administración

Se detallan a continuación las acciones ejecutadas, según el oficio CBCR-043037-2021-TIB-00958:

Recolección y ubicación de los manuales de los sistemas en una ubicación común y accesible para los responsables de estos.

Elaboración de un control para inventariar los manuales de usuario, técnico y de Base de Datos, considerando atributos como responsables, frecuencia, fechas de actualización, vigencia y ubicación. Adjunto "Control de Actualización de MANUALES Sistemas de Información".

Instrucción de acatamiento sobre el seguimiento y actualización de manuales por parte de la encargada del área de Sistemas y Aplicaciones a los responsables de estos.

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

Comentario de la administración

Actualmente se está a la espera de la revisión del documento final del Plan, para su debida aprobación. Posterior a su aprobación, se implementará el plan de simulación de este, para la socialización correspondiente.

Fecha máxima: 30/06/2022.

Comentario de la auditoría

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

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

Condición

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

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

Criterio

La metodología SCRUM se basa en la teoría de control de procesos empírica o empirismo y un enfoque interactivo e incremental para optimizar la predictibilidad y el riesgo. Para ello se base en tres pilares de control:

Transparencia: El proceso debe ser visible para todos aquellos responsables del proceso; estos procesos deben ser definidos en base a un estándar común.

Inspección: Los usuarios deben inspeccionar frecuentemente los artefactos y el progreso hacia el objetivo para detectar variaciones indeseadas.

Adaptación: Cuando se determina que uno o más aspectos de un proceso se desvían de los límites aceptables y el producto resultante serán inaceptable, el proceso o producto debe ajustarse cuanto antes para minimizar desviaciones mayores.

Causa

Carencia de herramientas de administración y gestión de proyectos orientadas a la aplicación real y eficiente de la metodología SCRUM.

La herramienta que actualmente se utiliza, es para formular planes de trabajo, control de recursos y tiempos de forma tradicional en proyectos.

Efectos

La gestión integral de la documentación del desarrollo de software no se encuentra centralizada con el fin de tener un control de la rendición de cuentas del equipo de proyecto y del proveedor.

No se evidenció documentalmente los cambios e incremento de recursos en el equipo en cada sprint.

Auditorías del ciclo SCRUM no cuenten con un único repositorio y de una posible pérdida de datos al no estar centralizados.

Recomendación

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

Comentario de la administración

Acciones ejecutadas:

1. Inicialmente se elaboró una herramienta con las principales funcionalidades que debería considerar el ciclo de vida del desarrollo en un proyecto. Adjunto “Tabla Comparativa Soft Agil”.

2. Analizar diferentes alternativas e innovadoras mediante instalaciones y reproducciones de prototipos de proyectos similares a los ejecutados por el Área de Sistemas y Aplicaciones, obteniéndose de ello una validación de las características requeridas versus los controles internos con que se cuenta. Se adjunta correos de contactos por proveedores y herramienta comparativa “Tabla Comparativa Soft Agil”, hojas “Cumplimiento de actividades” y “Monday”,” Jira & Complementos”,” Jira vs DevOps”,” Azure DevOps”.

3. Adicionalmente se realizó un estudio comparativo de costos de las soluciones:” Tabla Comparativa Soft Agil”, hoja “Comparativa de Costos”,” DevOps Precios”,” Monday Precios”,” Jira Precios”.

4. Posteriormente se compararon las diferentes alternativas con sus precios evaluando funcionalidades y costos a fin de determinar una opción apropiada.

Producto de este análisis y en consideración al costo beneficio que representa la inversión y las integraciones adicionales que se requerirían para la implementación de estas alternativas, se determina que no es requerido adquirir herramientas adicionales puesto que a lo interno de la unidad se cuentan con controles específicos que abarcan todas las etapas de un proyecto de desarrollo y están contenidas de conformidad en instrumentos normativos debidamente implementados en los procesos actuales, específicamente “2-03-16-009 Metodología para Administración de Proyectos” y “10-03-13-010 Estándar de implementación software e infraestructura de TIC”.