CASTILLO COUNTRY CLUB

Sistema de tecnología de información

Al 31 de diciembre de 2025

CASTILLO COUNTRY CLUB

Índice

Al 31 de diciembre de 2025

Página

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

19 de enero de 2026

Señores
Junta Directiva
Castillo Country Club
Atención: Jendry Madrigal Vásquez,
Gerente General
Fernando Vega Rodriguez
Jefe de Tecnologías de Información

ASUNTO: INFORME SOBRE GESTION DE TECNOLOGIA DE INFORMACION

Al revisar los Sistemas de Información del Castillo Country Club, como parte de la auditoría de los estados financieros al 31 de diciembre de 2025, observamos asuntos relacionados con los sistemas de información y procesos de TI, sobre los cuales preparamos las conclusiones en el informe. Este informe se estructura como resultado del cumplimiento de las NIA 315 y 330; no es ni debe interpretarse como una auditoría externa de la Jefatura de Tecnología de Información de forma específica.

Al planear y ejecutar la revisión evaluamos la estructura de control interno existente y aplicamos pruebas selectivas de cumplimiento con el fin de determinar el alcance de los procedimientos de auditoría para expresar opinión sobre los estados financieros al 31 de diciembre de 2025, y no para opinar sobre la estructura de control interno o los sistemas de información en su conjunto. Este informe no es ni debe interpretarse como una auditoría de los sistemas de información.

Es necesario señalar que nuestra evaluación es limitada, por lo que una revisión más detallada de controles de aplicación podría revelar más oportunidades de mejora de las que incluye este informe.

En este informe se incluyen comentarios de la administración que no modifican las revelaciones ni el criterio expresado y no son parte integral de los hallazgos.

Los temas tratados no se refieren a empleados en particular y tienen por objeto plantear medidas para fortalecer el sistema de tecnología de información.

Nuestra responsabilidad sobre este informe sobre sistema de tecnología de información al 31 de diciembre de 2025 se extiende hasta el día 19 de enero de 2026. La fecha de la carta de gerencia 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: 2026.02.13 11:50:46 -06'00'

Nombre del CPA: FABIAN ZAMORA AZOFEIFA
Carné: 2186
Cédula: 302870450
Nombre del Cliente: Castillo Country Club, S.A.
Identificación del cliente: 3101015794
Dirigido a: Castillo Country Club, S.A.
Fecha: 13-02-2026 10:28:56 AM
Tipo de trabajo: Sistema de Tecnología de Información

Timbre de ¢25 de la Ley 6663 adherido y cancelado en el original.

FABIAN ZAMORA AZOFEIFA
Contador Público Autorizado No. 2186
COSTA RICA

COSTA RICA TIMBRE
25 COLONES 25

Código de Timbre: CPA-25-631074

Fabian Zamora Azofeifa
Socio

Castillo Country Club, S.A.

Sistema de Tecnología de Información

Al 31 de diciembre de 2025

I. Resumen ejecutivo

Como parte del trabajo de la auditoría de estados financieros al 31 de diciembre de 2025 se llevó a cabo la evaluación de controles para el área de Tecnología de Información (TI) del Castillo Country Club, S.A., en adelante la Club, la cual se basó en el 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" y las buenas prácticas de control existentes para TI y no es ni debe interpretarse como una auditoría de los sistemas de información, ni el área de Tecnologías de Información de la Club.

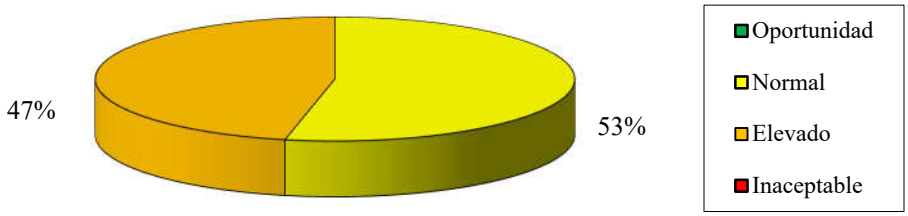
Los riesgos y recomendaciones informadas en la Carta de Gerencia Financiera con corte al 31 de diciembre de 2025 son vinculantes y deben ser revisados de forma integral con los resultados indicados en este informe.

El riesgo inherente de ciberseguridad representa una exposición significativa para la Institución, derivada de la dependencia de los sistemas de información, la infraestructura tecnológica y la conectividad digital. Este riesgo emana de la naturaleza dinámica de los entornos tecnológicos, donde la interconexión, la automatización y la evolución permanente de las amenazas generan vulnerabilidades que persisten aun con la existencia de controles establecidos. Su impacto potencial afecta los tres principios esenciales de la seguridad de la información: la confidencialidad, integridad y disponibilidad de los datos institucionales y de los sistemas críticos de operación.

Una gestión eficaz de este riesgo requiere un enfoque integral basado en su identificación, análisis y priorización, permitiendo asignar recursos de manera estratégica conforme al nivel de exposición detectado. En este contexto, el Club trabaja en fortalecer los controles tecnológicos mediante medidas como la segmentación de redes, la autenticación multifactor, el cifrado y el monitoreo continuo; consolidar la capacitación y concientización del personal para mitigar errores humanos y ataques de ingeniería social; realizar evaluaciones y auditorías de seguridad periódicas que validen la eficacia de los controles implementados; y mantener planes de respuesta y recuperación ante incidentes que garanticen la continuidad operativa y la resiliencia institucional frente a ciberataques o fallas tecnológicas.

En la evaluación a los sistemas de información se identifican 15 observaciones del periodo 2025 que de acuerdo con nuestra metodología para la clasificación de riesgos se distribuye de esta manera: 47% un riesgo elevado y 53% de riesgo normal. Se identifican 5 observaciones de periodos anteriores en proceso de atención, no incluidas en esta grafica porque fueron evaluadas por otros auditores y con otra metodología de riesgos.

Observaciones del Castillo Country Club



En la sección de conclusiones de este informe se comunican los resultados.

II. Objetivo

Evaluar el cumplimiento de requerimientos de seguridad y control en Tecnología de Información (TI) Castillo Country Club de acuerdo con las Normas Internacionales de Auditoría 315 y 330, el marco normativo interno y las buenas prácticas de control para gobierno y control de TI.

III. Alcance

El alcance incluyó aspectos relacionados con la gestión de control y sistemas de información de la Institución respecto a la elaboración de procedimientos y aplicación de controles que fortalezcan la seguridad, integridad, funcionalidad y precisión de los procesos de gestión del área de TI, gestión de la seguridad de la información, gestión de riesgos de TI, gestión de los sistemas de información, gestión de la continuidad y seguimiento de recomendaciones anteriores.

IV. Procedimientos

A partir del alcance se elaboraron y utilizaron instrumentos para recopilar la información referente al alcance indicado; entre estos, entrevistas, cuestionarios, revisión documental, levantamiento de minutas, selección de muestras y verificación de la funcionalidad de los sistemas.

Entre los temas evaluados en cada área se indican los hallazgos evidenciados.

V. Valoración basada en riesgo

Para determinar el nivel de riesgo al que se expone la entidad derivada del incumplimiento de aspectos normativos y/o deficiencias detectadas en el control interno, se procede a aplicar un análisis de impacto y frecuencia, que da como resultado la ubicación de este en un mapa de calor de 5x5 cuadrantes.

El riesgo puede evaluarse en términos de una combinación de frecuencia y magnitud y de acuerdo con dicha relación se concibe un nivel de exposición al riesgo y la posible medida a tomar en caso de mitigación.

VI. Criterios de evaluación

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

Los niveles de cumplimiento se describen a continuación:

Cumple	La entidad muestra desempeño adecuado respecto al factor evaluado.
Cumplimiento parcial alto	La entidad muestra algunas deficiencias, pero en general el desempeño respecto al factor evaluado es satisfactorio.
Cumplimiento parcial bajo	La entidad 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 riesgos se describen a continuación1:

Nivel de riesgo	Descripción
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.
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.
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.
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.

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

El formato de este informe fue estructurado para proporcionar dos referencias específicas; Cumplimiento y Nivel de riesgo.

En la práctica el "apetito de riesgo" puede ser definido en términos de una combinación de frecuencia y magnitud de un riesgo descritos en bandas de significancia del riesgo. Hemos establecido niveles de riesgo en las bandas descritas anteriormente basándonos en la frecuencia y magnitud de los riesgos.

La frecuencia y magnitud de los riesgos no necesariamente están directamente relacionados con niveles de cumplimiento de la normativa, debido a que, aunque haya incumplimiento, el impacto que puede ocasionar y la frecuencia de veces que puede ocurrir pueden tener efecto poco significativo en el proceso de administración integral de riesgos y en las operaciones.

VII. 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

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

Calificaciones:

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

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

VIII. Conclusiones generales del año 2025

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.

Hay observaciones que han sido comunicadas sobre riesgos inherentes, financieros y de mercado en la Carta de Gerencia de la auditoría financiera que deben ser revisados de forma integral con este informe.

Observaciones del periodo 2025

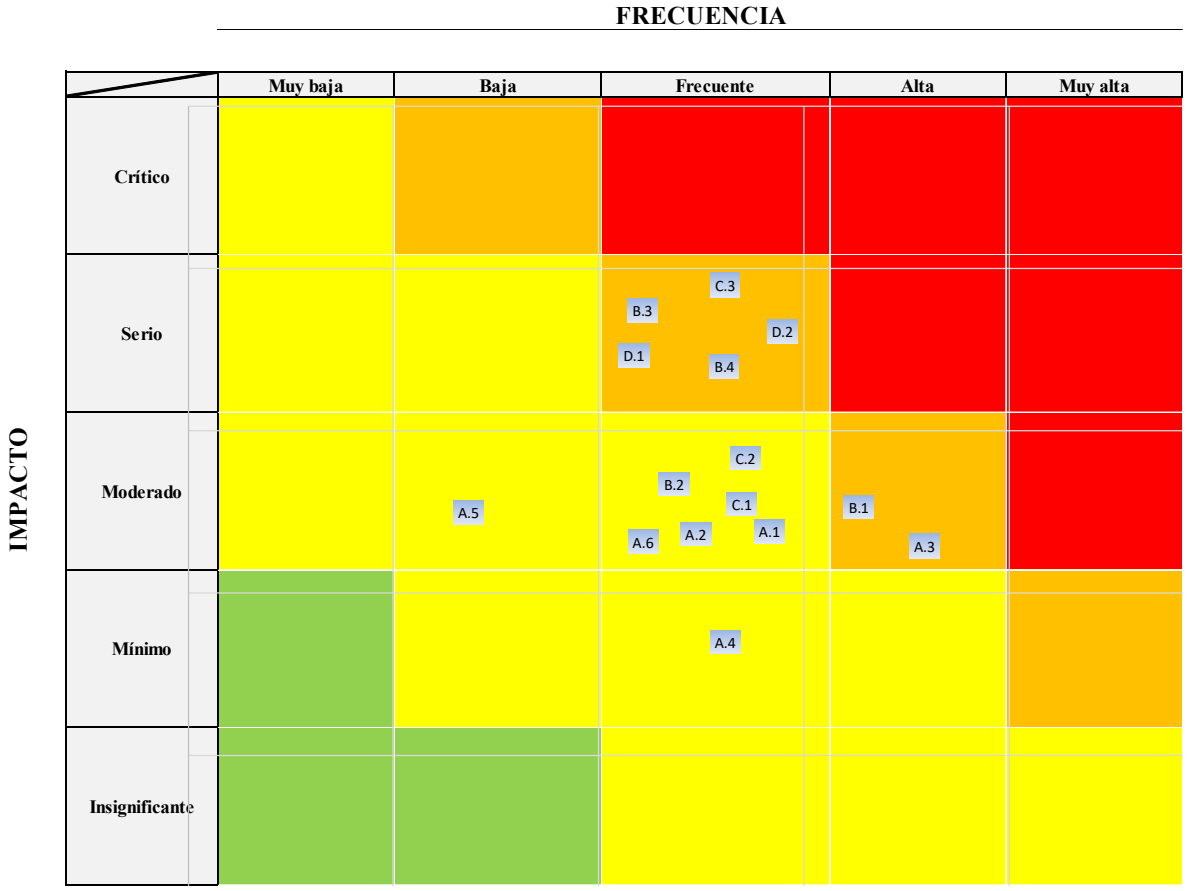
Ref.	Oportunidades de mejora	Nivel de cumplimiento	Impacto	Frecuencia	Categoría de riesgo
A.1	Informes formales de labores del área de Tecnología	Cumplimiento parcial alto	Moderado	Frecuente	Normal
A.2	Debilidades en el formato y control de la documentación institucional relacionada con Tecnología de Información	Cumplimiento parcial alto	Moderado	Frecuente	Normal
A.3	Plan de capacitación formal alineado a la gestión y seguridad de Tecnología de Información	Cumplimiento parcial bajo	Moderado	Alta	Elevado
A.4	Informes de seguimiento y mecanismos formales para la gestión de proyectos de Tecnología de Información	Cumplimiento parcial alto	Mínimo	Frecuente	Normal
A.5	Debilidades en el seguimiento y evaluación de los acuerdos de nivel de servicio (SLA) de proveedores de TI	Cumplimiento parcial alto	Moderado	Baja	Normal
A.6	Metodología formal para la gestión de riesgos de Tecnología de Información	Cumplimiento parcial alto	Moderado	Frecuente	Normal
B.1	Planificación estratégica formal de seguridad de la información	Cumplimiento parcial bajo	Moderado	Alta	Elevado
B.2	Procedimientos operativos para la administración de la seguridad de la información	Cumplimiento parcial alto	Moderado	Frecuente	Normal
B.3	Informes sobre revisión de roles y perfiles de usuario	Cumplimiento parcial bajo	Serio	Frecuente	Elevado
B.4	Marco normativo en el uso responsable de Inteligencia Artificial (IA)	Cumplimiento parcial bajo	Serio	Frecuente	Elevado
C.1	Estrategia formal para la migración de Windows 10 a Windows 11	Cumplimiento parcial alto	Moderado	Frecuente	Normal
C.2	Registros formales de cambios realizados a los sistemas de información	Cumplimiento parcial alto	Moderado	Frecuente	Normal
C.3	Limitaciones del sistema SKILL-4 y debilidades en los controles automatizados	Cumplimiento parcial bajo	Serio	Frecuente	Elevado
D.1	Ausencia de un Análisis de Impacto al Negocio (BIA)	Cumplimiento parcial bajo	Serio	Frecuente	Elevado
D.2	Ausencia de un Plan de Recuperación ante Desastres (DRP)	Cumplimiento parcial bajo	Serio	Frecuente	Elevado

Seguimiento de observaciones de periodos anteriores[2]

Ref.	Oportunidades de mejora	Riesgo
E.2	Mejoras en la gestión de usuarios	Medio
E.4	Debilidades físico-ambientales en el Centro de procesamiento	Alto
E.9	Formalización de procedimientos/instructivos técnicos de gestión sobre la infraestructura	Alto
E.10	Debilidades en la gestión de contraseña del aplicativo	Alto
E.13	Falta de un plan de continuidad del negocio	Alto

IX. Mapa de calor de los riesgos evidenciados

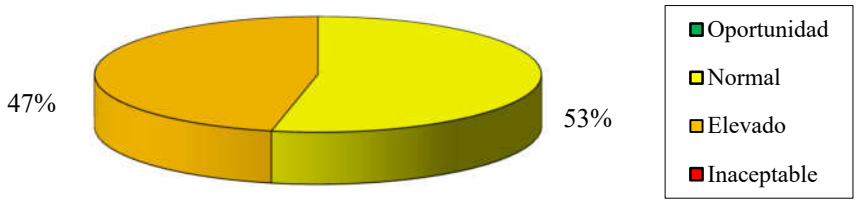
De acuerdo con nuestra revisión y a la metodología de calificación del nivel de exposición al riesgo, presentamos a continuación la matriz de 25 cuadrantes donde se resume de manera gráfica, las observaciones que incluimos en nuestro informe y su nivel de riesgo.



[2] Hallazgos reportados por otra firma de auditores

Mapa de riesgos identificado para hallazgos de los sistemas de información de la Club

Observaciones del Castillo Country Club



Como resultado de la revisión se comunican 15 observaciones que son clasificadas en la categoría de riesgo ubicada en las áreas revisadas en la siguiente forma:

- 8 de riesgo normal
- 7 de riesgo elevado

Las observaciones de periodos anteriores se califican en:

- 1 de riesgo medio
- 4 de riesgo alto

X. Procesos evaluados

A. Administración del área de TI

En la revisión de estas actividades se verificó lo siguiente:

1. Plan estratégico de TI.
2. Plan operativo de TI 2025.
3. Organigrama de TI.
4. Informes de labores de TI del periodo auditado.
5. Reglamento del Comité de TI.
6. Actas del Comité de TI.
7. Informe sobre la ejecución de proyectos del 2025.
8. Evaluaciones de los SLA´s con los proveedores actuales de servicios de TI.
9. Lista con el marco normativo (procedimientos, metodologías, etc.) para los procesos y servicios de TI.
10. Plan de capacitación a los colaboradores del periodo y su grado de ejecución.
11. Informes o recomendaciones en proceso de atención por parte de la auditoría interna.
12. Marco normativo para la gestión de los procesos y servicios de TI.
13. Metodología de riegos de TI.
14. Evaluaciones de riesgos de TI a los procesos, proyectos o servicios.

Se comunican las siguientes observaciones de mejora:

A.1 Informes de labores del área de Tecnología de Información

Normal
✔

Durante la revisión efectuada, no se identificaron informes de labores con un formato estandarizado y aprobado dentro de la Gestión Documental de la Institución del área de Tecnología de Información correspondientes al período auditado. Estos reportes que carece de fecha de elaboración y firmas de responsables, lo cual impide confirmar su validez, oportunidad y aprobación por parte de la administración.

La ausencia de informes estandarizados limita la trazabilidad de las actividades ejecutadas por TI y dificulta demostrar que las funciones relacionadas con el soporte a los sistemas que procesan información financiera han sido realizadas de manera adecuada y supervisada.

Se requiere de lineamientos mínimos para la elaboración, revisión y aprobación de informes periódicos de labores del área de TI.

Criterio

COBIT 2019 en el proceso APO01: Gestionar el Marco de Gestión de TI indica lo siguiente:

"Las prácticas de gestión deben realizarse de manera consistente y estructurada, y estar respaldadas por la documentación adecuada que proporcione evidencia de su ejecución y responsabilidad."

Recomendaciones

1. Definir y documentar un formato de informe de labores del área de TI, que incluya como mínimo: período cubierto, actividades realizadas, incidencias relevantes, responsables y firmas de revisión y aprobación.

2. Establecer en un procedimiento la periodicidad razonable para la elaboración de estos informes de labores de TI y mantenerlos como evidencia de control en un repositorio con acceso al mismo.

Comentario de la Administración

En la actualidad se realizan informes formales de labores del área de Tecnología en un formato diferente al recomendado. Se definirá un documento de informe que se adapte a las recomendaciones indicadas y cumpla con COBIT 2019 en el proceso APO01: Gestionar el Marco de Gestión de TI.

A.2 Debilidades en el formato y control de la documentación institucional relacionada con Tecnología de Información

Normal
✔

Durante la auditoría se identificó que el formato utilizado por la entidad para la documentación formal no contempla elementos básicos de gestión documental que permitan asegurar la trazabilidad, actualización y aprobación de la información. Esta situación se evidencia en diversos documentos aportados para la revisión, tales como: "Plan de Trabajo Anual 2025 TI, Informe de Labores – Resumen de logros y opciones de mejora, Informe Guía Doble Factor de Autenticación 2025, Listado de Proyectos 2025, Listado de Proveedores más Importantes de TI, Plan de Acción – Recomendaciones de Seguridad, Evidencia de Respaldos, Plan de estrategia y seguridad de la información y Políticas y procedimientos para la administración de la seguridad".

Los documentos mencionados no incluyen firmas de elaboración, revisión o aprobación, ni mecanismos de control de cambios que permitan validar su revisión periódica y vigencia. La ausencia de estos elementos limita la confiabilidad de la documentación, dificulta demostrar su aplicación efectiva y reduce la capacidad de la administración para ejercer supervisión sobre los procesos de TI que apoyan la operación y la información financiera.

Criterio

La norma ISO/IEC 27001:2022 en la cláusula 7.5.3, indica lo siguiente: "La información documentada requerida por el sistema de gestión de la seguridad de la información debe controlarse para asegurarse de que esté disponible y sea adecuada para su uso, cuando y donde se necesite."

Recomendaciones

1. Definir un formato institucional para la documentación relacionada con Tecnología de Información, que incluya como mínimo la identificación del documento, versión, fecha de elaboración, responsables y firmas de revisión y aprobación.

2. Incorporar un mecanismo de control de cambios en la documentación de TI, que permita identificar las modificaciones realizadas, su fecha y el responsable de dichas actualizaciones, con el fin de asegurar la trazabilidad y vigencia de los documentos.

3. Establecer responsables para la elaboración, revisión y aprobación de la documentación de TI, de forma que exista claridad sobre la custodia y actualización de la información documentada.

Comentario de la Administración

Se definirá un formato para la documentación relacionada con TI, adaptando la documentación ya existente a ese formato, el cual incorpora los elementos recomendados. Los documentos tendrán una periodicidad de revisión anual y se llevara un control de cambios por medio de la gestión de versiones.

A.3 Plan de capacitación formal alineado a la gestión y seguridad de Tecnología de Información

Elevado
✔

No se evidenció la existencia de un plan de capacitación formal y estructurado para el personal de la Institución en temas de Tecnología de Información. Asimismo, no se identificaron lineamientos que permitan asegurar que las actividades de capacitación se encuentren alineadas con las necesidades del negocio en materia de seguridad de la información, continuidad operativa y gestión de TI.

La ausencia de un plan de capacitación dificulta garantizar que el personal cuente con los conocimientos necesarios para operar y proteger adecuadamente los sistemas que soportan los procesos administrativos y financieros de la entidad, lo cual incrementa el riesgo de errores operativos, incidentes de seguridad y una respuesta inadecuada ante eventos que afecten la continuidad del servicio.

Criterio

COBIT 2019 en el proceso APO07: Gestionar los Recursos Humanos, indica lo siguiente:

"La empresa debe asegurar que el personal tenga las habilidades y competencias necesarias para desempeñar sus funciones, y que estas se mantengan actualizadas de acuerdo con las necesidades del negocio."

Se identifican explícitamente "Planes de desarrollo de competencias" como salidas/artefactos de la práctica APO07.03 — *COBIT® 2019: Objetivos de gobierno y gestión*, APO07.03

En el componente de Personas, habilidades y competencias, se referencia la "Provisión de educación y capacitación" y la "Gestión del aprendizaje y desarrollo" como habilidades asociadas a APO07.

Recomendaciones

1. Identificar las necesidades de capacitación del personal involucrado en la gestión y operación de procesos y servicios considerando las funciones desempeñadas y los riesgos asociados a cada rol.

2. Definir un plan de capacitación alineado con los riesgos y necesidades actuales del Country Club El Castillo, priorizando temas relacionados con seguridad de la información, continuidad operativa y uso adecuado de los sistemas que soportan la información financiera.

3. Establecer una periodicidad razonable para la ejecución de las actividades de capacitación, de forma que los conocimientos del personal se mantengan actualizados conforme a la evolución de los riesgos y del entorno tecnológico.

4. Documentar las actividades de capacitación realizadas y conservar la evidencia correspondiente, con el fin de respaldar el fortalecimiento de las competencias del personal y facilitar su verificación durante procesos de auditoría.

Comentario de la Administración

Se presenta a la Gerencia General el plan de Capacitación Formal y actualizado para el Departamento de TI de acuerdo con COBIT 2019 en el proceso APO07: Gestionar los Recursos Humanos.

A.4 Informes de seguimiento y mecanismos formales para la gestión de proyectos de Tecnología de Información

Normal
✔

No se identificaron informes independientes detallados sobre el seguimiento a los proyectos de Tecnología de Información en ejecución. Asimismo, se evidenció que la entidad no cuenta con una Oficina de Gestión de Proyectos (PMO) institucional ni con herramientas formales para la planificación, seguimiento y control de proyectos.

La falta de mecanismos formales de gestión y reporte de proyectos limita la visibilidad sobre el avance, cumplimiento de plazos y uso de recursos, así como la capacidad de la administración para identificar oportunamente desviaciones que puedan afectar la operación y los sistemas que soportan los procesos financieros.

La gestión de proyectos se realiza de manera informal, sin lineamientos definidos para la elaboración de informes de avance ni para la supervisión estructurada de los proyectos.

Criterio

COBIT 2019 en el proceso BAI01: Gestionar Programas y Proyectos indica lo siguiente:

"La empresa debe gestionar los programas y proyectos para asegurar que se entreguen los resultados esperados, dentro de los plazos y presupuestos aprobados, y de acuerdo con los requisitos del negocio." y *"La empresa debe monitorear y controlar los programas y proyectos, y reportar el progreso y las desviaciones a las partes interesadas relevantes."*.

Recomendaciones

1. Definir un esquema básico de gestión de proyectos de Tecnología de Información, que establezca lineamientos mínimos para la planificación, ejecución y seguimiento de los proyectos.

2. Asignar responsables para cada proyecto de TI, identificando claramente las funciones relacionadas con la ejecución, el seguimiento y la toma de decisiones.

3. Establecer objetivos, plazos y alcances definidos para los proyectos de TI, de forma que exista claridad sobre los resultados esperados y los tiempos de entrega.

4. Elaborar informes periódicos de avance de los proyectos de TI que permitan dar seguimiento al cumplimiento de plazos, identificar desviaciones relevantes y comunicar el estado de los proyectos a la administración.

Comentario de la Administración

El Club realiza la gestión y el control de los proyectos de TI por medio de la herramienta PAO. Se trasladará el control de proyectos y programas del PAO solicitado por la Gerencia, a un esquema básico de gestión de acuerdo con las recomendaciones y con COBIT 2019 en el proceso BAI01: Gestionar Programas y Proyectos.

A.5 Debilidades en el seguimiento y evaluación de los acuerdos de nivel de servicio (SLA) de proveedores de TI

Normal
✔

No se identificaron informes formales y regulares de seguimiento de los acuerdos de nivel de servicio (SLA) establecidos con los proveedores de Tecnología de Información. Como evidencia, se aportó el documento denominado "Evaluación SLA Proveedores", el cual corresponde a una evaluación de carácter subjetivo que no incorpora indicadores definidos, métricas cuantificables ni criterios objetivos que permitan medir el porcentaje de cumplimiento de los servicios contratados.

La ausencia de indicadores medibles y auditables limita la capacidad de la administración para evaluar de forma objetiva el desempeño de los proveedores, dar seguimiento a incumplimientos y demostrar que los servicios tecnológicos que soportan los procesos administrativos y financieros se prestan conforme a lo esperado.

Criterio

COBIT 2019 en el proceso en el proceso APO10: Gestionar Proveedores indica lo siguiente:

"La empresa debe monitorear el desempeño de los proveedores y los contratos, y gestionar los incumplimientos cuando se presenten."

Además, en el proceso MEA01: Monitorear, Evaluar y Valorar el Desempeño y la Conformidad se indica lo siguiente:

"La empresa debe definir métricas e indicadores de desempeño, y monitorear los resultados para evaluar si se están logrando los objetivos establecidos."

Recomendaciones

1. Definir un esquema de seguimiento de los SLA de los proveedores de TI, incorporando indicadores medibles, tales como tiempos de atención, disponibilidad del servicio o cumplimiento de plazos acordados.

2. Establecer una periodicidad mínima para la evaluación del cumplimiento de los SLA´s de los proveedores.

3. Documentar en informes periódicos las evaluaciones y seguimientos realizados a los servicios brindados por los proveedores, las mismas deben aplicarse prioritariamente a los proveedores que brindan servicios críticos para la operación y la información financiera.

Comentario de la Administración

El club tiene un esquema de seguimiento y evaluación de los acuerdos de nivel de servicio (SLA) de los proveedores de TI. Estos se revisan en forma anual y permiten una retroalimentación de los resultados de las evaluaciones a los distintos proveedores. Se definirá un esquema de documentación y seguimiento de los SLA de los proveedores de TI, que incorpore los controles e informes utilizados actualmente, de acuerdo con COBIT 2019 en el proceso en el proceso APO10: Gestionar Proveedores.

A.6 Metodología formal para la gestión de riesgos de Tecnología de Información

Normal
✔

No se evidenció la existencia de una metodología formal para la gestión de riesgos de Tecnología de Información.

La entidad no cuenta con lineamientos documentados que definan cómo deben identificarse, analizarse, evaluarse y tratarse los riesgos asociados a los procesos y activos tecnológicos que soportan la operación del negocio.

La ausencia de una metodología limita la capacidad de la administración para gestionar los riesgos de TI de manera estructurada y consistente.

Criterio

COBIT 2019 en el proceso APO12: Gestionar el Riesgo indica lo siguiente:

"La empresa debe definir y mantener un marco de gestión de riesgos, que incluya métodos y prácticas coherentes para la gestión de riesgos de TI"

Adicionalmente la ISO/IEC 27001:2022, en la cláusula 6.1.2 indica lo siguiente:

"La organización debe definir y aplicar un proceso de evaluación de riesgos de seguridad de la información que establezca criterios de aceptación del riesgo y criterios para realizar las evaluaciones de riesgos."

Recomendaciones

1. Definir una metodología de gestión de riesgos de Tecnología de Información, que establezca criterios claros para la identificación, análisis, evaluación y tratamiento de los riesgos asociados a los procesos y activos tecnológicos.

2. Documentar los criterios de evaluación y aceptación del riesgo, incluyendo escalas simples de impacto y probabilidad, con el fin de asegurar un análisis consistente y repetible de los riesgos de TI.

3. Establecer responsabilidades para la aplicación y mantenimiento de la metodología de gestión de riesgos de TI, de forma que exista claridad sobre quién debe identificar, evaluar y dar seguimiento a los riesgos identificados.

Comentario de la Administración

El Club cuenta con una metodología de control de riesgos, que no está aprobada. Se generará un documento formal que incorpore el análisis de riesgos actual y los criterios de evaluación de acuerdo con COBIT 2019 en el proceso APO12: Gestionar el Riesgo e ISO/IEC 27001:2022, en la cláusula 6.1.2.

B. Gestión de las prácticas de seguridad de la información

En la revisión de estas actividades se verificó lo siguiente:

1. Lista con el marco normativo (procedimientos, metodologías, etc.) para los procesos y servicios de TI.
2. Plan de capacitación a los colaboradores del periodo y su grado de ejecución.
3. Informes o recomendaciones en proceso de atención por parte de la auditoría interna.
4. Informes sobre la revisión de roles y accesos.
5. Aplicación del doble factor de autenticación para accesos.
6. Aplicación de controles de cifrado de datos.
7. Gestión de incidentes.
8. Aplicación de pruebas de vulnerabilidades.
9. Marco normativo para la aplicación de las tecnologías emergentes.

Se comunican las siguientes observaciones de mejora:

B.1 Planificación estratégica formal de seguridad de la información

Elevado
✔

Se recibió un resumen de carácter general sobre la postura de seguridad del Country Club El Castillo. No obstante, dicho documento no constituye una planificación estratégica formal de seguridad de la información, ya que no define objetivos claros, métricas medibles, responsables, plazos ni mecanismos de seguimiento.

La ausencia de una planificación estructurada limita la capacidad de la administración para orientar y priorizar las iniciativas de seguridad, así como para evaluar de forma objetiva su avance y efectividad.

Esta situación incrementa el riesgo de que los controles de seguridad que protegen la información administrativa y financiera se implementen de manera reactiva y sin una alineación clara con las necesidades del negocio.

Criterio

COBIT 2019 en el proceso en el proceso APO13: Gestionar la Seguridad indica lo siguiente: *"La empresa debe definir, operar y monitorear un sistema de gestión de la seguridad de la información, alineado con los requisitos del negocio y el apetito de riesgo."*

Recomendaciones

1. Elaborar una planificación de seguridad de la información, alineada con los riesgos actuales, que contemple objetivos claros, responsables definidos y métricas simples para su seguimiento.

2. Establecer una periodicidad mínima para la actualización de la planificación de seguridad de la información para asegurar el mantenimiento del perfil de seguridad y asegurar su constante actualización.

Comentario de la Administración

El club cuenta con una política de seguridad de la información. Se adaptará la misma de tal forma que incluya la planificación de seguridad de la información de acuerdo con COBIT 2019 en el proceso en el proceso APO13: Gestionar la Seguridad. El club cuenta con una estructura robusta de seguridad de la información que incluye Firewall de Hardware, soluciones antivirus y endpoint, entorno Microsoft 365 seguro, políticas de seguridad a nivel de Watch Guard y Eset sólidas, robustas y revisables periódicamente. La actualización de la planificación de la seguridad de la información se realizará en forma anual.

B.2 Procedimientos operativos para la administración de la seguridad de la información

Normal
✔

Se requiere que los procedimientos operativos sean formales y aprobados para la administración de la seguridad de la información, que definan de manera clara las actividades específicas que deben ejecutarse, ni describe el cómo deben realizarse las tareas propias de la seguridad, tales como la gestión de accesos, la protección de la información, el manejo de incidentes o la ejecución de respaldos.

Criterio

La ISO/IEC 27002:2022 en el control 5.1 Políticas de seguridad de la información, indica lo siguiente:

"Los procedimientos operativos para la seguridad de la información deben documentarse, mantenerse y ponerse a disposición de las personas que los necesiten."

Recomendaciones

1. Formalizar y aprobar los procedimientos para la administración de la seguridad de la información, en los cuales se detallen de forma clara las actividades a realizar y la manera de ejecutarlas, así como sus responsables específicos.

2. Establecer una periodicidad mínima para la actualización de los procedimientos para la administración de la seguridad de la información para asegurar que las actividades propias de la seguridad de la información se encuentren actualizadas.

Comentario de la Administración

La empresa cuenta con los procedimientos operativos para la administración de la seguridad de la información, los cuales son revisados con una periodicidad anual. Se generará un documento formal que incorpores los procedimientos actuales de respaldo, manejo de incidentes y gestión de accesos, incorporando los definidos para la gestión del nuevo NAS.

B.3 Informes sobre revisión de roles y perfiles de usuario

Elevado
✔

No se identificaron informes que evidencien la revisión periódica de roles y perfiles de usuario en los sistemas de información utilizados por la entidad. En consecuencia, no se cuenta con documentación que respalde que los accesos otorgados a los usuarios han sido evaluados para verificar su adecuación a las funciones desempeñadas, ni que se hayan detectado y corregido accesos innecesarios o inapropiados.

La falta de revisiones documentadas de roles y perfiles incrementa el riesgo de accesos no autorizados o excesivos a los sistemas que soportan los procesos administrativos y financieros, lo cual puede afectar la confidencialidad, integridad y confiabilidad de la información.

Criterio:

La ISO/IEC 27002:2022 en el control 5.18 Gestión de derechos de acceso indica lo siguiente: *"Los derechos de acceso de los usuarios deben revisarse a intervalos regulares."*.

Recomendaciones

1. Establecer revisiones periódicas de roles y perfiles de usuario en los sistemas de información, con una frecuencia periódica, priorizando los sistemas que soportan procesos administrativos y financieros.

2. Documentar los resultados de las revisiones de accesos mediante informes que identifiquen los usuarios activos, los roles asignados, los accesos innecesarios o inadecuados detectados y las acciones correctivas definidas.

3. Asignar responsables para la ejecución y revisión de los controles de acceso, de forma que exista claridad sobre quién valida la adecuación de los permisos otorgados a los usuarios.

4. Aplicar los ajustes necesarios a los roles y perfiles de usuario como resultado de las revisiones realizadas, asegurando que los accesos se mantengan alineados con las funciones desempeñadas.

Comentario de la Administración

Las revisiones de roles y perfiles se realizan como un proceso mensual en el club y existe un procedimiento donde solo las jefaturas pueden aprobar los perfiles y roles en los sistemas de información. Existen responsables de realizar la revisión periódica y protocolos cuando se da la salida de algún colaborador. Se generará documentación sobre los resultados de las revisiones de acuerdo con la ISO/IEC 27002:2022 en el control 5.18 Gestión de derechos de acceso.

B.4 Marco normativo en el uso responsable de Inteligencia Artificial (IA)

Elevado
✔

No se identificaron lineamientos internos ni procedimientos formalizados que orienten el uso, desarrollo o adopción de herramientas de Inteligencia Artificial (IA) en los procesos tecnológicos u operativos de la organización.

Tampoco se evidencian políticas, guías o protocolos que regulen el uso responsable de IA, abarcando principios de ética, protección de datos, criterios de evaluación y validación de modelos, así como mecanismos de gestión y control de los riesgos tecnológicos asociados.

Si bien el aprovechamiento de tecnologías emergentes como la IA representa una oportunidad estratégica para fortalecer la eficiencia operativa y la innovación, la ausencia de directrices internas limita su adopción segura, trazable y alineada con los objetivos de transformación digital y gobierno corporativo.

Criterio

COBIT 2019, en los procesos APO02 (“Gestionar la estrategia”) y APO03 (“Gestionar la arquitectura empresarial”), recomiendan establecer políticas y procedimientos alineados a las tecnologías emergentes.

Adicionalmente la ISO/IEC 42001:2023 (Tecnología de la información-Inteligencia artificial-Sistema de gestión), Sistema de gestión de inteligencia artificial, establece la necesidad de definir controles, responsabilidades y procesos para un uso ético y seguro de la IA.

Recomendaciones

1. Definir lineamientos estratégicos que regulen el uso, adopción y desarrollo de soluciones de IA, asegurando su alineación con el marco de gobierno de TI, la estrategia digital institucional y los requerimientos regulatorios aplicables.

2. Elaborar un protocolo interno básico que establezca los criterios mínimos para el uso responsable de IA en proyectos de desarrollo de software o análisis de datos, considerando ética, privacidad y validación técnica.

3. Incluir el tema de IA dentro del plan de capacitación técnica del personal de la Sociedad, para fortalecer las competencias en tecnologías emergentes y fomentar una cultura de innovación responsable.

4. Realizar pilotos controlados antes de implementar soluciones de IA en producción con el objetivo de validar su eficacia, impacto y nivel de riesgo en entornos limitados, con documentación formal de resultados y autorizaciones antes de su despliegue.

Comentario de la Administración

Se definirá un protocolo interno con los criterios de uso de la IA considerando los factores mínimos. Actualmente en el club no se desarrolla software ni análisis de datos usando esta tecnología. Se incorporará esta tecnología en los planes de capacitación del área.

C. Gestión de sistemas de información

En la revisión de estas actividades se verificó lo siguiente:

1. Funcionalidad del sistema financiero contable. (SKILL)
2. Diagrama de la integración de los sistemas de información.
3. Validación de los sistemas, aplicativos y equipos obsoletos en caso de existir.
4. Inventario de los activos (software, hardware, aplicaciones) gestionados por TI.
5. Lista de los requerimientos o necesidades para la atención de los sistemas de información (desarrollo de sistemas) del periodo.
6. Marco normativo para la atención de requerimientos.
7. Inventario de licenciamiento.

Se comunican las siguientes observaciones de mejora:

C.1 Estrategia formal para la migración de Windows 10 a Windows 11

Normal
✔

De acuerdo con los comunicados oficiales de Microsoft, el soporte extendido de Windows 10 finalizó el 14 de octubre de 2025, lo que implica el cese de actualizaciones de seguridad gratuitas, asistencia técnica y mejoras funcionales.

Durante la revisión de la evidencia documental remitida, no se identificó una estrategia, plan o programa formal que defina el proceso de migración hacia Windows 11 en los equipos de la organización.

Tampoco se observaron documentos que detallen fases de ejecución, inventario de equipos, análisis de compatibilidad, estimación de costos, ni cronogramas de despliegue.

Esta situación podría exponer a la entidad a riesgos de seguridad, incompatibilidad y pérdida de soporte técnico, afectando la disponibilidad y estabilidad de los entornos operativos que continúan utilizando Windows 10.

Criterio:

En COBIT 2019, los procesos BAI09 Gestionar activos y DSS01 Gestionar operaciones, establecen la necesidad de mantener actualizada la infraestructura tecnológica para asegurar la continuidad operativa y la seguridad de la información.

Adicionalmente la ISO/IEC 27002:2022, en el control 8.9 Gestión del ciclo de vida de los activos indica que se requiere que los componentes de software y hardware sean mantenidos y actualizados conforme a su soporte oficial.

Recomendaciones:

1. Diseñar e implementar un plan formal de migración a Windows 11, que incluya diagnóstico de compatibilidad de hardware, estimación presupuestaria, cronograma de ejecución y estrategias de contingencia.

2. Priorizar la migración en equipos críticos, tales como estaciones de trabajo de usuarios con acceso a sistemas sensibles y servidores de soporte operativo.

3. Monitorear y documentar el avance del proceso, asegurando trazabilidad, gestión de riesgos y validación de controles de seguridad post-migración.

<u>Comentario de la Administración</u>

Se realizo el inventario de los equipos que actualmente usan Windows 10 dentro de la organización, su potencial de migración a una nueva versión de S.O. y se incluye dentro del plan de mantenimiento de abril 2026. Se incluye en el presupuesto del 2026 la compra de las licencias de Windows 11 de reemplazo a las licencias Windows 10.

C.2 Registros formales de cambios realizados a los sistemas de información

Normal
✔

A partir de la evidencia aportada, no se identificó una lista formalmente documentada de los cambios realizados a los sistemas de información de la entidad. No se dispone de registros que permitan dar seguimiento a las modificaciones efectuadas, ni evidencia que respalde su autorización, ejecución y validación posterior.

La ausencia de controles documentados sobre la gestión de cambios limita la posibilidad de auditar las modificaciones realizadas a los sistemas y aumenta el riesgo de errores, cambios no autorizados o afectaciones a los sistemas que soportan los procesos administrativos y financieros.

Criterio

COBIT 2019 en el proceso BAI06: Gestionar los Cambios indica lo siguiente: “La empresa debe gestionar todos los cambios de manera controlada, asegurando que sean registrados, evaluados, autorizados y probados antes de su implementación.”

Recomendaciones

1. Implementar un registro formal de cambios a los sistemas de información, que documente al menos la descripción del cambio, fecha, responsable, autorización y validación posterior.

2. Documentar la validación posterior de los cambios realizados, con el propósito de confirmar que las modificaciones implementadas cumplen con el objetivo previsto y no generan impactos no deseados en la operación de los sistemas.

3. Mantener el registro de cambios actualizado y disponible como evidencia de control, de forma que facilite el seguimiento interno y la revisión durante procesos de auditoría.

Comentario de la Administración

El departamento de TI no realiza cambios a los sistemas de información. Estos son solicitados al proveedor y existe un registro formal de la solicitud vía correo, la respuesta del proveedor y la comunicación al usuario final y retroalimentación de este. Se realizará un documento resumen que incorpore todas las solicitudes realizadas al proveedor y sus respuestas. Se generará un archivo digital en donde se almacenes todos los cambios solicitados y resultados obtenidos.

C.3 Limitaciones del sistema SKILL-4 y debilidades en los controles automatizados que soportan la información financiera

Elevado
✔

El Country Club El Castillo no cuenta con un sistema ERP integral que centralice y automatice los procesos financieros y administrativos. Actualmente, la entidad utiliza el sistema SKILL-4, el cual presenta limitaciones funcionales y de control relevantes desde la perspectiva de la auditoría financiera.

Se identificó que el Estado de Cambios en el Patrimonio no se genera automáticamente desde el sistema, y que determinados registros contables se realizan mediante asientos manuales, incluyendo reclasificaciones y ajustes, según lo indicado en la reunión sostenida con el área de Contabilidad. Esta práctica incrementa la dependencia de procesos manuales y reduce el nivel de automatización y control sobre la información financiera.

Los procesos de autorización, facturación y demás respaldos se gestionan de forma física, sin una integración directa con el sistema, lo cual dificulta la trazabilidad completa de las transacciones y el seguimiento automatizado de los controles.

En cuanto al control de accesos, cada usuario cuenta con una clave individual para acceder a todos los módulos del sistema; sin embargo, se evidenció que el sistema no solicita el cambio periódico de contraseñas, lo cual debilita los controles de seguridad lógica.

La contabilidad se cierra de forma mensual; no obstante, el sistema no genera automáticamente los Estados Financieros completos. La información se extrae del sistema y los estados financieros se confeccionan de manera externa, generándose únicamente el Estado de Resultados y el Flujo de Efectivo, lo cual incrementa el riesgo de errores en el proceso de preparación de la información financiera.

Criterio

COBIT 2019 en el proceso DSS06: Gestionar los Controles del Negocio indica lo siguiente:

"Cuando los controles automatizados no estén disponibles o no sean suficientes, la empresa debe implementar controles manuales o compensatorios, debidamente documentados y supervisados."

Recomendaciones

1. Evaluar las limitaciones actuales del sistema SKILL-4 y definir un plan de acción para atender las observaciones indicadas anteriormente:

a) Formalizar controles compensatorios para los asientos manuales, ajustes y reclasificaciones contables realizados fuera de las funcionalidades automáticas del sistema SKILL-4, documentando el motivo del registro, el responsable de su elaboración y la evidencia de revisión y aprobación por parte de un funcionario distinto, con el fin de mitigar el riesgo de errores o modificaciones no autorizadas en la información financiera.

b) Fortalecer la trazabilidad documental entre los procesos físicos de autorización, facturación y demás respaldos, y los registros contables efectuados en el sistema SKILL-4, mediante mecanismos de referencia cruzada que permitan identificar claramente el soporte de cada transacción registrada y facilitar su verificación durante procesos de revisión o auditoría.

c) Definir e implementar lineamientos básicos de seguridad lógica para el acceso al sistema SKILL-4, incluyendo el establecimiento de cambios periódicos de contraseñas y buenas prácticas de uso de credenciales, con el propósito de reducir el riesgo de accesos indebidos a los módulos que procesan información financiera.

d) Estandarizar el proceso de preparación de los estados financieros que se elaboran a partir de información extraída del sistema SKILL-4, definiendo etapas claras de extracción, conciliación, elaboración, revisión y validación documentada, a fin de disminuir el riesgo de errores y asegurar la consistencia y confiabilidad de la información financiera generada.

Comentario de la Administración

Se coordinará con la Jefatura Financiera las recomendaciones realizadas.

D. Gestión de la continuidad de negocio

En la revisión de estas actividades se verificó lo siguiente:

1. Marco normativo para la gestión de la continuidad de negocio.
2. Análisis de Impacto de Negocio (BIA).
3. Plan de continuidad de negocio.
4. Plan de continuidad de recuperación.
5. Plan de pruebas del plan de continuidad 2025.
6. Planes de acción de los resultados de las pruebas al plan de continuidad.
7. Evidencia de capacitación a los usuarios sobre la continuidad de operaciones.
8. Pruebas de validación de respaldos.

Se comunican las siguientes observaciones de mejora:

D.1 Ausencia de un Análisis de Impacto al Negocio (BIA)

Elevado
✔

No se identificó la existencia de un Análisis de Impacto al Negocio (BIA) que permita determinar el impacto operativo, financiero y reputacional ante la interrupción de los procesos críticos del Country Club El Castillo.

No se evidenció documentación que identifique los procesos prioritarios, los tiempos máximos tolerables de interrupción ni los recursos tecnológicos y humanos necesarios para su recuperación.

La ausencia de un BIA limita la capacidad de la administración para comprender y priorizar los impactos derivados de eventos que afecten la continuidad operativa, incluidos aquellos que puedan incidir en los sistemas y procesos que soportan la información financiera.

Criterio

COBIT 2019 en el proceso DSS04: Gestionar la Continuidad indica lo siguiente:

"La empresa debe identificar los procesos críticos del negocio y asegurar que se implementen medidas para mantener la continuidad de las operaciones ante eventos disruptivos." y "La empresa debe analizar el impacto de las interrupciones y definir los requisitos de continuidad, incluyendo tiempos de recuperación y recursos necesarios."

Adicionalmente la ISO 22301:2019 en la cláusula 8.2.2 indica lo siguiente:

"La organización debe establecer, implementar y mantener un proceso de análisis de impacto al negocio, que incluya la identificación de actividades prioritarias y la evaluación de los impactos que pueden resultar de una interrupción." y "El análisis de impacto al negocio debe establecer los períodos máximos tolerables de interrupción para las actividades prioritarias."

Recomendaciones

1. Realizar un Análisis de Impacto al Negocio (BIA) que permita identificar los procesos críticos del negocio, los impactos operativos, financieros y reputacionales asociados a su interrupción, así como los tiempos máximos tolerables de recuperación. Dicho análisis debe documentarse y utilizarse como insumo para la toma de decisiones relacionadas con la continuidad operativa y la protección de los procesos que soportan la información financiera.

2. Identificar y documentar los procesos críticos del negocio y los escenarios de interrupción relevantes, priorizando aquellos procesos y sistemas que soportan la información financiera y administrativa. Esta identificación debe permitir establecer dependencias entre procesos, recursos tecnológicos, personal clave y proveedores, de forma que la administración cuente con una visión clara de los impactos y prioridades ante eventos que afecten la operación normal de la entidad.

Comentario de la Administración

Se presento un plan de impacto y continuidad del negocio ante situaciones que puedan interrumpir los procesos críticos del club, con fecha 20 de diciembre del 2025. Se mejorará el documento de acuerdo con COBIT 2019 en el proceso DSS04: Gestionar la Continuidad, fortaleciendo el Análisis de Impacto al Negocio. Adicionalmente se tiene una metodología de control de riesgos y el impacto en los procesos críticos del negocio.

D.2 Ausencia de un Plan de Recuperación ante Desastres (DRP)

Elevado
✔

Se revisó el documento denominado *"Plan de Recuperación e Integridad de Respaldos",* cuya fecha de última evaluación corresponde a diciembre de 2025.

Dicho documento se encuentra enfocado exclusivamente en la ejecución, almacenamiento y validación de respaldos de bases de datos, incluyendo copias locales, en NAS y en la nube, así como pruebas de restauración de información.

No obstante, el documento revisado no constituye un Plan de Recuperación ante Desastres (DRP), dado que no contempla procedimientos orientados a la recuperación de la operación de los sistemas críticos del negocio. En particular, no se identificaron lineamientos que definan cómo restablecer servicios, aplicaciones, infraestructura tecnológica, accesos de usuarios ni dependencias necesarias para reanudar la operación ante un evento disruptivo.

La existencia de respaldos de información, por sí sola, no garantiza la recuperación oportuna de la operación tecnológica. La ausencia de un DRP limita la capacidad del Country Club El Castillo para restablecer los sistemas que soportan los procesos administrativos y financieros dentro de tiempos aceptables, incrementando el riesgo de interrupciones prolongadas con impacto operativo y financiero.

Criterio

COBIT 2019 en el proceso DSS04: Gestionar la Continuidad indica lo siguiente:

"La empresa debe establecer y mantener capacidades de recuperación para restaurar los servicios de TI en caso de un desastre o interrupción mayor.", "La empresa debe definir planes de recuperación, incluyendo procedimientos, responsabilidades y prioridades, para asegurar la restauración oportuna de los servicios críticos." y *"La empresa debe alinear los planes de continuidad y recuperación con los requisitos del negocio y los resultados del análisis de impacto."*

Recomendaciones

1. Desarrollar e implementar un Plan de Recuperación ante Desastres (DRP) que complemente el plan de respaldos existente y permita gestionar de forma integral la recuperación de los sistemas, aplicaciones y servicios tecnológicos críticos del Country Club El Castillo, más allá de la restauración de la información.

2. Definir dentro del DRP los sistemas críticos del negocio, las prioridades de recuperación, las dependencias tecnológicas y los responsables de ejecutar las acciones de recuperación, considerando un enfoque acorde con el tamaño y la complejidad de la entidad.

3. Establecer tiempos estimados de recuperación para los sistemas y servicios críticos, alineados con los resultados del Análisis de Impacto al Negocio y las necesidades de continuidad operativa.

4. Alinear el Plan de Recuperación ante Desastres con el Análisis de Impacto al Negocio y el Plan de Continuidad del Negocio, de forma que exista coherencia entre la identificación de impactos, la estrategia de continuidad y las acciones de recuperación tecnológica.
5. Documentar, mantener actualizado y comunicar el DRP al personal involucrado, asegurando que constituya una herramienta práctica para reducir el impacto operativo y financiero ante eventos disruptivos.

<u>Comentario de la Administración</u>

El club cuenta con un Plan de Operación Alternativa y un Plan de Continuidad Integral. Se mejorará el Plan de Recuperación ante Desastres (DPR) que actualmente tiene el club, tomando como base el documento ya existente en el club y fortaleciéndolo.

E. Seguimiento a recomendaciones del periodo anterior

Se presenta a continuación la matriz de seguimiento de recomendaciones que se ha incorporado en informes sobre tecnología de información.

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.

	Carta	Asunto	Estado		
			Atendido	En proceso	Se mantiene
E.1	**31/12/2023**	**HALLAZGO # 2 - Procedimiento para la revisión periódica de usuarios y perfiles de acceso** **Riesgo Medio**	☒	☐	☐

Dentro de la documentación aportada, no se observó la existencia de un procedimiento para gestionar revisiones periódicas de usuarios y sus privilegios.

Recomendación:

Como parte de los esfuerzos para desarrollar procedimientos operativos para gestionar las TI empresariales, es importante que se incluyan las políticas y procedimientos respectivos para:

a. Revisión periódica de usuarios: este proceso tiene como objetivo que, en intervalos establecidos durante el año, se realice una revisión de los usuarios registrados en toda la plataforma tecnológica, para determinar que todos los existentes son viables, e identificar posibles desviaciones a los controles. Comprendemos que la organización ejecuta este tipo de prácticas, pero no están formalizadas.

b. Revisión periódica de accesos y privilegios otorgados: otra buena práctica es que periódicamente, una o dos veces al año, se realice una revisión de los privilegios asociados a los usuarios en los sistemas. La tarea de TI es la de emitir un reporte con los usuarios y sus privilegios de acceso, para que las áreas de negocio (Jefaturas) validen que estos se encuentran conformes a los requerimientos del área, y posterior a la revisión, TI aplique los cambios requeridos y se mantenga documentación de la revisión y cambios solicitados. Lo anterior implica diseñar los procedimientos respectivos.

<u>Comentarios de la administración 2023:</u>

Se formalizará el proceso de revisión periódica de los usuarios y se establecerá el procedimiento requerido para la revisión periódica de accesos y privilegios otorgados a los usuarios, autorizadas por las respectivas Jefaturas.

Comentarios de la administración 2024:

Se elabora un Procedimiento para la revisión periódica de usuarios y perfiles de acceso. Este procedimiento está en pruebas desde el I Trimestre del 2024, para su implementación definitiva en el primer trimestre del 2025. Se adjunta procedimiento como evidencia.

Comentarios de la administración 2025:

El club ya tiene un procedimiento para la revisión periódica de usuarios y perfiles de acceso y se hacen las revisiones.

	Carta	Asunto	Estado		
			Atendido	En proceso	Se mantiene
E.2	**31/12/2023**	**HALLAZGO # 4 - Mejoras en la gestión de usuarios Riesgo Medio**	☐	☒	☐

Uso de usuarios genéricos en el servidor "Active Directory".

En el servidor Active Directory se observó el uso de usuarios genéricos, sin que se disponga de documentación formal sobre el uso de estos. Algunos de los usuarios observados corresponden a: asociación, comedor, info, saunas, seguridad, sistemas viejos, socio, sodas, tecc, asambleas, diseño, atsocio, pistahielo, piscina, biomecánicos, capitanes, emtec.

Recomendación:

a. Respecto a los usuarios genéricos, se recomienda que cada persona de negocio que requiere de un usuario para ingresar a servidores tenga un usuario asignado de uso personal, y se elimine la práctica de uso de usuarios genéricos. Por otra parte, también se recalca que en muchas empresas existen condiciones de negocio que ameritan el uso de este tipo de usuarios, sin embargo, para estos casos, se deben mantener listas formales y autorizadas de los usuarios que deben mantener esta condición y normarse en las políticas respectivas.

Comentarios de la administración 2023:

Se procederá a realizar un análisis de las recomendaciones brindadas, para proceder con las depuraciones que apliquen. Se generará una matriz de privilegios para generar nuevos accesos por puesto de trabajo, logrando minimizar el riesgo, a partir del principio de 'mínimo acceso requerido'.

Comentarios de la administración 2024:

Se está implementando una metodología para gestionar los usuarios genéricos debido a la alta rotación de áreas como A&B u Recreación. Se espera implementar en el tercer trimestre 2024.

Comentarios de la administración 2025:

Se está trabajando en este punto, debido a la alta rotación de áreas como A&B y Recreación y Deportes. A nivel de Skill cada usuario es único y debido a que se comparte el equipo de cómputo a nivel de AD se han usado usuarios genéricos. Se espera implementar en el tercer trimestre 2026 las modificaciones requeridas. El nivel de acceso a los sistemas de skill es único por usuario. Por ejemplo, los edecanes de recreación rotan en varias áreas y en saunas podrían estar diferentes edecanes en la misma semana, usando el mismo computador. Para ingresar al equipo usan un usuario genérico 'Saunas', pero cuando van a ingresar a los sistemas de información, ya usan un usuario único.

	Carta	Asunto	Estado		
			Atendido	En proceso	Se mantiene
E.3	**31/12/2022**	**HALLAZGO # 1 Falta de gestión de riesgo de TIC Riesgo Alto**	☒	☐	☐

Se carece de un método formal a través del cual el departamento de TI identifique, gestione y supervise los riesgos de TIC relevantes para el negocio.

Recomendación:

Desarrollar e implementar una metodología de gestión de riesgo mediante la cual se identifiquen analicen, evalúen, administren y supervisen los riesgos relevantes de TIC. La gestión de riesgos que se implemente deberá suministrar información clave para que sea utilizada por el negocio en la toma de decisiones. La gestión de riesgos de TIC que se desarrolle deberá contemplar al menos: contemplar al menos:

- ✓ Riesgos de Operación.
- ✓ Riesgos de Continuidad.
- ✓ Riesgos de Seguridad de Información.

Comentarios de la administración 2023:

Con el ingreso del nuevo jefe de Tecnologías de Información, se proyecta que en el mes de diciembre 2023 se iniciará el desarrollo de la metodología de gestión de riesgos de TIC. Se generará un manual que incorpore esta metodología y sea útil para la toma de decisiones de la organización.

Comentarios de la administración 2024:

Se está elaborando una Metodología de Gestión de Riesgo, para identificar y administrar adecuadamente los riesgos de operación, de seguridad de la información y de continuidad. Se proyecta finalizarlo e implementarlo en el primer trimestre 2025. Ya se cuenta con un documento preliminar que se está revisando según una normativa adecuada.

Comentarios de la administración 2025:

El club ya cuenta con una metodología de gestión de riesgos de TI.

	Carta	Asunto	Estado		
			Atendido	En proceso	Se mantiene
E.4	**31/12/2022**	**HALLAZGO # 2 Debilidades físico-ambientales en el Centro de procesamiento** **Riesgo Alto**	☐	☐	☒

Las condiciones físico-ambientales encontradas que se describen a continuación hacen que el centro de procesamiento principal esté altamente vulnerable a sufrir violaciones que provocarían daños en los equipos que consecuentemente afectaría la continuidad de las operaciones.

Seguidamente se detallan estas condiciones:

- El cuarto donde se ubican los equipos se encuentra distanciado de las oficinas de TI, lo que limita el accionar inmediato de estos funcionarios en acciones de emergencias que se pueda presentar en los equipos.
- El centro de procesamiento se ubica en pasillos de alto tránsito de personas ajenas a los funcionarios de TI.
- Los materiales con los que está construido el centro de procesamiento pueden ser fácilmente violentados.
- La puerta de ingreso es de un material fácilmente violentado y cuenta con un dispositivo convencional de cerradura que la hace más vulnerable.

Recomendación:

Reubicar el centro de procesamiento principal.

La reubicación del centro debe considerar el análisis de diversas alternativas, las cuales deberán ser sometidas a un estudio de costo/beneficio, seleccionando la que permita eliminar las debilidades identificadas.

Comentarios de la administración 2023:

Se programa para enero del 2024 el análisis del proyecto de mejoras físico-ambientales del Centro de Procesamiento de la organización.

Comentarios de la administración 2024:

Se analizó a inicio del año 2024 con la Jefatura Financiera la factibilidad presupuestaria de iniciar este proyecto, sin embargo, se indicó que hasta el presupuesto del 2025 se podrá iniciar el análisis de una reubicación del Data Center actual. Se requiere no solo migrar equipos físicos y aires acondicionados, sino cableados estructurados y fibra óptica de todo el club. Se procede a cotizar un acceso automático al Data Center para mejorar la seguridad física.

Comentarios de la administración 2025:

Este hallazgo se mantiene en el mismo estado, ya que no se ha autorizado el traslado por el impacto que podría generar a nivel de operaciones.

	Carta	Asunto	Estado		
			Atendido	En proceso	Se mantiene
E.5	**31/12/2022**	**HALLAZGO # 3 Falta de una política formal de seguridad de información** **Riesgo Alto**	☒	☐	☐

No se cuenta con una política formal de seguridad de la información en donde se establezcan todas las directrices con las cuales se administrarán los elementos que gestionan la información.

Sin esta política los esfuerzos de seguridad de información que el personal de TI desarrolle carecen de respaldo y pudiese no estar alineados a las necesidades del negocio.

Recomendación:

Formalizar una política de seguridad de la información, en la cual se definan como mínimo directrices para administrar:

- ✓ Clasificación de la información y la retención de datos para cada tipo.
- ✓ Gestión sobre la información que viaje fuera de la red interna.
- ✓ Gestión sobre la información impresa.
- ✓ Gestión sobre las contraseñas de acceso.
- ✓ Accesos a servicios como correo electrónico, sitios web, redes sociales, entre otros.
- ✓ Activación/desactivación de puertos de acceso.
- ✓ Capacidades de monitoreo sobre los elementos que gestionen la seguridad de la información.
- ✓ Responsabilidades de la seguridad de la información.
- ✓ Gestión de riesgos e incidentes asociados a la seguridad de la información.

El desarrollo y formalización de la política de seguridad de información debe ser un trabajo en el cual participen las distintas unidades de la Organización.

Comentarios de la administración 2023:

En el mes de noviembre del 2023 se inicia el desarrollo de una política formal de seguridad de la organización que contemple las directrices recomendadas. Esta política estará alineada con las necesidades empresariales.

Comentarios de la administración 2024:

Se está elaborando una política formal de seguridad de la organización, basado en las mejores prácticas de una normativa de seguridad de la información. Se proyecta finalizarlo e implementarlo en el segundo trimestre 2025. Ya se cuenta con un documento preliminar que se está revisando según una normativa apropiada.

Comentarios de la administración 2025:

El club ya cuenta con una política de seguridad de la información.

	Carta	Asunto	Estado		
			Atendido	En proceso	Se mantiene
E.6	**31/12/2022**	**HALLAZGO # 4 Debilidades en la cultura de seguridad de la información** **Riesgo Alto**	☒	☐	☐

No se identificó un programa formal de culturización en temas de seguridad de la información, a través del cual se instruya periódicamente a los colaboradores.

Recomendación:

Desarrollar e implementar un programa de culturización que permita concientizar periódicamente a los colaboradores en temas como:

- ✓ Qué es seguridad de la información.
- ✓ Lineamientos asociados a la seguridad de información.
- ✓ Sus responsabilidades en la seguridad de la información.
- ✓ Gestión de recursos que involucran seguridad de la información.

Comentarios de la administración 2023:

En el mes de noviembre del 2023 se inicia un programa integral de culturización de los colaboradores en temas de seguridad informática y de la información. Este programa deberá formar parte del programa de mejora continua de la organización.

Comentarios de la administración 2024:

Se está elaborando un programa formal de culturización en temas de seguridad de la información, basado en las mejores prácticas de una normativa de seguridad de la información. Se proyecta finalizarlo e implementarlo en el primer trimestre 2025. Ya se cuenta con un documento preliminar que se está revisando según una normativa apropiada.

Comentarios de la administración 2025:

El club ya cuenta con un programa de culturización en seguridad de la información.

	Carta	Asunto	Estado		
			Atendido	En proceso	Se mantiene
E.7	**31/12/2022**	**HALLAZGO # 5 Falta de procedimiento formal sobre la operación del centro de procesamiento** **Riesgo Medio**	☒	☐	☐

No se cuenta con un procedimiento que detalle las tareas que se ejecutan en la operación del centro de procesamiento.

Recomendación:

Desarrollar e implementar un procedimiento que detalle las diferentes rutinas que se ejecutan en el centro de procesamiento; de forma tal que el procedimiento recopile el detalle de ejecución tanto las tareas automatizadas de mantenimiento, así como ejecución de tareas de procesamiento de información que son aplicadas de manera periódica.

Comentarios de la administración 2023:

En el mes de enero 2024 se iniciará el desarrollo de un procedimiento formal de operación del centro de procesamiento, que incorpore todas las rutinas de mantenimiento, operación y procesamiento.

Comentarios de la administración 2024:

Se está trabajando en la elaboración de un procedimiento detallado de gestión de rutinas del Centro de Procesamiento. El mismo se elabora siguiendo las mejores prácticas y está en proceso de prueba y depuración para su implementación en el cuarto trimestre del 2024.

Comentarios de la administración 2025:

El club ya cuenta con un procedimiento para la ejecución de rutinas del centro de procesamiento.

	Carta	Asunto	Estado		
			Atendido	**En proceso**	**Se mantiene**
E.8	**31/12/2022**	**HALLAZGO # 6 Falta de un plan formal de mantenimiento Riesgo Medio**	☒	☐	☐

No se cuenta con un instrumento en el cual se planifique a lo largo de un periodo determinado los distintos tipos de mantenimiento preventivo que son soportados por el personal de TI.

Recomendación:

Implementar un planificador que permita organizar el trabajo de mantenimientos preventivos, de forma tal que todo el personal de TI involucrado en los mismos pueda contar con la distribución de trabajo de este tipo de manera oportuna.

Comentarios de la administración 2023:

En el mes de febrero 2024 se iniciará el desarrollo de un plan anual de mantenimiento de la infraestructura de TI, especificando cronogramas de trabajo por colaborador de TI y área funcional.

Comentarios de la administración 2024:

Se elabora un Plan de Mantenimiento Preventivo Anual, segregado por prioridad de equipo y plan específico. Este plan está en pruebas desde el I Trimestre del 2024, para su implementación definitiva en el segundo semestre del 2024.

Comentarios de la administración 2025:

Se elabora un Plan de Mantenimiento Preventivo Anual, segregado por prioridad de equipo y plan específico. Este plan está en pruebas desde el I Trimestre del 2024, para su implementación definitiva en el segundo semestre del 2024.

	Carta	Asunto	Estado		
			Atendido	**En proceso**	**Se mantiene**
E.9	**31/12/2022**	**HALLAZGO # 7 Formalización de procedimientos/instructivos técnicos de gestión sobre la infraestructura Riesgo Alto**	☐	☒	☐

No se cuenta con instrumentos formales que sirvan de guía a los funcionarios de TI en la aplicación de reglas de elementos de seguridad asociados a la infraestructura. Hasta el momento la aplicación de dichas reglas se ha venido implementando con un criterio subjetivo.

Recomendación:

Establecer procedimientos técnicos formales mediante los cuales se definan las reglas como las siguientes:

- ✓ Establecimiento y supervisión de las contraseñas.
- ✓ Bloqueo de usuarios.
- ✓ Gestión de usuarios con permisos o incapacidades.
- ✓ Restricciones de navegación de páginas de internet, redes sociales y similares.
- ✓ Activación/desactivación de puertos.

Las reglas deben tener el nivel de detalle suficiente que sirva de instructivo de aplicación para los funcionarios de TI. Además, la creación de cada regla debe estar alineada a la política de seguridad de información que se utiliza.

Comentarios de la administración 2023:

En el mes de diciembre 2023 se iniciará la revisión del proceso de gestión de contraseñas del ERP Skill que se utiliza en la organización.

Comentarios de la administración 2024:

Se está trabajando en la elaboración de un procedimiento enfocado a la seguridad de la infraestructura como parte de un programa de gestión de la seguridad de la información. El misma se elabora siguiente las mejores prácticas y está en proceso de prueba y depuración para su implementación en el cuarto trimestre del 2024.

Comentarios de la administración 2025:

Se desarrolla un procedimiento para la ejecución de rutinas en el centro de procesamiento, enfocado a la Gestión de la infraestructura.

	Carta	Asunto	Estado		
			Atendido	En proceso	Se mantiene
E.10	**31/12/2022**	**HALLAZGO # 8 Debilidades en la gestión de contraseña del aplicativo** **Riesgo Alto**	☐	☒	☐

Las contraseñas que gestiona el SKILL carece de controles como vencimiento y control de históricos.

Recomendación:

Las contraseñas del aplicativo deben gestionarse con las mismas políticas y procedimientos técnicos de contraseñas que el departamento de TI ha implementado para administrar las contraseñas de ingreso al ambiente productivo de la Organización.

Comentarios de la administración 2023:

En el mes de diciembre 2023 se iniciará la revisión del proceso de gestión de contraseñas del ERP Skill que se utiliza en la organización.

Comentarios de la administración 2024:

Se están gestionando las contraseñas de usuarios activos de Skill basado en estructura de seguridad recomendada. Se espera renovar totalidad de contraseñas durante tercer trimestre del 2024.

Comentarios de la administración 2025

Se están gestionando las contraseñas de usuarios activos de Skill basado en estructura de seguridad recomendada. Se espera renovar totalidad de contraseñas durante tercer trimestre del 2026.

	Carta	Asunto	Estado		
			Atendido	**En proceso**	**Se mantiene**
E.11	**31/12/2022**	**HALLAZGO # 11 Falta de un proceso formal para la gestión de incidentes y solicitudes** **Riesgo Alto**	☒	☐	☐

Se carece de un proceso formal para registrar, documentar, dar trazabilidad y supervisar todos los casos que los usuarios reportan a los funcionarios de TI. La práctica actual que la Organización tiene presenta los siguientes problemas:

- ✓ Se carece de definición de niveles de definición de niveles de servicio (SLA) que les permitan a las partes establecer ventanas de tiempo en la atención y solución de casos.
- ✓ No hay definición de tipos de casos, lo que impide gestionar los mismos de una forma más proactiva.
- ✓ Se carece de una definición de escalamiento que permita gestionar cada caso con la especialización técnica que se necesita optimizando con ello los recursos de TI.
- ✓ Los funcionarios de TI reciben cualquier tipo de caso por correo electrónico, llamada telefónica, radio o consulta personal; lo que imposibilita tener un registro centralizado y controlado.
- ✓ No hay un registro de acciones asociado a la atención, respuesta y solución de cada caso.
- ✓ Hay pérdida de casos, en ocasiones los usuarios recurren directamente a consultar al proveedor del SKILL.
- ✓ Existen necesidades ocultas de automatización que no han sido comunicadas ni analizadas.

Recomendación:

Para contar con un debido proceso de gestión de solicitudes e incidentes se debe desarrollar las siguientes acciones:

1. Desarrollo de un procedimiento formal para la gestión de casos que contemple al menos:

    a) La lista de servicios de TI que será soportada.
    b) Clasificación de casos de atención.
    c) Definición de niveles de servicio para la atención y solución de casos, según su clasificación.
    d) Niveles de escalamiento.
    e) Proceso de inclusión de casos.
    f) Información que se registrará, en cada estado, en el proceso de gestión de casos.
    g) Responsabilidades.
    h) Gestión de casos de emergencia.
    i) Estadísticas que se desean obtener de la gestión de casos. En el desarrollo del procedimiento deben participar tanto personal de TI como áreas usuarias.

2. Implementar un instrumento que operativice lo definido en el procedimiento. El instrumento debe ser el único medio en el cual se registren los casos y debe tener la capacidad de documentar la información necesaria y de controlar los tiempos definidos. Además, debe poder generar información estadística de la gestión.

Comentarios de la administración 2023:

En el mes de noviembre del 2023 se inicia el desarrollo de un procedimiento para la gestión de incidentes y solicitudes de usuarios al departamento de TI. Este procedimiento incorporara los instrumentos adecuados para la gestión de los diferentes niveles de servicio que ofrece el departamento de TI.

Comentarios de la administración 2024:

Se está trabajando en la elaboración de un procedimiento enfocado a la gestión de incidentes y solicitudes. El misma se elabora siguiente las mejores prácticas y está en proceso de prueba y depuración para su implementación en el cuarto trimestre del 2024.

Comentarios de la administración 2025:

Se elabora un Procedimiento formal para la atención de incidentes y solicitudes.

	Carta	Asunto	Estado		
			Atendido	**En proceso**	**Se mantiene**
E.12	**31/12/2022**	**HALLAZGO # 12 Falta de estrategia contingente alterna Riesgo Alto**	☒	☐	☐

Actualmente la estrategia de contingencia de equipos de procesamiento está concentrada en el cuarto de equipos; si se presentara una emergencia que dañara dicho cuarto, la continuidad de las operaciones de TI se vería altamente comprometida.

Recomendación:

Implementar una estrategia de operación alternativa fuera de las instalaciones del centro de procesamiento, y a lineado a las necesidades del negocio, que le permitan mantener la operación en caso de que este sitio se vea afectado por una emergencia.

Comentarios de la administración 2023:

En el mes de abril del 2024 se iniciará el desarrollo de un plan de contingencia alterna.

Comentarios de la administración 2024:

Se elabora una estrategia de contingencia para la operación alternativa de los server y sistemas. En proceso con fecha proyectada de implementación al I Trimestre del 2025.

Comentarios de la administración 2025:

El club ya cuenta con una estrategia de operación alternativa.

	Carta	Asunto	Estado		
			Atendido	**En proceso**	**Se mantiene**
E.13	**31/12/2022**	**HALLAZGO # 13 Falta de un plan de continuidad del negocio Riesgo Alto**	☐	☒	☐

No existe un plan formal mediante el cual se estructuren todos los procedimientos, recursos y responsables que se necesitan para que el negocio se encuentre preparado para gestionar una contingencia de manera integral.

Recomendación:

Desarrollar y formalizar un plan de continuidad integral. El plan debe considerar al menos:

- ✓ Procedimientos para estar preparados antes de un desastre.
- ✓ Gestión de Riesgos de Continuidad.
- ✓ Análisis del impacto sobre el negocio (BIA).

- ✓ Estrategias de recuperación.
- ✓ Declaración de desastre.
- ✓ Recursos de TI a recuperar.
- ✓ Equipos responsables con sus roles.
- ✓ Procedimientos para trabajo en contingencia.
- ✓ Procedimientos para trabajo de recuperación.

El desarrollo de este plan deberá considerar y revalorar todos los esfuerzos que el departamento de TI ha gestionado en materia de continuidad. El plan deberá ser probado periódicamente, y actualizado siempre que ocurra algún cambio que afecte la continuidad de las operaciones.

Comentarios de la administración 2023:

En el mes de mayo del 2024 se iniciará el desarrollo de un plan integral de continuidad del negocio.

Comentarios de la administración 2024:

Se está trabajando en la elaboración de un plan de continuidad de negocio como parte de un programa de gestión de la seguridad de la información. El mismo se elabora siguiendo las mejores prácticas y está en proceso de revisión y depuración para su implementación en el primer trimestre del 2025.

Comentarios de la administración 2025:

El club ya cuenta con un plan de continuidad integral.

Comentario de la auditoría

Este plan requiere mejorarse para incluir lo indicado en la recomendación.