17 de abril de 2024
AI-As-011-2024

Señor:
Alberto López Chaves
Gerente general

Asunto: *Servicio de asesoría sobre la gestión de la seguridad de la información institucional*

Estimado señor:

La Auditoría en cumplimiento del Plan Anual de Trabajo, revisa la gestión de seguridad de la información de la Institución, con el objetivo de verificar si se realiza de acuerdo con la normativa y las mejores prácticas, obteniéndose los resultados siguientes:

Gobernanza de la seguridad

1. Estrategia para la seguridad de la información

El ICT no cuenta con una estrategia formal para la seguridad de la información alineada con los objetivos estratégicos institucionales.

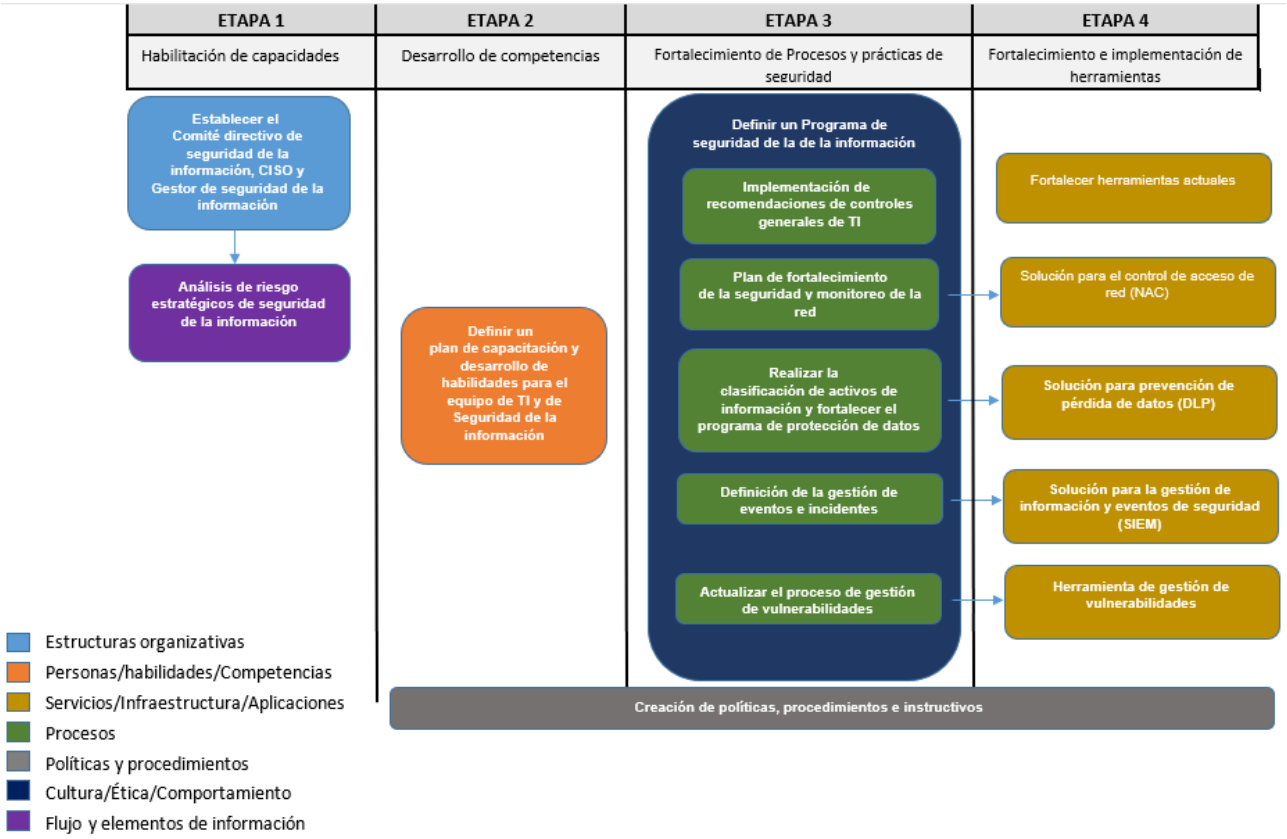
COBIT 2019[1] -marco de gestión de TI aprobado por la Junta Directiva en diciembre de 2020-, en su proceso APO02 *Gestionar la Estrategia*, establece la necesidad de establecer y formalizar una estrategia de TI que incluya la seguridad y que debe estar en línea con los objetivos y expectativas del negocio. Específicamente destacan los procesos 03, 04, 05 y 06 sobre definir el objetivo de las capacidades de TI, realizar un análisis de diferencias o de brechas, definir el plan estratégico y la hoja de ruta, así como comunicar la estrategia y la dirección de TI.

[1] SJD-498-2020 (14-12-2020)

(506) 2299.5800
San José, Costa Rica
www.ict.go.cr
www.visitcostarica.com

Las NTGCTI [2] en el punto XI, *Seguridad y ciberseguridad* estipula que, los procesos institucionales deben considerar los requerimientos de seguridad de la información, de forma tal que propicie el cumplimiento de los objetivos institucionales, como las responsabilidades que impone el ordenamiento jurídico, normativa vigente y demás compromisos contractuales adquiridos por la institución.

El manual de preparación para el examen CISM16°edición de ISACA, detalla las etapas para gestionar la seguridad de la información siguientes:



Fuente: Tomado del curso Auditando la Ciberseguridad y Seguridad de la Información del Instituto de Auditores Internos de Costa Rica, basado en el manual de preparación para el examen CISM 16°edición de ISACA, noviembre 2023.

[2] Marco de Gestión de Tecnología de Información Institucional emitido por el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones -MICITT-

2. Política de la seguridad de la información institucional -PSII-:

La Junta Directiva aprueba (22/12/22)[3] las políticas informáticas institucionales[4] en las cuales se incluye la PSII; sin embargo, ésta no ha sido divulgada en el ICT.

La Ley General de Control Interno -LGCI-, artículo 15, establece que, es responsabilidad del jerarca y los titulares subordinados divulgar internamente, las políticas, las normas y los procedimientos de control que garanticen la prevención de todo aspecto que conlleve a desviar los objetivos y las metas trazados por la institución en el desempeño de sus funciones.

3. Sistema de gestión de seguridad de la información -SGSI-

El SGSI institucional tiene oportunidades de mejora en los temas siguientes:

3.1 Roles y responsabilidades

La Institución no cuenta con un área o persona encargada formalmente de la seguridad de la información, además, no se indica en las PSII si las responsabilidades en seguridad de la información se pueden delegar a un tercero.

La jefatura de TI con la asesoría de una empresa contratada en seguridad, realiza esfuerzos para atender las acciones de un rol de CISO[5] . Además, ha definido roles en el procedimiento de restauración de la plataforma tecnológica; pero no están actualizadas[6].

Las NTGCTI[7], en el punto XI, *Seguridad y ciberseguridad* norma, que la institución debe tener y aplicar en forma consistente una estructura formal al nivel institucional, que permita establecer las acciones para administrar la seguridad de la información, ciberseguridad debidamente respaldada con la política de seguridad de la información / ciberseguridad.

---

[3] Comunicado de acuerdo SJD-358-2022
[4] DTI-456-2022 emitido por el Depto. de TI
[5] Acrónimo de Chief Information Security Officer
[6] Emitidas el 14-08-2018
[7] Marco de Gestión de Tecnología de Información Institucional emitido por el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones -MICITT-

COBIT 2019 en su proceso APO13.01 *Establecer y mantener un sistema de gestión de seguridad de la información* (SGSI), establece que, se debe definir y comunicar los roles y responsabilidades de la gestión de seguridad de la información.

La norma ISO 27001:2022 (E), apartado 5.3 *Roles, responsabilidades y autoridades en la organización* indica que, se debe designar a personas responsables de garantizar el SGSI, asignar responsabilidades específicas relacionadas con la seguridad de la información en toda la organización y establecer líneas claras de autoridad para la toma de decisiones en relación con la seguridad de la información.

3.2 Gestión de los riesgos de la seguridad de la información.

El ICT no determina los riesgos tecnológicos relacionados con la seguridad de la información en los procesos institucionales. TI gestiona los riesgos administrativos y operativos propios de su unidad, pero no gestiona los riesgos tecnológicos, así como la asesoría en este aspecto a las demás unidades institucionales.

Las NTGCTI, punto IV. *Gestión de riesgos tecnológicos* indica que:

> *"La institución debe establecer un proceso formal de gestión de riesgos que responda a las amenazas que puedan afectar el logro de los objetivos institucionales, basado en una gestión continua de riesgos que esté integrada al sistema específico de valoración del riesgo institucional y considerando el marco normativo que le resulte aplicable.*
>
> *La Unidad de TI debe aplicar el marco de gestión de riesgo tecnológico, con el fin de identificar, valorar, priorizar y gestionar los riesgos al nivel de TI en cualquiera de sus escenarios, que impliquen una eventual afectación a la continuidad operacional, así como la integridad y confidencialidad de la información y el cumplimiento regulatorio de la institución."*

COBIT 2019, APO13.02 *Definir y gestionar un plan de tratamiento de riesgos de seguridad de la información y privacidad*, establece que, se debe mantener un plan de seguridad de la información que describa cómo se debe manejar el riesgo de

(506) 2299.5800
San José, Costa Rica
www.ict.go.cr
www.visitcostarica.com

seguridad de la información y cómo se debe alinear con la estrategia y la arquitectura de la empresa.

La norma ISO 27001:2022 (E), apartado 6.1.3 *Tratamiento de los riesgos de seguridad de la información,* estipula que, la organización debe definir y efectuar un proceso de tratamiento de los riesgos de seguridad de la información para:

a) seleccionar las opciones adecuadas de tratamiento de riesgos de seguridad de la información teniendo en cuenta los resultados de la apreciación de riesgos.
b) determinar todos los controles que sean necesarios para implementar las opciones elegidas de tratamiento de riesgos de seguridad de la información.
c) comparar los controles determinados para comprobar que no se han omitido controles necesarios.

3.3 Protección de los activos tecnológicos y de la información institucional

El ICT no cuenta con procedimientos, directrices u otros que permitan determinar:

- los mecanismos para una protección razonable de los activos de información[8] institucionales –datos, software, hardware, servicios infraestructura y recurso humano- que permitan la gestión de riesgos de los mismos.
- los requerimientos de preservación de la confidencialidad, integridad y disponibilidad de la información, clasificada de acuerdo con su valor, criticidad y sensibilidad a la divulgación o modificación no autorizada.

Las NTGCTI, punto XI *Seguridad y ciberseguridad,* norma que, la institución debe establecer los mecanismos necesarios para asegurar una protección razonable de los activos tecnológicos, activos de información institucionales, dando énfasis en su clasificación como elemento definitorio para establecer los requerimientos de preservación de la confidencialidad, integridad y disponibilidad de la información.

3.4 Concienciación y capacitación en seguridad de la información

[8] Conjunto de información relacionada entre sí, que conforma un tema de interés para el negocio

a) Capacitación del personal de TI en seguridad de la información

TI no cuenta con un programa formal de capacitación y formación en materia de seguridad de la información para el personal.

Las NCISP, norma 2.4 *Idoneidad del personal*, estipula que, las políticas y actividades de capacitación deben dirigirse técnica y profesionalmente con miras a la contratación y actualización de personal idóneo para el logro de los objetivos institucionales.

Las NTGCTI, punto XI *Seguridad y ciberseguridad* indica que, se debe establecer un plan efectivo de capacitación, formación y actualización tecnológica para los funcionarios, contemplando la participación o involucramiento de los usuarios finales, dueños de procesos y responsables de los diferentes procesos y servicios institucionales.

COBIT 2019, práctica de gestión APO07.03 *Mantener las habilidades y competencias del personal*, indica que, se debe identificar las habilidades y competencias disponibles actuales; identificar las brechas entre las habilidades requeridas y las disponibles; y desarrollar planes de acción, como capacitación, contratación, reasignación y cambio de las estrategias de abastecimiento, para resolver las brechas.

b) Estrategia para promover la cultura de seguridad de la información en la institución

El ICT no cuenta con un programa o estrategia para promover la cultura sobre seguridad de la información y privacidad entre los colaboradores internos, externos y proveedores de servicios del Instituto.

Las NTGCTI, punto XI *Seguridad y ciberseguridad* establece que, la Institución debe establecer un plan efectivo de capacitación, formación y actualización tecnológica para los funcionarios, contemplando la participación o involucramiento de los usuarios finales, dueños de procesos y responsables de los diferentes procesos y servicios institucionales.

COBIT 2019, proceso de gestión APO13.02 *Definir y gestionar un plan de tratamiento de riesgos de seguridad de la información y privacidad,* actividad 5,

indica que, se debe implementar programas de formación y concienciación sobre seguridad de la información y privacidad.

3.5 Gestión de incidentes

TI no cuenta con protocolos formalmente establecidos para la gestión de incidentes de seguridad de la información -atención, contención, solución y recuperación-

COBIT 2019, proceso de gestión APO13.02 *Definir y gestionar un plan de tratamiento de riesgos de seguridad de la información y privacidad,* actividad 6, establece que, se debe integrar la planificación, diseño, implementación y monitorización de procedimientos de seguridad de la información y privacidad y otros controles capaces de permitir la prevención, detección rápida de eventos de seguridad y la respuesta a incidentes de seguridad.

La Norma ISO 27001, cláusulas A.16.1.1 y A.16.1.5 sobre *responsabilidades y procedimientos de respuesta a incidentes de seguridad*, norma que, se deben establecer responsabilidades y procedimientos de gestión para asegurarse tener una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información y esa respuesta a incidentes debe ser de acuerdo con procedimientos documentados.

Causas

Las condiciones determinadas se presentan porque:

a. el ICT no cuenta con un "*Plan Estratégico de Tecnologías de Información*" -PETI-, razón por la cual, no se cuenta con la dirección estratégica en TI y de la seguridad de la información.

   La Auditoría comunica a la Administración[9] que no se cuenta con un PETI. La Junta Directiva[10] acuerda contratar la actualización del PETI, a la fecha se encuentra en proceso de contratación.

b. el Comité TI ha avanzado poco en la implementación de COBIT 2019, marco aprobado por la Junta Directiva en diciembre de 2020, TI indica que se debe a

[9] AI-As-008-2023 "Asesoría sobre la automatización de los procesos del ICT"
[10] SJD-189-2023 (24/05/2023)

la atención de la Directriz del MICITT sobre ciberseguridad y la contratación para actualizar el PETI.

c. TI no tiene establecida una estrategia o una hoja de ruta para gestionar la seguridad de la información institucional.

Efectos

Las condiciones determinadas pueden materializar los riesgos siguientes:

- **Estratégico:**
  - daño a la reputación de la Institución por pérdida o compromiso de datos críticos.
  - la Institución no logre alcanzar los objetivos estratégicos establecidos en la misión y visión.

- **Cumplimiento normativo**
  - la normativa emitida por el MICITT y el marco de gestión -COBIT 2019- adoptado por la Junta Directiva en diciembre de 2020.
  - que se afecte negativamente la rendición de cuentas por no estar definidos los roles y responsabilidades de los funcionarios que participan en la seguridad de la información.

- **Operativos:**
  - pérdida de confidencialidad, disponibilidad e integridad de la información institucional.
  - interrupción de servicios y tiempo excesivo de recuperación ante un evento.
  - disponibilidad de sistemas críticos y eventuales contingencias por incumplimiento y exposición a ataques externos.
  - daños de los equipos y posibles accesos no autorizados de la información.
  - que los incidentes se transformen en desastres y afecten de manera significativa la seguridad de la información y continuidad de los procesos institucionales.
  - que los activos estén desprotegidos.

(506) 2299.5800
San José, Costa Rica
www.ict.go.cr
www.visitcostarica.com

Valor agregado de la Auditoría

El valor agregado que la Auditoría está aportando con este preventivo es en lo siguiente:

1. Contribuir con el cumplimiento del objetivo estratégico “Optimizar los procesos”.
2. Fortalecer los objetivos del sistema de control interno:
    a. Proteger y conservar el patrimonio público contra cualquier pérdida, despilfarro, uso indebido, irregularidad o acto ilegal.
    b. Exigir confiabilidad y oportunidad de la información.
    c. Garantizar eficiencia y eficacia de las operaciones.
    d. Cumplir con el ordenamiento jurídico y técnico.
3. Que se administren los riesgos identificados y se fortalezcan los controles para minimizarlos.
4. Mejorar el sistema de gestión de la seguridad de la información en los temas de gobernanza y gestión de riesgos, con el fin de garantizar que los activos de información estén protegidos y cuenten con la preservación de la confidencialidad, integridad y disponibilidad para mitigar la posible materialización.

La Ley Orgánica, artículo 32, establece que la Gerencia es el responsable del eficiente y correcto funcionamiento administrativo de la Institución y debe ejercer las funciones inherentes a su condición de administrador general y jefe superior del Instituto, vigilando la organización, funcionamiento y coordinación de todas sus dependencias y la observación de las leyes, reglamentos y resoluciones de la Junta Directiva, razón por la cual, se comunica lo determinado sobre sistema de gestión de la seguridad de la información, con el propósito que se tomen las acciones pertinentes para que se subsanen las causas identificadas y administrar al menos los riesgos determinados en este servicio preventivo.

Se solicita a la Gerencia, informar a esta Auditoría Interna dentro de los próximos diez días hábiles, sobre las acciones tomadas en relación con este servicio preventivo, a efecto de determinar lo procedente.

(506) 2299.5800
San José, Costa Rica
www.ict.go.cr
www.visitcostarica.com

El presente servicio se realiza con fundamento en las competencias conferidas a la Auditoría Interna en la Ley Orgánica del ICT, artículos 33 y 35, la Ley General de Control Interno, artículo 22, inciso d), las “Normas para el Ejercicio de la Auditoría Interna en el Sector Público”, norma 1.1.4 y en atención del Plan Anual de Trabajo.

Atentamente,

ROMEL ALVAREZ NAVARRO (FIRMA)
Firmado digitalmente por ROMEL ALVAREZ NAVARRO (FIRMA)
Fecha: 2024.04.17 12:41:14 -06'00'

Romel Álvarez Navarro
Auditor interno

KAREN PATRICIA BARQUERO MURILLO (FIRMA)
KAREN PATRICIA BARQUERO MURILLO (FIRMA)
2024.04.17 12:10:07 -06'00'

Karen Barquero Murillo
Ejecutivo de turismo 3

RODRIGO QUIROS TORRES (FIRMA)
Firmado digitalmente por RODRIGO QUIROS TORRES (FIRMA)
Fecha: 2024.04.17 12:34:09 -06'00'

Rodrigo Quirós Torres
Coordinador

C. Sra. Karen Hernández Bonilla
Jefe Departamento de Tecnologías Información
Comité de Tecnología de Información -CTI-
Comité de Auditoría y Riesgo -CAR-
Consecutivo

RAN/RQT/kbm