ICANH

MINISTERIO DE CULTURA

MEMORANDO

ICANH – MI 2023130000009903

Bogotá D.C., 05 de abril de 2023

PARA: **ALHENA CAICEDO FERNANDEZ**
Directora General ICANH.

DE: **EDINSON MURILLO ALBORNOZ**
Jefe Oficina de Control Interno

ASUNTO: Informe final de auditoria al área funcional de Tecnologías de la Información.

Estimada doctora Alhena, cordial saludo:

El presente con el fin de darle a conocer, el resultado de la auditoria al área funcional de Tecnologías de la Información; dicha información, fue socializada con la responsable del área.

Atentamente,

EDINSON MURILLO ALBORNOZ

INFORME DE AUDITORIA N.º 015_2023 AL PROCESO DE GESTIÓN DE TECNOLOGIA DE LA INFORMACIÓN DEL 01 DE ENERO AL 31 DE DICIEMBRE DE 2022.

OBJETIVO

Verificar el cumplimiento de requisitos del Sistema de Gestión de Seguridad de la Información-SGSI bajo la norma ISO 27001:2013 y el Modelo de Seguridad y Privacidad de la Información –MSPI-

ALCANCE

Determinar el cumplimiento de los requisitos del Sistema de Gestión de Seguridad de la Información-SGSI del Instituto Colombiano de Antropología e Historia con sede principal en Bogotá D.C, bajo la norma ISO 27001:2013 y el Modelo de Seguridad y privacidad de la Información –MSPI- en el Proceso de Gestión de Tecnologías de la Información para la vigencia 2022.

CRITERIO

- Normatividad legal Vigente aplicable en la Entidad.
- Capítulos y numerales Norma ISO 27001:2013.
- Caracterización del Proceso de Gestión de Tecnologías de la Información
- Documentación del Sistema de Gestión de Seguridad de la Información de la Entidad

RESULTADO

Durante la auditoría Interna del Sistema de Gestión de Seguridad de la Información-SGSI del Instituto Colombiano de Antropología e Historia, se verificaron los requisitos establecidos en la Norma ISO 27001:2013.

Es así como a través de lista de chequeo de la auditoría, se dejó evidencia de la revisión, verificación y evaluación de los siguientes componentes específicos dentro de los requisitos:

DESCRIPCIÓN	REQUISITO NORMA
Conocimiento de la organización y su contexto, Comprensión de las necesidades y expectativas de las partes interesadas, determinación del alcance del SGSI.	4.1, 4.2, 4.3 y 4.4
Liderazgo y compromiso.	5.1
Política del SGSI.	5.2
Roles, responsabilidades y autoridades en la organización.	5.3
Acciones para tratar riesgos y oportunidades.	6.1
Comunicación.	7.4
Información documentada.	7.5
Planificación y control operacional.	8.1
Valoración de riesgos de la seguridad de la información.	8.2
Mejora continua.	10.2

En desarrollo de la auditoría se verificaron los requisitos legales, lineamientos y reglamentos establecidos en el ICANH, las partes interesadas y los establecidos para el Sistema de Gestión de Seguridad de la Información Norma ISO 27001:2013.

1. REQUISITOS

A. Contexto de la Organización.

Se realizó la verificación del requisito 4.1 conocimiento de la organización y su contexto, respecto a este tema el proceso no hace entrega de documento Contexto ISO/IEC 27001:2013; encontrando que es importante solicitar la alineación con el contexto institucional, con énfasis en el análisis del entorno tecnológico, también es importante documentar la matriz DOFA frente a los temas de seguridad de la información.

B. Comprensión de las necesidades y expectativas de las partes interesadas.

El proceso no cuenta con información de contacto con grupos de interés y de partes interesadas (actores y responsabilidades en datos personales), encontrando que no se soporta los requerimientos establecidos en el numeral de la norma.

C. Determinación del alcance del SGSI.

Respecto a la determinación del alcance del sistema de gestión de la seguridad de la información, se evidenció que se encuentra descrito en la política general de seguridad y privacidad de la información, la cual fue aprobada a través del comité institucional de gestión y desempeño, sin embargo, es importante que el alcance del SGSI se encuentre orientado a establecer los límites y la aplicabilidad de la seguridad, teniendo en cuenta la comprensión de las necesidades y expectativas de las partes interesadas, así como su relación con la áreas institucionales.

Finalmente, a través de la resolución 013 del 22 de enero del 2018, se evidenció el cumplimiento del numeral 4.4 Sistema de Gestión de Seguridad de la Información en donde la Entidad ha establecido la implementación del SGSI, mantenimiento y mejora continua del SGSI.

D. Liderazgo.

se evidenció cumplimiento de los numerales 5.1 liderazgo y compromiso, 5.2 política; sin embargo y 5.3 Roles, Responsabilidades y Autoridades de la Organización.
Como evidencia del proceso aporta las siguientes:

- Resolución 013 del 22 de enero del 2018, en donde se evidencian las funciones de la designación del Oficial de seguridad de la información, implementación y seguimiento del SGSI
- Política de seguridad y privacidad de la información aprobada en el año 2020, evidenciando las responsabilidades, sin embargo, y teniendo en cuenta los cambios institucionales no se evidencia actualización de la política.

E. Acciones para tratar riesgos y oportunidades.

Respecto al requisito 6 planificación en su numeral 6.1, se evidenció la matriz de riesgos orientados a seguridad de la información, la cual contiene, valoración del riesgo, tratamiento orientado a actividades y responsables de ejecución; por otra parte, se tuvieron en cuenta los controles que están establecidos en el anexo A de la Norma ISO 27001:2013. A través de la matriz de aplicabilidad, el proceso se encuentra en proceso de implementación de los 114 controles de la norma.
Sin embargo, como no se cuenta con directrices sobre la gestión del riesgo, no se evidencia la aprobación del plan de tratamiento de riesgos y la aceptación del riesgo residual por parte del responsable de ejecutar las actividades o en su defecto por parte del dueño del activo de información sobre el cual se realizó el análisis del riesgo.

F. Soporte.

En el requisito 7 soporte, se evidenció cumplimiento de los numerales 7.5 Información Documentada; sin embargo, en la verificación de la comunicación del SGSI, el proceso aporta documento del plan de capacitaciones que solo consideran las partes internas (institucional), situación que presenta incumplimiento del numeral 7.4 comunicación en donde se determina… "determinar la necesidad de comunicaciones internas y externas pertinentes al sistema de gestión de la seguridad de la información…"

G. Operación.

Se evidenció incumplimiento de los numerales 8.1 Planificación y Control Operacional y 8.2 Valoración de Riesgos de la Seguridad de la Información; si bien se realiza la identificación de riesgos de seguridad de la información y se documentan a través de la matriz dispuesta para tal fin, el proceso no logró demostrar el seguimiento a la implementación de las actividades propuestas para el tratamiento del riesgo, así como la valoración en intervalos planificados.

Se argumenta que se encuentra en proceso de articulación con el procedimiento de administración de riesgos, en donde se incorporan temas relacionados con riesgos de seguridad de la información, pero no se evidencia la relación de seguridad de la información en la política institucional de administración de riesgo que se encuentra publicada en la página web.

H. Mejora continua

Finalmente, en el requisito 10 mejora, se evidenció el cumplimiento parcial del numeral 10.2 mejora continua, soportado en el plan de mejoramiento del SGSI producto de la auditoría interna y de gestión realizada en la vigencia 2021. Esto teniendo en cuenta que aún existen acciones abiertas que se encuentran en proceso de implementación.

2. ANEXO A ISO 27001:2013

Se realizó seguimiento al Anexo A de la norma ISO 27001:2013, Objetivos de Control y Controles de Referencia, los cuales fueron acogidos por la Entidad; se identificaron 114 controles en el documento Declaración de Aplicabilidad.

Con el fin de validar su implementación el equipo auditor seleccionó una muestra de controles en los siguientes dominios

DESCRIPCIÓN	REQUISITO NORMA
Políticas de la Seguridad de la información	Dominio A.5
Seguridad de los recursos humanos	Dominio A.7
Gestión de activos	Dominio A.8
Control de acceso	Dominio A.9
Derechos de acceso privilegiado	Dominio A 9.2.3
Controles de acceso físicos	Dominio 11.1.2
Seguridad del cableado	Dominio 11.2.3
Gestión de la capacidad	Dominio A.12.1
Protección contra códigos maliciosos	Dominio A.12.2

A. Políticas de la Seguridad de la información.

Se cuenta con una política de seguridad y privacidad de la información aprobada y publicada a través de la página web institucional, sin embargo, se evidenció que (i) dicha política no se encuentra actualizada y (ii) como parte integral de la implementación de la política, se encuentra en proceso de actualización el manual de políticas de seguridad de la información.

B. Seguridad de los recursos humanos.

Se evidenció la incorporación de la cláusula contractual vigésima segunda -Confidencialidad- en las minutas de los contratos de prestación de servicios, pero no se logra evidenciar la responsabilidad sobre el cumplimiento de las políticas y procedimiento establecidos por el SGSI para funcionarios y contratistas.

Se verificó la aplicabilidad de toma de conciencia, educación y formación en la seguridad de la información para los colaboradores de la entidad a través de piezas gráficas.

C. Gestión de activos

El SGSI actualmente se encuentra en proceso para incorporar dentro de su información documentada el procedimiento de gestión de activos de información, se evidencia matriz con activos de información y publicación del indicado de información clasificada y reservada en la página web.
No se logró evidenciar para la vigencia auditada el etiquetado de la información.

D. Control de accesos.

El proceso no cuenta con procedimiento documentado sobre la gestión de acceso de redes y sistemas de información, en donde se establezca el proceso formal de registro, cancelación de usuarios, revisión de los derechos de acceso, sin embargo, a través de correo electrónico enviado en el mes de mayo del año 2022, se evidencia solicitud de diligenciamiento del formato AIN-10100.310101 FORMATO ACTUALIZACIÓN ROLES Y RESPONSABILIDADES EN UNIDADES COMPARTIDAS, con el fin de validar los permisos de accesibilidad sobre las unidades de almacenamiento.

E. Control de accesos físicos

Durante el recorrido a las áreas donde se encuentran ubicados el centro de datos y cableado de la entidad, se evidencio que el centro de datos principal, se encuentra controlado mediante puerta con llave y se encuentra centralizado a través de cámaras de monitoreo externas.

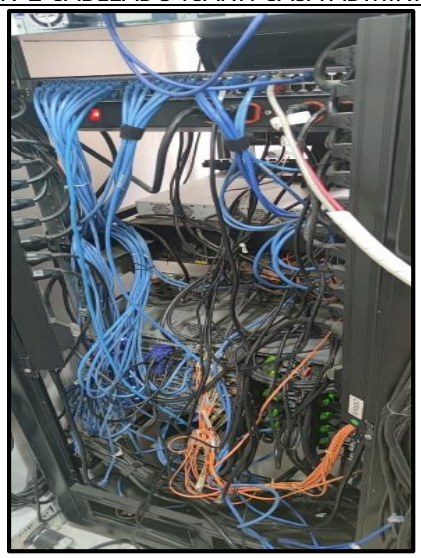
IMAGEN N°1 ZONAS DE ACCESO ICANH

Fuente: Registro fotográfico auditor OCI

- En general se evidenció que ninguna de las dos zonas recorridas cuenta con bitácoras o registros de ingreso.

- Centro de datos y cableado principal.
- Acceso físico controlado

IMAGEN N°2 CABLEADO ICANH CASA ADMINISTRATIVA



Fuente: Registro fotográfico auditor OCI

El cableado de telecomunicaciones que porta datos o brinda soporte a los servicios de información, no se encuentra organizado ni protegido contra interceptación, interferencias o daño.

IMAGEN N°3 CABLEADO ENERGÍA ELECTRICA ICANH

Fuente: Registro fotográfico auditor OCI

El cableado de energía eléctrica se encuentra protegido contra interceptación, interferencia o daño.

IMAGEN N°4 ACCESO A CENTRO DE CABLEADO CASA MISIONAL

Fuente: Registro fotográfico auditor OCI

No cuenta con protección de acceso físico, la puerta se encuentra abierta sin candado. Esta zona está ubicada al ingresar a las instalaciones de la Entidad, lo cual genera riesgo de acceso no autorizado.

IMAGEN N°5 CENTRO DE CABLEADO CASA MISIONAL

Fuente: Registro fotográfico auditor OCI

Al ingresar se evidencia que el lugar cuenta con cajas y un mueble en donde se almacenan elementos que no corresponden al centro de cableado.

IMAGEN N°6 CABLEADO CASA MISIONAL

Fuente: Registro fotográfico auditor OCI

El cableado de telecomunicaciones que porta datos o brinda soporte a los servicios de información, no se encuentra organizado, sin embargo, se evidencia protegido contra interceptación, interferencias o daño a través de puerta con llave.

IMAGEN N°7 ACCESO UPS

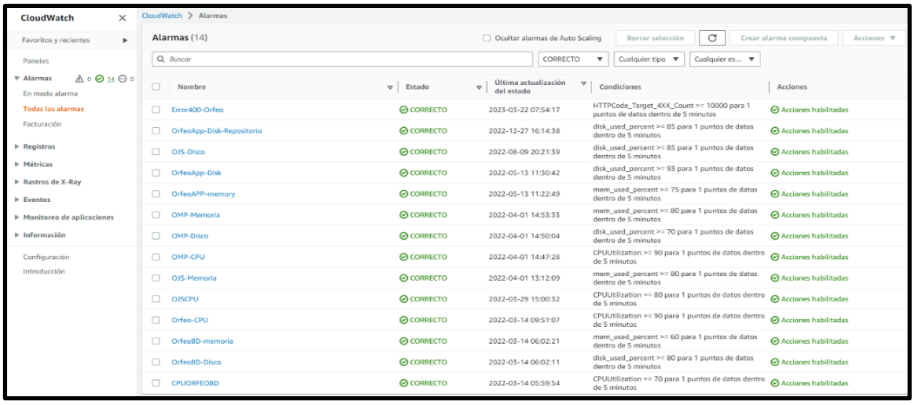
Fuente: Registro fotográfico auditor OCI

La UPS tiene control de acceso a través de llave, sin embargo, esta se encuentra pegada en la misma unidad lo cual genera riesgos de manipulación no controlada.

F. Gestión de la capacidad.

Se evidenció que el proceso mantiene alarmas para el seguimiento al uso de recursos a los servicios en la nube, lo cual permite hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido de los servicios tecnológicos.

IMAGEN N°8 SEGUIMIENTOS USO DE RECURSOS DE LA NUBE



Fuente: Información compartida por el área evaluada.

No se evidenció monitoreo de recursos para los servicios que se encuentran alojados en el centro de datos físico de la entidad.

G. Protección contra códigos maliciosos

Durante la verificación en recorrido se tomó la muestra de tres equipos, realizando las siguientes pruebas

- 2 equipos desatendidos: realizando simulación de infección ejecutando .bat
- 1 equipo con usuario: validando la ejecución de archivo .exe, encontrando que el sistema desempaqueta todos los archivos realizando la instalación sin control de solicitud usuario administrador.

El proceso tiene implementado controles de recuperación a través del plan de Backus.

CONCLUSIONES

1. El Proceso de Gestión de Tecnologías de la información cuenta con un Sistema de Gestión de Seguridad de la Información fundamentado en el Modelo de seguridad y privacidad de la información y los requisitos de la norma ISO 27001:2013, sin embargo, es importante continuar gestionando la implementación de los requisitos para el mejoramiento continuo del mismo.

2. Para el tratamiento de riesgos de la seguridad de la información es necesario implementar una gestión de seguimiento sobre las actividades definidas para mitigarlos.

3. Se debe continuar con la implementación de los criterios definidos en modelo de seguridad y privacidad de la información y los definidos en la ISO 27001:2013, permitiendo fomentar el cumplimiento de la política de seguridad digital establecida en el MIPG.

4. De acuerdo a las no conformidades y oportunidades de mejora se debe establecer plan de mejoramiento; así mismo atender cada una de las recomendaciones expuestas en el presente informe.

RECOMENDACIONES

A continuación, se establecen los Hallazgos y/o No Conformidades, las Fortalezas y las Recomendaciones que se encontraron durante del proceso de auditoría al Sistema de Gestión de Seguridad de la Información-Norma ISO 27001:2013 y el Modelo de Seguridad y Privacidad de la Información –MSPI.

Fortalezas

1. Disposición del líder del proceso de TI, el responsable del SGSI y su equipo de trabajo frente a la auditoría del SGSI.

2. Liderazgo y compromiso del líder del proceso TI y responsable del SGSI en la implementación del Sistema de Gestión de Seguridad de la Información-SGSI, trabajo que permite propender por la seguridad de la información en la Entidad.

3. Se realiza gestión de vulnerabilidades técnicas a través del encargado de Seguridad de la información.

4. Compendio de normas externas aplicables al SGSI actualizadas -Nomograma-.

5. Se cuenta con la identificación de los activos de información institucionales.

6. Documentación de la matriz de aplicabilidad.

7. Avance en la implementación del Modelo de Seguridad y Privacidad de la Información a través de los controles de la ISO 27001:2013.

No conformidades.

1. Contexto de la organización.

a) Comprensión de las necesidades y expectativas de las partes interesadas
El proceso no ha determinado las partes interesadas -internas y externas- relacionadas con el sistema de gestión de seguridad de la información -SGSI, por tanto, no se encuentra documentado.

b) Planificación.
No se identifica la aprobación del plan de tratamiento de riesgos de la seguridad de la información, y la aceptación de los riesgos residuales de la seguridad de la información por parte de los dueños de los activos de información.

2. Soporte.

a) Comunicación

Verificado el plan de capacitaciones aportado por el proceso, no se evidencia la comunicación desagregada por parte interesada, esto teniendo en cuenta que no se han definido en el SGSI.

3. Operación.

a) Planificación y Control Operacional - Valoración de Riesgos de la Seguridad de la Información

No se evidencia una valoración a intervalos planificados de los riesgos de seguridad de la información con criterios establecidos.

No se evidencia una planificación para la implementación y documentación de los resultados del tratamiento de riesgos de seguridad de la información.

4. Oportunidades de Mejora

4.1. Establecer el alcance del SGSI a través de Resolución.

4.2. Establecer los criterios para la gestión de riesgos de seguridad de la información.

4.3. Realizar el seguimiento de la implementación de la matriz de aplicabilidad a través del comité institucional de gestión y desempeño.

4.4. Articular la gestión de riesgos de seguridad de la información con la política institucional de gestión del riesgo.

4.5. La entidad debe garantizar que se cumplan las directrices y controles establecidos para restringir el acceso a la información, como se establece en el Anexo A, Dominio A9 de la Norma ISO 27001:2013, toda vez para ingresar al área de TI cuenta con un control que asegura la puerta mediante llave, sin embargo, tiene un espacio hueco que conecta a las otras oficinas por el cual se puede realizar un acceso no autorizado. De otra parte, el centro de cableado de la casa contigua se observa sin protección de acceso físico permitiendo ingresos no autorizados.

4.6. Formalizar la documentación del SGSI que se encuentra en proceso y comunicarla a las partes interesadas.

4.7. Verificar y actualizar la política de seguridad y privacidad de la información conforme los cambios de la entidad.

4.8. Documentar procedimiento sobre gestión de vulnerabilidades.

4.9. Complementar documento de plan de backups, con ítem para restaurar y probar las copias de seguridad ejecutadas.

4.10. Implementar etiquetado de la información sobre los activos institucionales.

4.11. Implementar acciones documentadas que permitan dar cuenta de la seguridad del recurso humano.

5. Recomendaciones:

5.1. Se recomienda hacer un análisis detallado de los incidentes/eventos de seguridad y las vulnerabilidades encontradas para la identificación de riesgos, llevarlos a la matriz de riesgos y establecer controles.

5.2. Generar un manual de identificación de riesgos de seguridad de la información que permita a los responsables realizar una adecuada gestión sobre estos.

5.3. Coordinar sesiones y boletines informativos con periodicidad frecuente que permitan mejorar las competencias de los colaboradores institucionales en temas relacionados con seguridad de la información.

5.4. Se recomienda documentar un formato que permita mantener el registro de los accesos al centro de cableado y datos de la entidad.

5.5. Validar y regular la temperatura del centro de datos, toda vez, que al ingresar el lugar no se sentía frío y tampoco se logró determinar control sobre este.

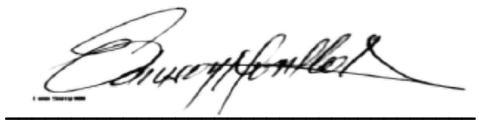
5.6. Respecto a la zona de cableado se recomienda limpiar y retirar todos los elementos que no pertenecen a estos espacios, adicional anclar y organizar de manera adecuada el trenzado del cable.

5.7. Revisar, ajustar y probar la política de instalación archivos .exe con el fin de prevenir la ejecución de programa malicioso

5.8. Implementar recurso que permita monitorear la capacidad del servidor físico que se encuentra en el centro de datos de la entidad.

5.9. Revisar y documentar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.

RESUMEN	
RECOMENDACIONES	9
OPORTUNIDADES DE MEJORA	11
NO CONFORMIDADES	3



Edinson Murillo Albornoz
Jefe Oficina de Control Interno

Elaboró: Auditor Interno María Alejandra del Pilar Suarez Rojas
Fecha de elaboración: 27-03-2023
Revisó: Diana Carolina Garzón Ochoa – Contratista Oficina de Control Interno
Fecha de revisión: 31-03-2023
Aprobó: Edinson Murillo– jefe de Oficina de Control Interno
Fecha de aprobación: 31-03-2023