

MEMORANDO**ICANH – MI** 2022130000030693

Bogotá D.C., 30 de septiembre de 2022

Para: **ALHENA CAICEDO FERNÁNDEZ**
Directora General

De: **EDINSON MURILLO ALBORNOZ**
Oficina de Control Interno

Asunto: Informe evaluación tratamiento de Riesgos Tecnologías de la Información.

Estimada Dra. Caicedo

El informe adjunto corresponde a la evaluación realizada a la ejecución de actividades que controlan la materialización de riesgos de tecnologías de la información en lo referente al primer semestre de 2022

Atentamente,



EDINSON MURILLO ALBORNOZ
Oficina de Control Interno



	PROCESO EVALUACIÓN Y SEGUIMIENTO	CÓDIGO	F-CI-02		
	OFICINA DE CONTROL INTERNO	VERSIÓN	1.0		
	INFORME DE AUDITORIA, EVALUACIÓN Y/O SEGUIMIENTO	PÁGINA	1	DE	19

**INFORME N° 025-2022 EVALUACIÓN DE CONTROLES Y TRATAMIENTO DE RIESGOS
SEGURIDAD DE INFORMACIÓN PRIMER SEMESTRE 2022.**

Objetivo

Evaluar y analizar el plan de tratamiento de riesgos a cargo del área de Tecnologías de la Información en el primer semestre de la vigencia 2022; de acuerdo a la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, en cumplimiento de lineamientos para las entidades públicas en materia de implementación y adopción de buenas prácticas, tomando como referencia estándares internacionales, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), permitiendo habilitar la implementación de la Política de Gobierno Digital.

Alcance

El proceso de evaluación a desarrollarse, se ejercerá con corte a 30 de junio de 2022, y aplicará la metodología establecida para esta clase de evaluaciones en concordancia con la implementación MSPI. De acuerdo con los compromisos adquiridos en el Plan Integral de trabajo de la Oficina de Control Interno para la actual vigencia; con lo anterior, se verificará si el área de Tecnologías de la Información tuvo en cuenta las normas, preceptos, controles y tratamiento de riesgos de la seguridad de la información de tal manera que se evidencie confiabilidad del MSPI y la existencia y efectividad de los controles inherentes.

Criterio

Norma ISO/IEC 27001:2013 en su Anexo A.

- Políticas de seguridad de la información: A. 5.
- Organización de la seguridad de la información: A.6.
- Seguridad de los recursos humanos: A. 7.
- Gestión de Activos: A.8.
- Controles de acceso: A.9.
- Criptografía – Cifrado y gestión de claves: A.10.
- Seguridad física y ambiental: A.11.
- Seguridad operacional: A.12.
- Seguridad de las comunicaciones: A.13.
- Adquisición, desarrollo y mantenimiento del sistema: A.14.
- Gestión de incidentes de seguridad de la información A.16.
- Cumplimiento: A.18

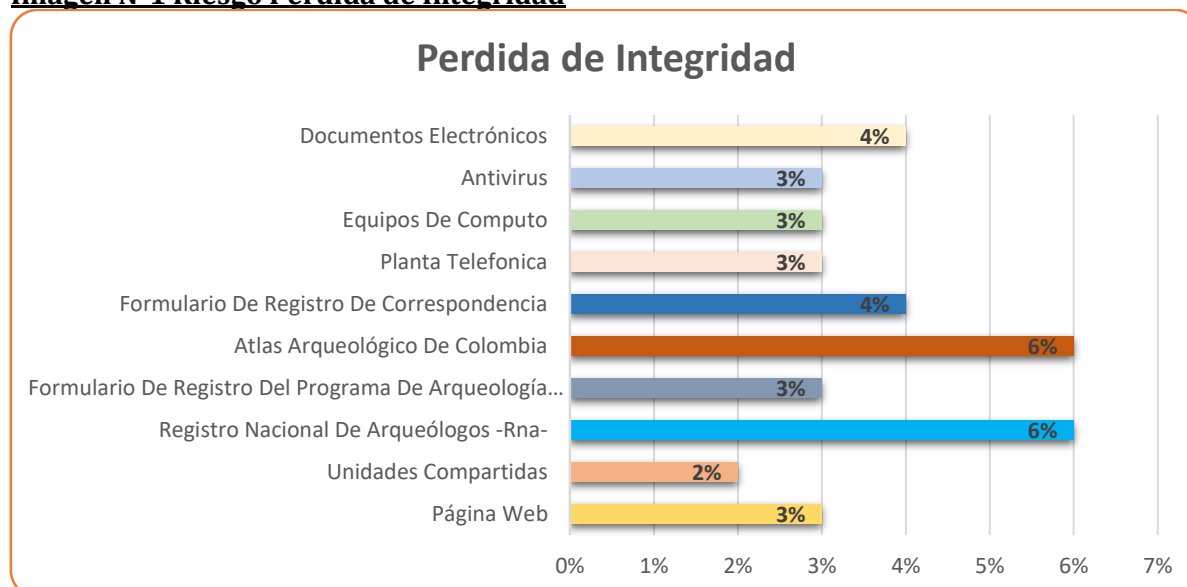
	PROCESO EVALUACIÓN Y SEGUIMIENTO	CÓDIGO	F-CI-02		
	OFICINA DE CONTROL INTERNO	VERSIÓN	1.0		
	INFORME DE AUDITORIA, EVALUACIÓN Y/O SEGUIMIENTO	PÁGINA	2	DE	19

Resultados

La información es suministrada por el área de Tecnología de Información, corresponde al seguimiento y el tratamiento aplicado a los riesgos de seguridad de información en la Entidad; en la cual se establecen unas actividades requeridas como control que mitigue la materialización del riesgo en el ICANH; del seguimiento y la evaluación realizada se evidencio el ítem principal del riesgo, el riesgo que afecta dicho criterio; así como el porcentaje que representa la acción que incide en cada uno de los riesgos identificados en la Entidad.

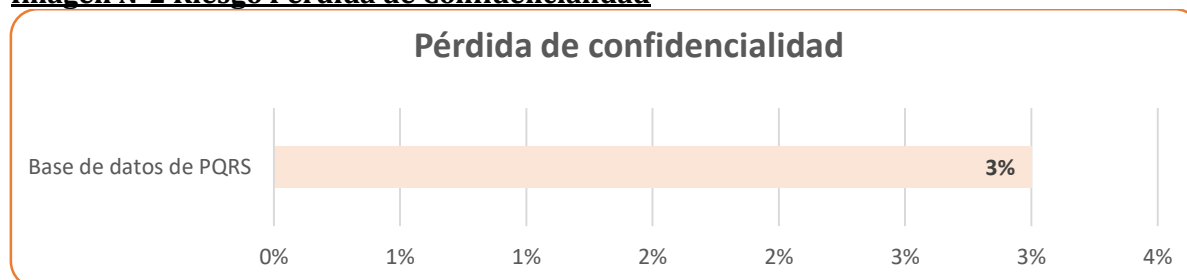
1. EVALUACIÓN MATRIZ DE RIESGOS SEGURIDAD DE INFORMACIÓN.

Imagen N°1 Riesgo Perdida de Integridad



Fuente: Matriz de Riesgos de Información del ICANH.

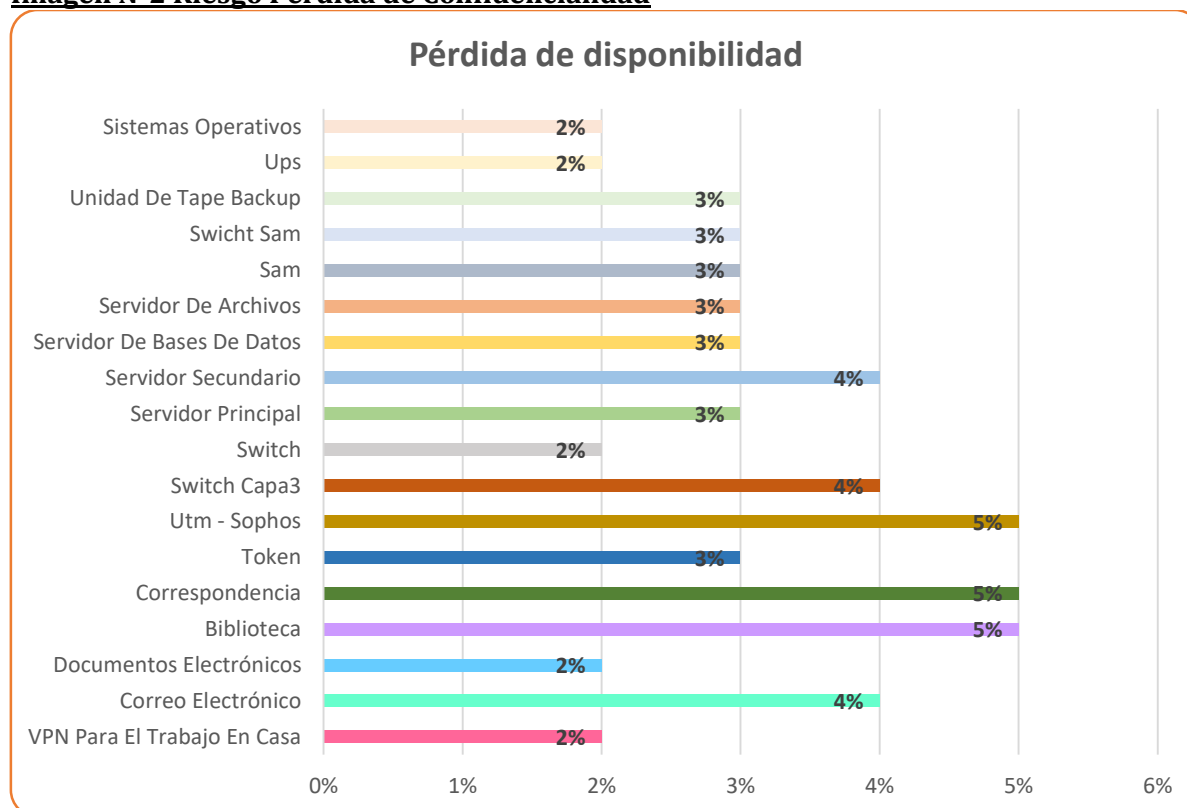
Imagen N°2 Riesgo Perdida de Confidencialidad



Fuente: Matriz de Riesgos de Información del ICANH.

	PROCESO EVALUACIÓN Y SEGUIMIENTO	CÓDIGO	F-CI-02		
	OFICINA DE CONTROL INTERNO	VERSIÓN	1.0		
	INFORME DE AUDITORIA, EVALUACIÓN Y/O SEGUIMIENTO	PÁGINA	3	DE	19

Imagen N°2 Riesgo Perdida de Confidencialidad



Fuente: Matriz de Riesgos de Información del ICANH.

Como se puede evidenciar en la gráfica, hay tres riesgos identificados para los sistemas de información de la entidad y en cada uno de ellos se relacionan diferentes componentes a los cuales se les implementan acciones que deben realizarse para mitigar y minimizar la materialización del Riesgos de seguridad de información conforme a los ITEMS específicos al cumplimiento de la Norma ISO/IEC 27001:2013 en su Anexo A, adicionalmente se establecen unas actividades requeridas para minimizar, en ese sentido, frente a esas actividades, la Oficina de Control Interno requiere una serie de evidencias que serán usadas como soporte documental para validar el cumplimiento por parte del área responsable.

La Oficina de Control Interno evaluó veintinueve (29) componentes de Seguridad de Información, los cuales contenían un total de ciento dieciséis (116) acciones por ejecutarse durante el periodo evaluado, a continuación, se detalla el estado de cumplimiento de cada uno de los mismos:



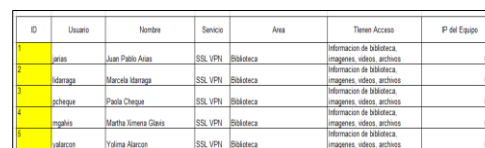
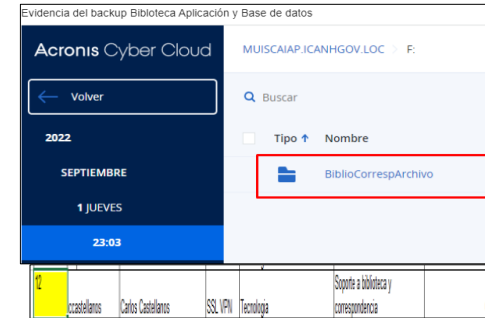
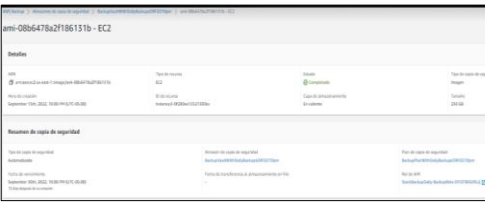
	PROCESO EVALUACIÓN Y SEGUIMIENTO	CÓDIGO	F-CI-02		
	OFICINA DE CONTROL INTERNO	VERSIÓN	1.0		
	INFORME DE AUDITORIA, EVALUACIÓN Y/O SEGUIMIENTO	PÁGINA	4	DE	19

1.1.Riesgo: Perdida de disponibilidad

N	ITEM	RIESGO	ACTIVIDAD REQUERIDA	Norma ISO/IEC 27001:2013 en su Anexo A	OBSERVACIÓN	Evidencia LINK
1	VPN para el trabajo en casa	Pérdida de disponibilidad	1. Aplicar el manual de políticas en lo referente a política de control de acceso. 2. Aplicación de la resolución de protección de información y la utilización de las unidades compartidas	Políticas de seguridad de la información: A. 5.	Se cuenta con la respectiva evidencia Política u manual de control de acceso, protección de información y unidades drive.	 https://drive.google.com/drive/u/1/folders/1E0x41KbR_k08L5
2	Correo electrónico	Pérdida de disponibilidad	1.Mantener el cambio de contraseña cada 60 días 2.Instalar y mantener actualizado un software antivirus. 3. Configurar restricciones en el controlador de dominio para evitar la ejecución de programas no autorizado 4.Definir la lista blanca de aplicaciones: El listado del software y tipos de instalaciones permitidas por ejemplo actualizaciones y parches de seguridad al software existente.	Controles de acceso: A.9.	Se realizan configuraciones en el servidor - Documento Política del Directorio Activo. (Cuenta de contraseña)- Página 9 Ítem 5 Se realiza actualización de antivirus mediante el sistema mediante programación en el servidor. Se establece periodicidad. Documento Lógica Sophos. Página 9 Ítem 5 Política del Director Activo, acciones de seguridad, la ejecución del control se realiza mediante la Red en el Servidor de Dominio. Página 13 Ítem 7 Pantallazo Configuración de Dominio restricciones de programas. Página 13 Ítem 7 El documento se encuentra en borrador es necesario realizar su gestión para aprobación, publicación y divulgación con toda la ciudad ICANH.	 https://docs.google.com/spreadsheets/d/1KP6IB/M-bmBbSGOQ9iBjurvrHXv7uWCNd8h5j4icy4/edit#gid=



	PROCESO EVALUACIÓN Y SEGUIMIENTO	CÓDIGO	F-CI-02		
	OFICINA DE CONTROL INTERNO	VERSIÓN	1.0		
	INFORME DE AUDITORIA, EVALUACIÓN Y/O SEGUIMIENTO	PÁGINA	5	DE	19

			5.Realizar una campaña de seguridad para sensibilizar en los peligros del correo electrónico (Spam, Phishing, scam, Malware, Hoaxes entre otros)		Pantallazo de Correos electrónicos de peligros.	 https://drive.google.com/drive/u/1/folders/15guxpNrwoL0jiiUQ5PPyivOCqEkS-v0
4	Documentos electrónicos	Pérdida de disponibilidad	Aplicar el manual de políticas de seguridad en lo referente a política de control de acceso. Aplicación de la resolución de protección de información y la utilización de las unidades compartidas	Gestión de Activos: A.8.	Listados de unidades compartidas	Carpeta de todos los formatos de unidades compartidas  https://drive.google.com/drive/u/1/folders/1T0DV1ZSSWqevC6ju8g0I3L2X-juct0YK
			Aplicar el manual de políticas de seguridad en lo referente a política de control de acceso. Se le tiene una VPN al soporte externo para los arreglos que requiera el aplicativo	Gestión de Activos: A.8.	Listado Control de acceso al aplicativo Pantallazo de Backup Aplicativo Biblioteca	
9	Biblioteca	Pérdida de disponibilidad	Establecer las personas que pueden acceder al aplicativo Establecer un periodo de copia de la información por parte del líder de la oficina y el soporte Investigación por parte del líder para el cambio del aplicativo Se tiene una política de confidencialidad con los proveedores los cuales no podrán divulgar la configuración ni el usuario y la clave para acceder al aplicativo de correspondencia	Controles de acceso: A.9.	Pantallazo VPN Ingeniero Carlos Castellanos	Evidencia del backup Biblioteca Aplicación y Base de datos 
10	Correspondencia	Pérdida de disponibilidad	Aplicar el manual de políticas de seguridad en lo referente a política de control de acceso. Se le tiene una VPN al soporte externo para los arreglos que requiera el aplicativo Establecer las personas que pueden acceder al aplicativo Establecer un periodo de copia de la información por parte del líder de la oficina y el soporte externo Investigación por parte del líder para el cambio del aplicativo	Adquisición, desarrollo y mantenimiento del sistema: A.14. Organización de la seguridad de la información: A.6. Controles de acceso: A.9.	Listado de usuarios en el programa Orfeo Pantallazo Backup de Orfeo Cláusula Contractual nuevo proveedor (PDF)	Se evidencia listados en Excel. 

3.3.10 Abstenerse de divulgar total o parcialmente la información que maneje en desarrollo de sus obligaciones contractuales en forma diferente a la autorizada por el ICANH.

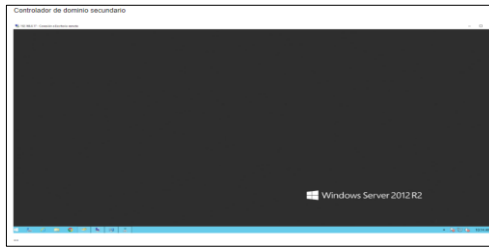
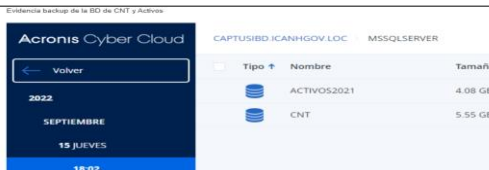


	PROCESO EVALUACIÓN Y SEGUIMIENTO		CÓDIGO	F-CI-02		
	OFICINA DE CONTROL INTERNO		VERSIÓN	1.0		
	INFORME DE AUDITORIA, EVALUACIÓN Y/O SEGUIMIENTO		PÁGINA	7	DE	19

			Se tiene una política de confidencialidad con los proveedores los cuales no podrán divulgar la configuración ni el usuario y la clave para acceder al UTM	Criptografía – Cifrado y gestión de claves: A.10.		
15	SWITCH CAPA3	Pérdida de disponibilidad	Aplicar el manual de políticas de seguridad	Seguridad operacional: A.12.	Contrato de compra de UPS y de Switch Listado de UPS.	Contrato CO1_PCCNTR_2306559 de 2021 - Se relacionan evidencias con fechado de la vigencia inmediatamente anterior dado que corresponde al contrato para la adquisición de UPS la cual se encuentra activa en el primer periodo de la vigencia 2022.
			En caso de daño se debe utilizar el switch secundario que debe estar configurado con todas las VLANs existentes	Adquisición, desarrollo y mantenimiento del sistema: A.14.		
			En caso de fallo eléctrico las dos UPS funcionaran con una capacidad de 30 minutos es suficientes tiempo si es necesario apagar.	Organización de la seguridad de la información: A.6.		
			Los switches están ubicados en el centro de cómputo, con eso se limita el acceso del personal no autorizado ya que este se encuentra bajo llave, y además se monitorea con una cámara.	Controles de acceso: A.9.		Listado UPS: Actualmente se tienen 2 UPS de 10KVA en datacenter principal y una UPS de 20KVA ubicada en el cuarto de datos de la casa misional.
			Se tiene una política de confidencialidad con los proveedores los cuales no podrán divulgar la configuración ni el usuario y la clave para acceder al switch			
16	SWITCH	Pérdida de disponibilidad	Se debe aplicar el manual de políticas de seguridad.	Controles de acceso: A.9.	Contrato de compra de UPS y de Switch Listado de Switch	De acuerdo a la Información reportada por el área de TI el Instituto cuenta con Switches: Cuatro (4) equipos Huawei y dos (2) Dell ubicados en casa administrativa; además tres (3) Huawei en casa misional. Se obtuvo evidencia de los equipos adquiridos en 2021; los demás ya se encontraban en el Instituto.
			En caso de daño físico se debe utilizar uno de los switcs disponibles en la oficina, para el cambio no es necesario apagar el centro de cómputo.	Adquisición, desarrollo y mantenimiento del sistema: A.14.		
17	SERVIDOR PRINCIPAL	Pérdida de disponibilidad	Aplicación del manual de políticas de seguridad.	Adquisición, desarrollo y mantenimiento del sistema: A.14.	Pantallazo de servidores activos principal y secundarios.	Recomendación: La OCI recomienda unificar los riesgos enumerados 17y 18 en uno solo Riesgo Macro que abarque la gestión general y la actividad de control de los servidores; lo anterior obedece a que se evidencio que la misma actividad de control responde a los dos riesgos.
			En caso de daño físico se debe promover el servidor secundario a primario.			
			Se debe llamar a el soporte de DELL, para la revisión del equipo lo cual lo hacen con una conexión remota.			
			Para el cambio de la parte se demora entre 48 y 72 horas, DELL envía un personal para el cambio.			

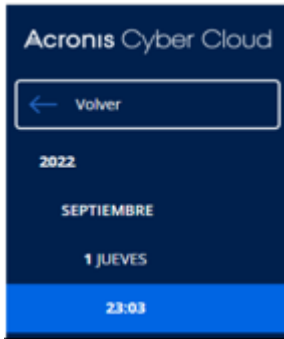


	PROCESO EVALUACIÓN Y SEGUIMIENTO		CÓDIGO	F-CI-02		
	OFICINA DE CONTROL INTERNO		VERSIÓN	1.0		
	INFORME DE AUDITORIA, EVALUACIÓN Y/O SEGUIMIENTO		PÁGINA	8	DE	19

18	SERVIDOR SECUNDARIO	Pérdida de disponibilidad	El servidor secundario, debe permanecer actualizado porque en caso de falla del servidor principal se debe realizar lo siguiente:	Seguridad operacional: A.12.	Pantallazo de servidores activos principal y secundarios. Recomendación: La OCI recomienda unificar los riesgos enumerados 17 y 18 en uno solo Riesgo Macro que abarque la gestión general y la actividad de control de los servidores; lo anterior obedece a que se evidencio que la misma actividad de control responde a los dos riesgos.	Se evidencio soporte documental de servidor secundarios activo en el primer semestre 2022. 	
			Promoverlo a Servidor Principal.	Adquisición, desarrollo y mantenimiento del sistema: A.14.			
			Renombrar las IP y colocar las del Servidor Principal.	Gestión de incidentes de seguridad de la información A.16.			
			Revisar el directorio activo.	Controles de acceso: A.9.			
			CONTINUIDAD DEL NEGOCIO				
19	SERVIDOR DE BASES DE DATOS	Pérdida de disponibilidad	Aplicación del manual de políticas de seguridad.	Organización de la seguridad de la información: A.6.	Pantallazo de BACKUP base de datos CNT	Se evidenció los respectivos Backup del aplicativo CNT en el primer periodo 2022. 	
			Instalar el SQL SERVER EN ORO SERVIDOR.				
			Llamar a CNT para poner en funcionamiento el aplicativo				
20	SERVIDOR DE ARCHIVOS	Pérdida de disponibilidad	Aplicación del manual de políticas de seguridad.	Organización de la seguridad de la información: A.6.	La información de la Entidad se encuentra en la nube; por lo anterior se recomienda eliminar dicho riesgo toda vez que no se realizan actividades de control.	 PROCESO DE GESTIÓN DE RECURSOS ACTA DE INICIO Código IR1.14300.021 Versión 3 Fecha Enero de 2021 ACTA DE INICIO ORDEN DE COMPRA No. 52569 DE 2022 En Bogotá, el primer (01) día del mes de julio de 2022, SONIA YANETH CARDOZO MUÑOZ, identificada con cédula de ciudadanía No. 53.118.525 expedida en Bogotá, quien se desempeña en el cargo de líder del Área de Tecnologías de la Información, en su calidad de Supervisora y HECTOR MARTÍN RODRIGUEZ ACEVEDO, identificado con número de cédula 4.119.065 expedida en Firavitoba - Boyacá, actuando en nombre y representación, de UNIÓN TEMPORAL TIGO BEXT 2021, con NIT. No. 901.537.095-3, en su condición de contratista, y una vez surtida la adjudicación, se procede a dar inicio a la ejecución del citado contrato, de conformidad con las condiciones que se transcriben a continuación: OBJETO: Mantener los servicios de Geoparques-atlas y Orfeo en la nube. Realizar migración a la nube de servicios QJS-PMP VALOR TOTAL: Cien millones cinco mil trescientos cuarenta y nueve pesos con veintinueve centavos (\$100.005.349,29), M.L., incluido IVA y demás impuestos y contribuciones que se causen.	
			En caso de daño físico se debe llamar a el soporte de DELL, para la revisión del equipo lo cual lo hacen con una conexión remota.				
			Para el cambio de la parte se demora entre 48 y 72 horas, DELL envía un personal para el cambio.				
			Restaurar el backup de la información en otro servidor y darle permisos de acceso a los usuarios que tengan allí su información				
21	SAM	Pérdida de disponibilidad	Aplicación del manual de políticas de seguridad.	Seguridad física y ambiental: A.11.	Pantallazo del SAM - Importante resaltar que está activo, pero no en uso dado que la información se almacén en la Nube. Por lo anterior se recomienda eliminar dicho riesgo toda vez que no se realizan actividades de control. - No se requiere evidencia.	 	
			En caso de daño físico se debe llamar a el soporte de DELL, para la revisión del equipo lo cual lo hacen con una conexión remota.				
			Para el cambio de la parte se demora entre 48 y 72 horas, DELL envía un personal para el cambio.				
			Para que la SAM la reconozcan los servidores se debe prender primero y esperar unos 15 minutos para luego si empezar a encender los servidores.				



	PROCESO EVALUACIÓN Y SEGUIMIENTO		CÓDIGO	F-CI-02		
	OFICINA DE CONTROL INTERNO		VERSIÓN	1.0		
	INFORME DE AUDITORIA, EVALUACIÓN Y/O SEGUIMIENTO		PÁGINA	9	DE	19

22	SWICHT SAM	Pérdida de disponibilidad	Aplicar el manual de políticas de seguridad. En caso de fallo eléctrico las dos UPS funcionarían con una capacidad de 30 minutos es suficiente tiempo si es necesario apagar. El switch está ubicado en el centro de cómputo, con eso se limita el acceso del personal no autorizado ya que este se encuentra bajo llave, y además se monitorea con una cámara. Un daño en el switch se debe revisar si prende o no porque puede ser que lo que está fallando es uno de los puertos.	Seguridad física y ambiental: A.11. Seguridad operacional: A.12.	Contrato UPS que soporta funcionamiento equipos en datacenter	Se evidencio la respectiva adquirió en la vigencia inmediatamente anterior de UPS funcionando para el periodo evaluado mediante Contrato CO1_PCCNTR_2306559 de 2021 Información general Identificación del contrato ID del contrato en SECOP: CO1_PCCNTR_2306559 Versión del contrato: 1 Estado del contrato: En ejecución Fecha de generación del estado: 26/02/2021 5:43:44 PM (UTC-05:00) Bogotá, Lima, Quito Número del Contrato: CO1_PCCNTR_2306559 Objeto del contrato: Adquisición e instalación de UPS para el ICANH Tipo de Contrato: Compraventa
23	UNIDAD DE TAPE BACKUP	Pérdida de disponibilidad	Aplicar el manual de políticas de seguridad. La unidad de Tape Backup esta ubicada en el centro de cómputo, con eso se limita el acceso del personal no autorizado ya que este se encuentra bajo llave, y además se monitorea con una cámara. Los daños en la unidad de Tape Backup lo ocasionan son las cintas las cuales el las reporta y solo se cambian por otra para que el backup de la información que de bien hecho.	Seguridad operacional: A.12. Seguridad física y ambiental: A.11.	A partir de la vigencia 2021 se realizó contratación para generar Backup en la Nube. No se encuentra en uso. Se recomienda eliminar dicho riesgo toda vez que la unidad no se encuentra en uso y no requiere actividades de control.	 
24	UPS	Pérdida de disponibilidad	Ninguna persona está autorizada para manipular las UPS. En caso de pérdida de energía las ups automáticamente se ponen en funcionamiento.	Adquisición, desarrollo y mantenimiento del sistema: A.14.	Contrato de compra de UPS y de Switch Listado de Switch Recomendación: Unificar y eliminar riesgos de TI (15, 16 y 24) que se repitan y que gestionen con una misma evidencia; con el fin de no generar duplicidad de información.	Se evidencio la respectiva adquirió en la vigencia inmediatamente anterior de UPS funcionando para el periodo evaluado mediante Contrato CO1_PCCNTR_2306559 de 2021 Información general Identificación del contrato ID del contrato en SECOP: CO1_PCCNTR_2306559 Versión del contrato: 1 Estado del contrato: En ejecución Fecha de generación del estado: 26/02/2021 5:43:44 PM (UTC-05:00) Bogotá, Lima, Quito Número del Contrato: CO1_PCCNTR_2306559 Objeto del contrato: Adquisición e instalación de UPS para el ICANH Tipo de Contrato: Compraventa
28	SISTEMAS OPERATIVOS	Pérdida de disponibilidad	Se debe revisar cada PC para determinar la versión del sistema operativo. Se debe incluir en el plan de compras el cambio de estos PC debido a la obsolescencia del sistema operativo o mirar si se puede subir de versión el sistema operativo y el hardware de la máquina aguanta	Seguridad operacional: A.12.	Reporte de Sistemas Operativos - Contrato Windows 10. Recomendación: Eliminar el Riesgo y unificarlo con el N°26 y 27; con el fin de no generar duplicidad. Se deben actualizar las actividades de control en el riesgo 26, 27 y 28 y se debe incluir Actualización de Antivirus y Sistema Operativo de equipo de cómputo.	Se evidenció la Orden de compra 77565; con la cual se realiza la adquisición de licenciamiento de Microsoft para la Entidad. 



	PROCESO EVALUACIÓN Y SEGUIMIENTO	CÓDIGO	F-CI-02		
	OFICINA DE CONTROL INTERNO	VERSIÓN	1.0		
	INFORME DE AUDITORIA, EVALUACIÓN Y/O SEGUIMIENTO	PÁGINA	10	DE	19

Respecto a la evaluación de los controles y las acciones ejecutadas del Riesgo de Disponibilidad, la Oficina de Control Interno evidencio que del cincuenta y ocho por ciento (58%), el área de Tecnología de la Información en el primer semestre cumplió con el tratamiento del riesgo en un cincuenta y cinco por ciento (55%); siendo esto un nivel satisfactorio en lo referente al cumplimiento de su rol como segunda línea de defensa y en harás de mitigar la materialización de riesgos en la seguridad de la información de la entidad.

Es necesario que se implementen acciones de mejoramiento para el tres por ciento (3%) restante que presenta oportunidad de mejora a las acciones propuestas; esta Oficina se permite establecer las siguientes recomendaciones:

Nº 13 Ítem Token: Presentar a la Oficina de Control Interno en el segundo semestre de la vigencia 2022, el listado de responsables de Token, fecha de adquisición y vencimiento; además que se tramiten las aprobaciones correspondientes del documento borrador “*Lineamiento tokens-v2 22-07*” y a su vez se realice la socialización del documento con el usuario líder, para que desde allí se implemente y ejecute el procedimiento que busca mitigar el riesgo de seguridad de la información financiera de la Entidad.

Nº 15 Ítem SWITCH CAPA3; Nº 16 Ítem SWITCH y Nº24 Ítem UPS: La Oficina de Control Interno recomienda unificar y eliminar riesgos de seguridad de la información enumerados Nº15, 16 y 24, teniendo en cuenta que la OCI identificó que las acciones a seguir en cada uno de los componentes se repite y la evidencia corresponde a un mismo soporte documental; con el fin de no generar duplicidad de información, y establecer controles robustos que permitan mitigar de manera práctica y simplificada los posibles riesgos de información.

Nº 17 Ítem Servidor Principal y Nº 18 Ítem Servidor secundario: La OCI recomienda unificar los riesgos enumerados 17 y 18 en uno solo riesgo macro, de tal manera que el mismo abarque la gestión general y que la actividad de control mitigue los riesgos asociados con los servidores, herramienta en la cual reposa el 100% de la información de la Entidad; lo anterior obedece a que se evidencio que la misma actividad de control y soporte documental responde a los dos riesgos, es necesario simplificar actividades que permitan mejorar la gestión del área de Tecnología de la Información.

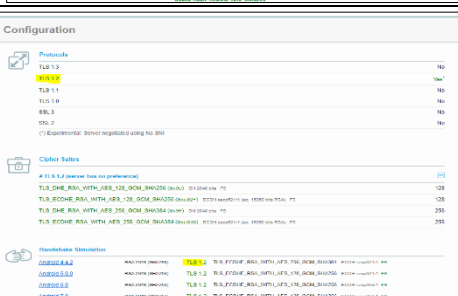
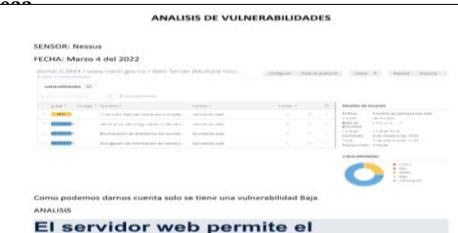
Nº 20 ítem Servidor De Archivos, Nº 21 Ítem SAN y Nº 23 Unidad de Tape Backup: Al realizar la evaluación se evidenció que, existen riesgos y actividades de control construidos desde la vigencia 2021, los cuales han dejado de ejecutarse debido a la adquisición, actualización e implementación de herramientas tecnologías que van a la vanguardia con los sistemas de información; lo anterior sustenta, porque los riesgos citados no ha ejecutado actividades de control debido a que la información de la Entidad se encuentra en la nube y dejó de almacenarse en el servido de archivos y el uso de SAN; ésta Oficina, recomienda eliminar dichos riesgos toda vez que no se realizan actividades de control, así como actualizar la matriz de Riesgo de Seguridad de la Información conforme a la realidad de la Entidad tanto en recursos humanos, como físicos y tecnológicos.



	PROCESO EVALUACIÓN Y SEGUIMIENTO	CÓDIGO	F-CI-02		
	OFICINA DE CONTROL INTERNO	VERSIÓN	1.0		
	INFORME DE AUDITORIA, EVALUACIÓN Y/O SEGUIMIENTO	PÁGINA	11	DE	19

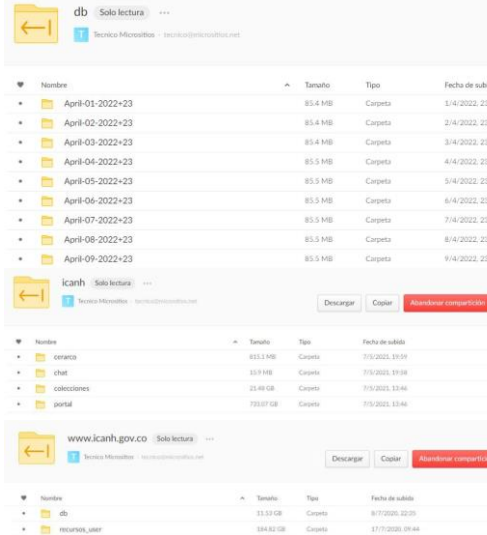
N° 26 ítem Equipos de Cómputo, N° 27 Ítem Antivirus y N° 28 Sistemas Operativos: La Oficina de Control Interno identificó que, las actividades de control para los riesgos y los componentes se repiten duplicando la información y dejando de generar valor agregado a la gestión de los riesgo; así mismo identificó que las actividades que pueden simplificarse en un solo riesgo hacen parte del Riesgo de Pérdida de disponibilidad y de integridad, es necesario que desde el área de Tecnologías de la Información se evalúe la pertinencia del riesgo y los controles para establecer en donde debe quedar ubicado las acciones o actividades de control; la OCI recomienda eliminar el Riesgo y unificarlo con el N°26, 27 y 28; es importante que su actualización se incluyan actividades de actualización de antivirus y Sistema operativo de equipo de cómputo de la Entidad.

1.2.Riesgo: Perdida de Integridad

N	ITEM	RIESGO	ACTIVIDAD REQUERIDA	Norma ISO/IEC 27001:2013 en su Anexo A	OBSERVACIÓN	Evidencia LINK
3	Página Web	Pérdida de integridad	1.Renovar el certificado SSL de la página web.	Controles de acceso: A.9.	Certificado SSL - Micrositios	Se puede validar desde cualquier página web check ssl: https://www.ssllabs.com/ssltest/analyze.html?d=www.icanh.gov.co&latest 
			2. Actualizar a la última versión el TLS		Certificado TLS- Micrositios	
			3.Aplicar parches de Seguridad a los softwares institucionales para reducir o eliminar problemas de seguridad.	Organización de la seguridad de la información: A.6.	Informe de vulnerabilidad página WEB - Micrositios	Se evidenció informe de vulnerabilidad primer semestre 2022 
			4. Análisis de vulnerabilidades de la página web			



	PROCESO EVALUACIÓN Y SEGUIMIENTO		CÓDIGO	F-CI-02		
	OFICINA DE CONTROL INTERNO		VERSIÓN	1.0		
	INFORME DE AUDITORIA, EVALUACIÓN Y/O SEGUIMIENTO		PÁGINA	12	DE	19

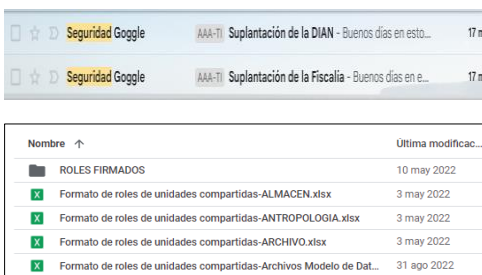
5	Unidades Compartidas	Pérdida de integridad	Aplicar el manual de políticas de seguridad en lo referente a política de control de acceso. Aplicación de la resolución de protección de información y l utilización de las unidades compartidas	Gestión de Activos: A.8.	Listados de unidades compartidas.	https://docs.google.com/spreadsheets/d/1zRhVbTPwE3aYDfPUl4jglqt5liv37Fj5/edit#gid=136926778 <table><thead><tr><th>UNIDADES COMPARTIDAS</th><th>AREA</th><th>AREA/OFICINA</th><th>RESPONSABLE</th></tr></thead><tbody><tr><td>Formato de roles de unidades compartidas-ALMACEN</td><td>SECRETARIA GENERAL</td><td>Área Funcional de Almacén</td><td>ALBA INES ESPITALA-PEÑA</td></tr><tr><td>Formato de roles de unidades compartidas-ANTROPOLOGIA</td><td>SUBDIRECCION DE INVESTIGACION Y PRODUCCION CENTRICA</td><td>Grupo de Antropología</td><td>MARIA TERESA SUZCDO</td></tr><tr><td>Formato de roles de unidades compartidas-ARCHIVO</td><td>SECRETARIA GENERAL</td><td>Área Funcional de Archivo</td><td>FERNANDO CARULLO</td></tr><tr><td>Formato de roles de unidades compartidas-Archivo modelo de datos</td><td>Subdirección de Gestión del Patrimonio</td><td>Área Funcional de Tecnologías Aplicadas al Patrimonio y</td><td>CARLOS PERA</td></tr><tr><td>Formato de roles de unidades compartidas-AREA DE TI</td><td>SECRETARIA GENERAL</td><td>Área Funcional de Tecnologías y</td><td>SINIA CARDOSO</td></tr><tr><td>Formato de roles de unidades compartidas-ARQUEOLOGIA</td><td>Subdirección de Gestión del Patrimonio</td><td>Sistemas de Información</td><td>JUAN MANUEL DIAZ</td></tr><tr><td>Formato de roles de unidades compartidas-ATENCION AL CIUDADANO</td><td>Subdirección de Atención Social y Relacionamento con el Ciudadano</td><td>Grupo de Arqueología</td><td>Laura Perra Márquez</td></tr><tr><td></td><td></td><td>Área Funcional de Relacionamento con el Ciudadano</td><td></td></tr></tbody></table>	UNIDADES COMPARTIDAS	AREA	AREA/OFICINA	RESPONSABLE	Formato de roles de unidades compartidas-ALMACEN	SECRETARIA GENERAL	Área Funcional de Almacén	ALBA INES ESPITALA-PEÑA	Formato de roles de unidades compartidas-ANTROPOLOGIA	SUBDIRECCION DE INVESTIGACION Y PRODUCCION CENTRICA	Grupo de Antropología	MARIA TERESA SUZCDO	Formato de roles de unidades compartidas-ARCHIVO	SECRETARIA GENERAL	Área Funcional de Archivo	FERNANDO CARULLO	Formato de roles de unidades compartidas-Archivo modelo de datos	Subdirección de Gestión del Patrimonio	Área Funcional de Tecnologías Aplicadas al Patrimonio y	CARLOS PERA	Formato de roles de unidades compartidas-AREA DE TI	SECRETARIA GENERAL	Área Funcional de Tecnologías y	SINIA CARDOSO	Formato de roles de unidades compartidas-ARQUEOLOGIA	Subdirección de Gestión del Patrimonio	Sistemas de Información	JUAN MANUEL DIAZ	Formato de roles de unidades compartidas-ATENCION AL CIUDADANO	Subdirección de Atención Social y Relacionamento con el Ciudadano	Grupo de Arqueología	Laura Perra Márquez			Área Funcional de Relacionamento con el Ciudadano	
UNIDADES COMPARTIDAS	AREA	AREA/OFICINA	RESPONSABLE																																							
Formato de roles de unidades compartidas-ALMACEN	SECRETARIA GENERAL	Área Funcional de Almacén	ALBA INES ESPITALA-PEÑA																																							
Formato de roles de unidades compartidas-ANTROPOLOGIA	SUBDIRECCION DE INVESTIGACION Y PRODUCCION CENTRICA	Grupo de Antropología	MARIA TERESA SUZCDO																																							
Formato de roles de unidades compartidas-ARCHIVO	SECRETARIA GENERAL	Área Funcional de Archivo	FERNANDO CARULLO																																							
Formato de roles de unidades compartidas-Archivo modelo de datos	Subdirección de Gestión del Patrimonio	Área Funcional de Tecnologías Aplicadas al Patrimonio y	CARLOS PERA																																							
Formato de roles de unidades compartidas-AREA DE TI	SECRETARIA GENERAL	Área Funcional de Tecnologías y	SINIA CARDOSO																																							
Formato de roles de unidades compartidas-ARQUEOLOGIA	Subdirección de Gestión del Patrimonio	Sistemas de Información	JUAN MANUEL DIAZ																																							
Formato de roles de unidades compartidas-ATENCION AL CIUDADANO	Subdirección de Atención Social y Relacionamento con el Ciudadano	Grupo de Arqueología	Laura Perra Márquez																																							
		Área Funcional de Relacionamento con el Ciudadano																																								
6	Registro Nacional de Arqueólogos - RNA-	Pérdida de integridad	Aplicar el manual de políticas de seguridad en lo referente a política de control de acceso. Se tiene un acceso VPN al soporte del aplicativo para ajuste o arreglos del aplicativo Establecer un periodo de copia de la información por parte del soporte del aplicativo Backup del SQL server (aplicativo) Realizar Backup de la información en cintas Se tiene una política de confidencialidad con los proveedores los cuales no podrán divulgar la configuración ni el usuario y la clave para acceder al aplicativo Se debe investigar porque uno de los componentes del aplicativo, utiliza el programa FLASH que dejara de funcionar a finales del 2020.	Controles de acceso: A.9.	Pantallazo de Backup - Micrositios	 Se evidencio la cláusula de confidencialidad de los proveedores en el contrato; para el primer semestre de 2022 se celebraron ocho (8) contratos que cuentan con la cláusula de confidencialidad. - Sandra Silva:070-2022 - Walter Posso:085-2022 - Wilson Fajardo:071-2022 - Camilo Pintor: 086-2022 - Julio Jiménez:087-2022 - Carlos Castellanos:147-2022 - Micrositios:148-2022 - EnterTelecomunicaciones:201-2022 VIGÉSIMA SEGUNDA. CONFIDENCIALIDAD: La información compartida en virtud del presente contrato es considerada sensible y de carácter restringida en su divulgación y utilización. Esta información puede abarcar entre otros: documentos, datos, tecnología o material que se considera único y confidencial o que es objeto de protección legal. En razón a lo anterior, la información que EL CONTRATISTA conozca por causa o con ocasión de la ejecución del contrato, durante y posterior a su vigencia, no deberá divulgarla de manera directa, indirecta o remota, ni a través de ninguna otra persona, ni utilizarla en beneficio propio o de terceros, sin antes contar con la autorización por escrito del ICANH, así mismo deberá conocer y dar cumplimiento a las políticas generales y específicas de seguridad y privacidad de la información así como a los procedimientos, guías, y lineamientos derivados de ella, como la política de tratamiento de datos personales. Ley Habeas Data todos estos publicados en el ICANH.																																				



	PROCESO EVALUACIÓN Y SEGUIMIENTO	CÓDIGO	F-CI-02		
	OFICINA DE CONTROL INTERNO	VERSIÓN	1.0		
	INFORME DE AUDITORIA, EVALUACIÓN Y/O SEGUIMIENTO	PÁGINA	13	DE	19

7	Formulario de registro del Programa de Arqueología Preventiva	Pérdida de integridad	Aplicar el manual de políticas de seguridad en lo referente a política de control de acceso. Aplicar el manual de políticas de seguridad en lo referente a política de control de acceso. Aplicar el manual de políticas de seguridad en lo referente a política de control de acceso.	Controles de acceso: A.9.	Listado de personas con acceso - permisos Drive en el formulario de arqueología preventiva PAP, es un formulario ubicado en la gsuite	https://docs.google.com/spreadsheets/d/1oRkScUYFvu0MVL57WH08KsjFBD0eY10/edit#gid=246129373 <table><tr><th colspan="3">FORMULARIO DE ARQUEOLOGIA PAP</th></tr><tr><th>USUARIO</th><th>CORREO</th><th>ROL</th></tr><tr><td>Maria Jose Ramirez</td><td>mmiramez@icanh.gov.co</td><td>EDITORES</td></tr><tr><td>Juan Manuel Diaz</td><td>jdiaz@icanh.gov.co</td><td>EDITORES</td></tr><tr><td>Yahir Herrera</td><td>yherrera@icanh.gov.co</td><td>EDITORES</td></tr><tr><td>Maria Helena Gonzalez</td><td>apoyoarqueologia1@icanh.gov.co</td><td>EDITORES</td></tr><tr><td>Claudia Jaime</td><td>apoyoarqueologia2@icanh.gov.co</td><td>EDITORES</td></tr><tr><td>Diana Marcela Garcia</td><td>apoyoarqueologia3@icanh.gov.co</td><td>EDITORES</td></tr><tr><td>Diana Paola Garcia</td><td>dgarcia@icanh.gov.co</td><td>EDITORES</td></tr><tr><td>Walter Posso</td><td>wposso@icanh.gov.co</td><td>PROPIETARIO</td></tr></table>	FORMULARIO DE ARQUEOLOGIA PAP			USUARIO	CORREO	ROL	Maria Jose Ramirez	mmiramez@icanh.gov.co	EDITORES	Juan Manuel Diaz	jdiaz@icanh.gov.co	EDITORES	Yahir Herrera	yherrera@icanh.gov.co	EDITORES	Maria Helena Gonzalez	apoyoarqueologia1@icanh.gov.co	EDITORES	Claudia Jaime	apoyoarqueologia2@icanh.gov.co	EDITORES	Diana Marcela Garcia	apoyoarqueologia3@icanh.gov.co	EDITORES	Diana Paola Garcia	dgarcia@icanh.gov.co	EDITORES	Walter Posso	wposso@icanh.gov.co	PROPIETARIO												
FORMULARIO DE ARQUEOLOGIA PAP																																																
USUARIO	CORREO	ROL																																														
Maria Jose Ramirez	mmiramez@icanh.gov.co	EDITORES																																														
Juan Manuel Diaz	jdiaz@icanh.gov.co	EDITORES																																														
Yahir Herrera	yherrera@icanh.gov.co	EDITORES																																														
Maria Helena Gonzalez	apoyoarqueologia1@icanh.gov.co	EDITORES																																														
Claudia Jaime	apoyoarqueologia2@icanh.gov.co	EDITORES																																														
Diana Marcela Garcia	apoyoarqueologia3@icanh.gov.co	EDITORES																																														
Diana Paola Garcia	dgarcia@icanh.gov.co	EDITORES																																														
Walter Posso	wposso@icanh.gov.co	PROPIETARIO																																														
8	Atlas Arqueológico de Colombia	Pérdida de integridad	Aplicar el manual de políticas de seguridad en lo referente a política de control de acceso. Se tiene un acceso VPN al soporte del aplicativo para ajuste o arreglos del aplicativo Establecer un periodo de copia de la información por parte del soporte del aplicativo Backup del SQL server (aplicativo) Realizar Backup de la información en cintas	Controles de acceso: A.9.	Listado de usuarios con acceso a la herramienta alojada en Nube.	Se evidencio link de VPN activado con corte a Junio de 2022, sin embargo al cierre de la evaluación no se encuentra activo porque no hay un contrato vigente con el proveedor <table><tr><th>ID</th><th>Usuario</th><th>Nombre</th><th>Servicio</th><th>Area</th><th>Tienen Acceso</th></tr><tr><td>1</td><td>Comandante</td><td>Ruth Martinez</td><td>SSL VPN</td><td>Contabilidad</td><td>Acceso a el sistema CHZ</td></tr><tr><td>2</td><td>Comandante</td><td>John Alca - Henry Blagus</td><td>SSL VPN</td><td>Seguridad Arqueologica</td><td>Reporte al sistema generadores, atlas geografico</td></tr><tr><td>3</td><td>Comandante</td><td>Carlos Mendoza Puerto</td><td>SSL VPN</td><td>Biblioteca</td><td>Consulta informacion de biblioteca, imagenes, videos, archivos</td></tr><tr><td>4</td><td>Asesor</td><td>Sebastian Marin</td><td>SSL VPN</td><td>Rut Administrativa</td><td>Realiza procesos del sistema del ICANH</td></tr><tr><td>5</td><td>Bentosa</td><td>Empresa encargada de la migracion para AVOIS</td><td>SSL VPN</td><td>Empresa contratista Bentosa</td><td>Acceso a servidor para migracion esta</td></tr><tr><td>7</td><td>Bentosa</td><td>Empresa encargada de migracion PVS</td><td>SSL VPN</td><td>Empresa contratista Bentosa</td><td>Acceso a firewall</td></tr></table>	ID	Usuario	Nombre	Servicio	Area	Tienen Acceso	1	Comandante	Ruth Martinez	SSL VPN	Contabilidad	Acceso a el sistema CHZ	2	Comandante	John Alca - Henry Blagus	SSL VPN	Seguridad Arqueologica	Reporte al sistema generadores, atlas geografico	3	Comandante	Carlos Mendoza Puerto	SSL VPN	Biblioteca	Consulta informacion de biblioteca, imagenes, videos, archivos	4	Asesor	Sebastian Marin	SSL VPN	Rut Administrativa	Realiza procesos del sistema del ICANH	5	Bentosa	Empresa encargada de la migracion para AVOIS	SSL VPN	Empresa contratista Bentosa	Acceso a servidor para migracion esta	7	Bentosa	Empresa encargada de migracion PVS	SSL VPN	Empresa contratista Bentosa	Acceso a firewall
ID	Usuario	Nombre	Servicio	Area	Tienen Acceso																																											
1	Comandante	Ruth Martinez	SSL VPN	Contabilidad	Acceso a el sistema CHZ																																											
2	Comandante	John Alca - Henry Blagus	SSL VPN	Seguridad Arqueologica	Reporte al sistema generadores, atlas geografico																																											
3	Comandante	Carlos Mendoza Puerto	SSL VPN	Biblioteca	Consulta informacion de biblioteca, imagenes, videos, archivos																																											
4	Asesor	Sebastian Marin	SSL VPN	Rut Administrativa	Realiza procesos del sistema del ICANH																																											
5	Bentosa	Empresa encargada de la migracion para AVOIS	SSL VPN	Empresa contratista Bentosa	Acceso a servidor para migracion esta																																											
7	Bentosa	Empresa encargada de migracion PVS	SSL VPN	Empresa contratista Bentosa	Acceso a firewall																																											
11	Formulario de registro de correspondencia	Pérdida de integridad	Aplicar el manual de políticas de seguridad en lo referente a política de control de acceso. Establecer las personas que pueden acceder a la hoja de cálculo. Establecer un periodo de copia de la información por parte del líder de correspondencia Realizar Backup de la hoja de cálculo que está ubicado en Drive y colocar la copia a una unidad compartida. Mantener el aplicativo actualizado	Adquisición, desarrollo y mantenimiento del sistema: A.14.	El riesgo debe ser eliminado, dado que se implementó el aplicativo Orfeo y está funcionando desde el 01-01-2022. No se ejecutaron actividades de control porque no se hizo uso del formulario.	Actualmente se cuenta con un sistema de gestión documental ORFEO, mediante el cual se realiza toda la gestión de la información que entra y sale del Instituto.																																										
25	PLANTA TELEFONICA	Pérdida de integridad	Aplicar el manual de políticas de seguridad en lo referente a política de control de acceso. Ninguna persona está autorizada para intentar acceder a la planta telefónica, en caso de un cambio en la planta se pide apoyo al soporte que es por un año. Para la configuración de los teléfonos se tiene una persona encargada de la esta tarea.	Seguridad física y ambiental: A.11.	Directrices - protección de la infraestructura de información crítica	Se evidencio borrador del documento Directrices Protección de la Información crítica; sin embargo, aún no se encuentra formalizada aprobada, publicada y socializada. Se recomienda gestionar su debida aprobación y tramitar lo correspondiente.																																										
26	EQUIPOS DE COMPUTO	Pérdida de integridad	Se debe aplicar el manual de políticas de seguridad.	Gestión de Activos: A.8.	Resolución de uso de Google Workspace. Reporte antivirus instalado. Política de Seguridad Ítem 7. Se deben actualizar las actividades de control en el riesgo 26, 27 y 28 y se debe	Resolución Workspace adjunta																																										

	PROCESO EVALUACIÓN Y SEGUIMIENTO	CÓDIGO	F-CI-02		
	OFICINA DE CONTROL INTERNO	VERSIÓN	1.0		
	INFORME DE AUDITORIA, EVALUACIÓN Y/O SEGUIMIENTO	PÁGINA	14	DE	19

			Se debe generar una campaña con los usuarios para que empiecen a utilizar las unidades compartidas para la protección de información	Seguridad física y ambiental: A.11.	incluir Actualización de Antivirus y Sistema Operativo de equipo de computo	https://docs.google.com/spreadsheets/d/1-v4-yh8Wpmm7MWprpab-zLny0vBAUBD/edit#gid=282195857 
			Con el soporte del ICANH se debe mirar que todos los equipos de los usuarios tengan instalado el antivirus.	Seguridad operacional: A.12.		https://drive.google.com/drive/u/1/folders/1EOx41KbR_kQ8L5hAbGqS6H2leA6htiGf 
			Se debe generar un documento de roles y responsabilidades para cada usuario en lo que respecta en los controles que se implementen para la seguridad de la información.			
27	ANTIVIRUS	Pérdida de integridad	Se debe revisar que cada PC tenga el antivirus instalado e actualizado. Cuando un usuario el correo le avise de que un archivo adjunto es peligroso debe informar al área de TI para su análisis y bloquear el remitente. El usuario cuando este navegando en internet debe de estar pendiente de las recomendaciones sobre los sitios que visita porque pueden ser peligrosos.	Seguridad operacional: A.12.	Reporte antivirus instalado. Recomendación: Eliminar el Riesgo y unificarlo con el N°26; con el fin de no generar duplicidad. Se deben actualizar las actividades de control en el riesgo 26, 27 y 28 y se debe incluir Actualización de Antivirus y Sistema Operativo de equipo de computo	https://docs.google.com/spreadsheets/d/1-v4-yh8Wpmm7MWprpab-zLny0vBAUBD/edit#gid=282195857 
29	Documentos electrónicos	Pérdida de integridad	Atender a todas las charlas de MINTIC e implementar las normas o recomendaciones que sugieran. Asistir a todas las invitaciones del Comando Conjunto Cibernético en lo referente a infraestructuras críticas. Estar pendientes de todos los boletines informáticos del CSIRT de la Policía Nacional. Participar de los diferentes charts de seguridad de información. Revisión de literatura sobre ciberseguridad en internet	Organización de la seguridad de la información: A.6. Gestión de Activos: A.8. Controles de acceso: A.9. Seguridad operacional: A.12. Adquisición, desarrollo y mantenimiento del sistema: A.14.	Listado de unidades compartidas. Pantallazo de invitaciones reuniones de seguridad. Pantallazo de correos masivos de seguridad.-En el primer semestre no se realizó la actividad. Esta Oficina recomienda modificar actividades de control; dado que se evidencio que las actividades que se realizan están encaminadas a la divulgación, socialización y prevención y no tienen relación directa con la mitigación del riesgo perdida de integridad de los documentos electrónicos.	https://drive.google.com/drive/u/0/folders/1tODV1ZSSWqevC6ju8OI3L2X-juetOYK 

Respecto a la evaluación de los controles y las acciones ejecutadas del Riesgo de Integridad, la Oficina de Control Interno evidenció que del treinta y seis por ciento (36%), el área de Tecnología de la Información en el primer semestre cumplió con el tratamiento del riesgo en un treinta y seis por ciento (36%); siendo esto un nivel satisfactorio en lo referente al cumplimiento



	PROCESO EVALUACIÓN Y SEGUIMIENTO	CÓDIGO	F-CI-02		
	OFICINA DE CONTROL INTERNO	VERSIÓN	1.0		
	INFORME DE AUDITORIA, EVALUACIÓN Y/O SEGUIMIENTO	PÁGINA	15	DE	19

de su rol como segunda línea de defensa y en harás de mitigar la materialización de riesgos en la seguridad de la información de la entidad.

Es necesario que se implementen acciones de mejoramiento para aquellas acciones que presenta oportunidad de mejora; esta Oficina se permite establecer las siguientes recomendaciones:

Nº 11 ítem Formulario de registro de correspondencia: Durante la evaluación el área manifestó que las actividades de control no se están realizando, de acuerdo a que a partir del 01 de enero de 2022 se encuentra en funcionamiento el aplicativo Orfeo, sistema de información por donde se lleva el control de entradas y salidas de correspondencia; el riesgo y las actividades de control se habían establecido para la herramienta tecnológica anterior al Orfeo. Por lo anteriormente expuesto no se obtuvo soporte documental de ejecución y esta Oficina recomienda que dicho riesgo debe ser eliminado, dado que se implementó el aplicativo Orfeo, es necesario que desde el área de TI se evalúe la recomendación realizada por esta Oficina, o si por el contrario debe ser ajustado de acuerdo a las necesidades y posibles riesgos del nuevo aplicativo en la Entidad.

Nº 26 ítem Equipos de Cómputo, Nº 27 Ítem Antivirus y Nº 28 Sistemas Operativos: La Oficina de Control Interno identifico que las actividades de control para los riesgos y los componentes se repiten duplicando la información y dejando de generar valor agregado a la gestión de los riesgos; así mismo identifico que las actividades que pueden simplificarse en un solo riesgo hacen parte del Riesgo de Pérdida de disponibilidad y de integridad, es necesario que desde el área de Tecnologías de la Información se evalúe la pertinencia del riesgo y los controles para establecer en donde debe quedar ubicado las acciones o actividades de control; la OCI recomienda eliminar el Riesgo y unificarlo con el Nº26, 27 y 28; es importante que su actualización se incluyan actividades de actualización de antivirus y Sistema operativo de equipo de cómputo de la Entidad.

Nº 29 ítem Documentos electrónicos: Esta Oficina recomienda modificar las actividades de control; dado que se evidenció que la ejecución realizada está encaminada a la divulgación, socialización y prevención y no tiene relación directa con la mitigación del riesgo pérdida de integridad de los documentos electrónicos.

Sí para el segundo semestre de la vigencia 2022 no se ha realizado actualización a la matriz de riesgos de seguridad de información, deberá implementarse actividades de divulgación como correos masivos de seguridad y/o capacitaciones que permitan a los usuarios de información de la Entidad estar alerta y atentos a posibles irregularidades de seguridad en la información.



	PROCESO EVALUACIÓN Y SEGUIMIENTO	CÓDIGO	F-CI-02		
	OFICINA DE CONTROL INTERNO	VERSIÓN	1.0		
	INFORME DE AUDITORIA, EVALUACIÓN Y/O SEGUIMIENTO	PÁGINA	16	DE	19

1.3. Riesgo: Pérdida de Confidencialidad

N	ITEM	RIESGO	ACTIVIDAD REQUERIDA	Norma ISO/IEC 27001:2013 en su Anexo A	OBSERVACIÓN	Evidencia LINK
12	Base de datos de PQRS	Pérdida de confidencialidad	Controlar los derechos de acceso de los usuarios, por ejemplo, a leer, escribir, borrar y ejecutar-	Organización de la seguridad de la información: A.6.	La Oficina de Control Interno evidencio borrador del Procedimiento copia de seguridad; sin embargo, recomienda que su incorporación se tramite ante la Oficina Asesora de Planeación y su aprobación ante el Comité Institucional de Gestión y Desempeño del ICANH, antes de finalizar la vigencia 2022.	Se evidencio actualización del procedimiento "Gestión de Copia y Restauración de Backup"
			Establecer un procedimiento de copias de respaldo		Política de tratamiento de Datos	
			Establecer o actualizar la Política de tratamiento de datos personales			https://www.icanh.gov.co/index.php?idcategoria=14169
			Comunicar la política a toda la Entidad, especialmente a todas las personas involucradas en el procesamiento de información de datos personales.			

Respecto a la evaluación de los controles y las acciones ejecutadas del Riesgo de Integridad la Oficina de Control Interno evidencio que del seis por ciento (6%), el área de Tecnología de la Información en el primer semestre cumplió con el tratamiento del riesgo en un cuatro punto cinco por ciento (4.5%); siendo esto un nivel satisfactorio en lo referente al cumplimiento de su rol como segunda línea de defensa y en harás de mitigar la materialización de riesgos en la seguridad de la información de la entidad.

Es necesario que se implementen acciones de mejoramiento para el uno punto cinco por ciento (1.5%) restante que presenta oportunidad de mejora a las acciones propuestas; esta Oficina se permite establecer las siguientes recomendaciones:

Nº 12 ítem Base de datos de PQRS: La Oficina de Control Interno evidenció borrador del Procedimiento copia de seguridad; sin embargo, recomienda que su incorporación se tramite ante la Oficina Asesora de Planeación y su aprobación ante el Comité Institucional de Gestión y Desempeño del ICANH, antes de finalizar la vigencia 2022.

2. EVALUACIÓN INFRAESTRUCTURA DE ACTIVOS DE INFORMACIÓN (ACTIVOS CRÍTICOS)

Respecto a la infraestructura de los activos de información la Oficina de Control Interno, mediante reunión de evaluación indago con el área de TI el estado de los documentos: Identificación de activos, activos críticos, sistema de gestión de seguridad de la información SGSI y declaración de aplicabilidad de controles y tratamiento de riesgos, como resultado de dicha



	PROCESO EVALUACIÓN Y SEGUIMIENTO	CÓDIGO	F-CI-02		
	OFICINA DE CONTROL INTERNO	VERSIÓN	1.0		
	INFORME DE AUDITORIA, EVALUACIÓN Y/O SEGUIMIENTO	PÁGINA	17	DE	19

indagación durante la reunión fueron presentado los avances en estado borrador de los documentos antes citado, dada la importancia de dicha documentación la Oficina de Control Interno y el área de TI, establecieron fechas de cumplimiento antes del cierre de la presente vigencia para su finalización, aprobación por parte del Comité Institucional de Gestión y Desempeño, publicación y socialización con la comunidad ICANH.

A continuación, se detallan las actividades y las fechas:

- Avance de algunos activos de información 15/12/2022
- Identificación de Activos Críticos 30/09/2022
- Documentos Sistema de Gestión de Seguridad de la Información SGSI 15/12/2022
- Declaración de aplicabilidad de controles y tratamiento de riesgos 15/12/2022

De acuerdo a la nueva estructura del ICANH, es necesario realizar actualización a la matriz de riesgos de seguridad de información, con el fin de adherir a las áreas nuevas en dicha matriz y actualizar aquellas actividades que ya no se realizan por actualización e implementación de herramientas tecnológicas; por lo anteriormente expuesto también se estableció una fecha tentativa de cumplimiento para la actividad citada.

- Actualización de riesgos conforme a la nueva estructura del ICANH 15/12/2022

Conclusiones

La Oficina de Control Interno evidenció cumplimiento en la gestión realizada por parte del área evaluada, en cuanto a las actividades de control para evitar la materialización de riesgos al interior del ICANH.

Teniendo en cuenta la información suministrada por el área de Tecnología de Información, y de acuerdo a la verificación realizada por esta Oficina a los soportes documentales y a las evidencias que dan cuenta del avance de las actividades de control y el tratamiento de riesgos para el primer semestre de la vigencia 2022, en las herramientas Matriz de Riesgos de Seguridad de la Información, concluye que el tratamiento de riesgos de seguridad de información ejecutados por el área de Tecnología de Información presenta cumplimiento del ochenta y uno por ciento (81%).

Revisados los soportes de las actividades de control de riesgos y del tratamiento de los mismos, se evidenció el cumplimiento en un alto porcentaje de ejecución a la fecha de corte del informe; en este proceso, se pudo observar que el área cuenta con los soportes documentales correspondientes al ejercicio de control y tratamiento de riesgos de TI; así mismo se identificó



	PROCESO EVALUACIÓN Y SEGUIMIENTO	CÓDIGO	F-CI-02		
	OFICINA DE CONTROL INTERNO	VERSIÓN	1.0		
	INFORME DE AUDITORIA, EVALUACIÓN Y/O SEGUIMIENTO	PÁGINA	18	DE	19

avancen significativos en la elaboración de documentación que incide tanto en el tratamiento de riesgos, el cumplimiento del rol de segunda línea de defensa y la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI.

Se cumplió con el objetivo de la evaluación, validándose la aplicación de las normas, el grado de desempeño, los controles establecidos, la trazabilidad de su operación y mejoramiento continuo, fortaleciéndose la gestión de los procedimientos del ICANH.

Recomendaciones

Analizar integralmente y con detenimiento, el contenido de las recomendaciones a cada uno de los riesgos del presente informe de evaluación, de tal manera que, se presente coherencia entre la acción de mejora propuesta, la observación y las respectivas evidencias.

El área tiene un término de tres (3) días para formular el plan de mejora, el cual debe contener todas las acciones que subsanen las observaciones realizadas por el grupo auditor, con el fin de mitigar las inconsistencias evidenciadas.

Dar estricto cumplimiento a la normatividad que regula las actuaciones del tratamiento de riesgos de seguridad de la información, acatar lo dispuesto en los manuales de procesos y procedimientos; para lo cual, deberá solicitar capacitaciones si se requieren con el fin de mantener la buena gestión que hasta el momento se ha evidenciado.

Cumplir a cabalidad los compromisos y las fechas establecidas en el presente informe de acuerdo a la siguiente documentación:

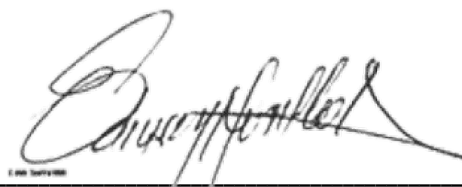
- Avance de algunos activos de información 15/12/2022
- Identificación de Activos Críticos 30/09/2022
- Documentos Sistema de Gestión de Seguridad de la Información SGSI 15/12/2022
- Declaración de aplicabilidad de controles y tratamiento de riesgos 15/12/2022
- Actualización de riesgos conforme a la nueva estructura del ICANH 15/12/2022

Finalizar, formalizar ante el Comité Institucional de Gestión y Desempeño, publicar y socializar con la comunidad ICANH los documentos que fueron presentados en estado borrador en la presente evaluación y cuya finalización debe darse antes del cierre del segundo semestre de la vigencia 2022:



	PROCESO EVALUACIÓN Y SEGUIMIENTO	CÓDIGO	F-CI-02		
	OFICINA DE CONTROL INTERNO	VERSIÓN	1.0		
	INFORME DE AUDITORIA, EVALUACIÓN Y/O SEGUIMIENTO	PÁGINA	19	DE	19

- Procedimiento “Gestión de Copia y Restauración de Backup”
- Documentos Lineamiento tokens-v2 22-07
- Documento Políticas de Grupo Directorio Activo Instituto Colombiano De Antropología E Historia
- Documento Guía para la Gestión de Incidentes.
- Documento Directrices Protección de la Información crítica



Edinson Murillo Albornoz
Oficina de Control Interno

Elaboró: Diana Carolina Garzón – Contratista Control Interno

Fecha de elaboración: 22 septiembre de 2022

Aprobó: Edinson Murillo Albornoz – Jefe de Control Interno

Fecha de Aprobación: 30 septiembre de 2022