



SUBRED INTEGRADA DE SERVICIOS
DE SALUD NORTE E.S.E.



Al contestar por favor cite estos datos:

Radicado No.: 20221400034093

Fecha: 21-11-2022

Bogotá D. C., 21 de noviembre de 2022

Doctor:

DANIEL BLANCO SANTAMARÍA

GERENTE

SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE ESE

Ciudad

ASUNTO: Informe Final Auditoría de Control Interno al Proceso Gestión de Sistemas de información y TICs

Respetado doctor Blanco,

En cumplimiento del Plan Anual de Auditorías de la actual vigencia la Oficina de Control Interno, realizó auditoría al proceso de Gestión de Sistemas de información y TICs.

Como resultado del trabajo realizado adjuntamos el respectivo informe, el cual incluye conclusiones, recomendaciones y oportunidades de mejora de las cuales destacamos:

Conclusiones:

- Con relación al Índice de Desempeño Institucional (IDI) 2021, la Subred presenta una sobrevaloración en FURAG de las políticas de Gobierno Digital (85.9) y Seguridad y Privacidad de la Información (80.4). Esta auditoría evidenció que gran parte de las respuestas entregadas no cuentan con la totalidad de los requisitos técnicos relacionados con el objetivo de la pregunta. En este sentido es importante que tanto los líderes de política como la primera y segunda línea de defensa, realicen una evaluación y análisis al nivel de implementación de las políticas, teniendo en cuenta las recomendaciones de mejora dadas por la medición del FURAG.
- Teniendo en cuenta la tabla de evaluación de efectividad de los controles y de acuerdo con el estándar ISO 27001, se puede evidenciar que la Subred Norte se encuentra en un estado INICIAL, dicho estado hace referencia principalmente a que no hay procesos estandarizados, que los procedimientos están documentados, pero no se aplican y/o están desactualizados. No obstante, se ha logrado avanzar en ciertos grupos de controles que se encuentran en estado REPETIBLE, lo cual indica que existen controles y procedimientos, pero estos no han sido comunicados y la seguridad se basa en los conocimientos y experticia de quienes ejecutan los controles.
- Con la exposición a ataques informáticos sobre equipos de cómputo y servidores causada por malware, más la falta de esquemas y controles de backup sobre activos de información de bases de datos de sistemas de misión crítica, la Subred corre con un altísimo riesgo de experimentar un desastre informático de consecuencias catastróficas.



- La oficina de control interno evaluó el diseño y efectividad de los controles internos en las diferentes etapas del proceso de Sistemas de información y Tic's, evidenciándose debilidades en las actividades de control de acuerdo a lo recomendado por la metodología del DAFP, al no describir claramente el propósito y las acciones a tomar en cuanto se presenten desviaciones que puedan impactar al proceso.
- La Subred Norte, en el proceso de gestión de la información y TICs en términos generales, presenta debilidades en el cumplimiento de los lineamientos y requisitos de seguimiento y controles que tiene establecidos en el mapa de riesgos y la normatividad. Teniendo en cuenta los hallazgos y oportunidades de mejora evidenciadas, es necesario que se tomen acciones correctivas con el propósito de reducir los riesgos que puedan impactar el proceso.

Recomendaciones sobre los hallazgos evidenciados:

- Revisar y actualizar los documentos vigentes del proceso para que sean acorde con las actividades que deben realizarse según las necesidades de cada área.
- Efectuar verificaciones periódicas a las obligaciones contractuales de los proveedores de los servicios contratados por el proceso, para tomar decisiones sobre el pago de las facturas y Cumplir las disposiciones de la Circular Externa 01 de 2021 de Colombia Compra Eficiente, relacionada con la publicación de la totalidad de documentos del proceso de seguimiento Contractual en la plataforma SECOP II.
- Gestionar en coordinación con la Oficina de Desarrollo Institucional, la actualización del mapa de riesgos del proceso de gestión de la información y TIC, reforzando la identificación de causas, descripción y redacción de riesgos y controles, metas e indicadores de acuerdo a la metodología institucional que sea definida.
- Evaluar la implementación del mapa de riesgos de corrupción del proceso
- Realizar verificación de lo establecido por las TRD, para la oficina de sistemas de información y TICs código AP-GI-T-20-01 y del acuerdo 042 del Archivo General de la Nación.
- Mantener un expediente individual de los equipos de cómputo con todo lo relacionado con hoja de vida, mantenimientos, repuestos, software y licencias para garantizar la información de estos activos.
- Realizar seguimientos periódicos y realizar ajustes necesarios al cronograma de mantenimientos teniendo en cuenta las modificaciones que se van presentado para lograr el cumplimiento del cronograma y/o plan de mantenimiento.
- Fortalecer el proceso de diligenciamiento del instrumento de evaluación de las políticas y realizar seguimiento adecuado a las respuestas que son entregadas durante el diligenciamiento del FURAG
- Implementar un plan de contingencia para situaciones en las que se presenten fallas de los aplicativos que soportan los procesos internos de la institución para mitigar los impactos por pérdida de información.
- Hacer seguimiento periódico a las fechas de vencimiento de las licencias y permisos de los programas que son requeridos por la institución para su normal funcionamiento y de esta manera anticiparse para tomar decisiones y agilizar los procesos de adquisición de los bienes y servicios requeridos.



SUBRED INTEGRADA DE SERVICIOS
DE SALUD NORTE E.S.E.

9. Gestionar oportunamente incidentes de Seguridad de la Información que impacten negativamente en las operaciones de la Subred, con cabal cumplimiento de los procedimientos de reporte, análisis, contención, aprendizaje y mejora de los controles.

Cualquier inquietud información adicional con gusto será suministrada.

Cordialmente,

LUIS ANTONIO RODRÍGUEZ OROZCO
Jefe Oficina Control Interno
Subred Integrada de Servicios de Salud Norte E.S.E.

Copia; Dr. Oscar Javier Manrique Ladino. Subgerente Corporativo
Dra. Yanith Piragauta Gutiérrez. Subgerente de Prestación de Servicios de Salud
Dra. Luz Myriam Roncancio. Directora Financiera
Dr. Oscar Javier Manrique Ladino. Director Oficina de Desarrollo Institucional (E)
Dra. Mónica Etelmira González Montes. Jefe Oficina Jurídica
Dra. Diana Marcela Caballero Arias Jefe Oficina de Calidad
Ing. Yolanda Bernal González. Jefe Oficina de Sistemas de información y TICs (E)

	Nombre	Cargo	Firma
Elaborado y Proyectado por:	Oscar Iván Vergara Medina / Luis Antonio Trisancho Robles	Profesional Oficina de Control Interno	
Aprobado por:	Luis Antonio Rodríguez Orozco	Jefe Oficina Control Interno	
Declaramos que hemos revisado el presente documento y lo encontramos ajustado a las normas y disposiciones legales y por lo tanto lo presentamos para la firma			

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO	CÓDIGO: EV-EG-F-03-01
		VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN	PÁGINA: 1 DE 70
		FECHA: 03/05/2021

AUDITORÍA “GESTIÓN DE LA INFORMACION Y TICS SUBRED NORTE E.S.E”

Fecha de elaboración del informe	Noviembre de 2022
Periodo auditado	enero 2022 – junio 2022
Macro proceso	Apoyo – Gestión de la Información y Tics
Proceso	Gestión de la Información y Tics
Líder de Proceso	Yolanda Bernal González
Auditor responsable	Oscar Iván Vergara M. / Luis Antonio Trisancho R.

TABLA DE CONTENIDO

INTRODUCCIÓN.....	3
1. OBJETIVOS.....	3
1.1. General.....	3
1.2. Específicos.....	3
2. ALCANCE.....	4
3. EXCLUSIONES Y LIMITACIONES DE LA AUDITORÍA.....	4
4. METODOLOGÍA.....	4
5. CRITERIOS NORMATIVOS DEL PROCESO.....	6
6. GENERALIDADES DEL PROCESO.....	7
6.1. Verificación de Documentación y Procedimientos.....	7
6.2. Verificación de Contratos de Servicios Tecnológicos.....	9
6.3. Verificación de Metas del POA.....	10
7. RESULTADO DE LA AUDITORÍA.....	15
7.1. Resumen de hallazgos.....	15
7.2. Nivel de Aseguramiento de Controles y Gestión de Riesgo.....	18
7.3. Verificación de Controles de los riesgos.....	19
7.4. Riesgos relacionados con la seguridad y privacidad de la Información - Evaluación de la Política de Seguridad Digital.....	24

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO	CÓDIGO: EV-EG-F-03-01
		VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN	PÁGINA: 2 DE 70
		FECHA: 03/05/2021

7.5. Evaluación de la Política de Gobierno Digital	40
7.6. Riesgos de corrupción	50
7.7. Descripción de hallazgos generados	50
8. CONCLUSIONES.....	67
FORTALEZAS	68
OPORTUNIDADES DE MEJORA.....	69
SOLICITUD DE PLAN DE MEJORAMIENTO.....	70
ANEXOS	70

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO	CÓDIGO: EV-EG-F-03-01
		VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN	PÁGINA: 3 DE 70
		FECHA: 03/05/2021

INTRODUCCIÓN.

En cumplimiento del rol de evaluación y seguimiento de la Oficina de Control Interno de la Subred Norte y al Plan Anual de Auditorías de la vigencia 2022, se lleva a cabo la auditoría al proceso de Gestión de la Información y Tics; proceso cuyo objetivo es *“Proponer, desarrollar e implementar herramientas tecnológicas, de comunicaciones, manejo de información y documentación que permitan a Subred Integrada de Servicios de Salud Norte E.S.E, apoyar el proceso de toma de decisiones de la dirección”*.

En este sentido, la auditoría al proceso en mención, tiene como propósito revisar y evaluar aspectos relacionados con procesos, procedimientos, actividades y controles previstos, así como el uso eficiente y seguro de los recursos tecnológicos de información que dan soporte a la operación de la entidad.

Es importante resaltar que el tratamiento eficiente de los riesgos, es una estrategia de la Subred Norte para el cumplimiento de los objetivos estratégicos; por lo tanto adopta mecanismos y acciones que permitan prevenir los riesgos y minimizar su impacto, dentro de los que se encuentra la auditoría que se presenta a continuación.

1. OBJETIVOS.

1.1. General.

Evaluar la implementación de los mecanismos de control establecidos en el proceso de Sistemas de Información y TIC's, con el fin de verificar el cumplimiento normativo, lineamientos internos y externos, buenas prácticas de gestión de TICS y metodologías implementadas.

1.2. Específicos.

- Evaluar el cumplimiento del proceso de Gestión de la Información y TICS's, verificando el estado documental de procedimientos, planes, contratos de servicios tecnológicos, manuales y políticas.
- Evaluar el nivel de aseguramiento de los controles y gestión de riesgos del proceso Gestión de la Información y TIC's.
- Identificar los posibles riesgos que impacten en las actividades críticas del proceso de Gestión de Información y TIC's.

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO	CÓDIGO: EV-EG-F-03-01
		VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN	PÁGINA: 4 DE 70
		FECHA: 03/05/2021

- d. Revisar y evaluar el avance en la implementación las políticas de Gobierno Digital y Seguridad y Privacidad de la Información.
- e. Verificar el cumplimiento de planes de mejora vigentes, establecidos para el proceso.
- f. Evaluar el soporte de las respuestas dadas por la entidad en el diligenciamiento del Formulario Único de Reporte y Avance de Gestión - FURAG, relacionadas con la política de Gobierno y Seguridad Digital.
- g. Presentar recomendaciones y oportunidades de mejora.

2. ALCANCE.

La auditoría se realizó entre el 8 de agosto y el 26 de octubre de 2022 en las instalaciones de la Subred Norte, verificando la gestión realizada por el proceso en el periodo comprendido por el primer semestre de 2022

3. EXCLUSIONES Y LIMITACIONES DE LA AUDITORÍA.

En la fase de planeación de la presente auditoría se priorizaron actividades del proceso de Gestión de la Información y Tics, excluyendo aquellas que cumplieran con los siguientes criterios: (1) actividades y procedimientos evaluados por otros sistemas (actividades de acreditación) y/o procesos (actividades de gestión documental), y (2) procesos puntuales abordados en auditorías recientes (auditoría de derechos de autor).

4. METODOLOGÍA.

La presente auditoría se encuentra basada en riesgos, cumpliendo así con las fases y procedimientos definidos en la versión 4 de la “Guía de *auditoría interna basada en riesgos para entidades públicas*” y contempla lo siguientes aspectos

1. Planificación de la auditoría

- Conocimiento del proceso: Esta actividad se llevó a cabo a través de la verificación de la documentación obtenida de la Intranet y la página WEB de la Subred. En este trabajo se pudo identificar el proceso SI-C-01-01-Gestión de la Información y Tics y la documentación anexa de procedimientos, guías y manuales.
- Presentación del plan de la auditoría: Teniendo en cuenta la anterior actividad, se diseñó el plan y cronograma de trabajo, el alcance, objetivos y las pruebas requeridas para

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO	CÓDIGO: EV-EG-F-03-01
		VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN	PÁGINA: 5 DE 70
		FECHA: 03/05/2021

determinar el adecuado diseño de controles. Con la reunión de apertura del 5 de agosto de 2022, se dio a conocer el plan de la auditoría al grupo determinado por la líder de la oficina de Sistemas de Información y Tics y se determinaron los enlaces.

- Levantamiento de Información: Para esta fase se realizó una revisión documental detallada junto con inspección de evidencia física, un recorrido del proceso y flujo de información apoyado través de entrevistas y validación de información con el líder del proceso y el personal involucrado.

2. Ejecución de la auditoría

- Análisis de la Información recolectada: Con el fin de verificar los requisitos del proceso, se analizaron los riesgos relacionados con el proceso, descritos en el mapa de riesgos de la Subred, los manuales, procedimientos, instructivos, formatos, políticas, indicadores, reportes y en general documentos definidos y estandarizados del proceso y publicados en la intranet de la Subred y solicitados con posterioridad al inicio de la auditoría.
- Diseño y ejecución de Pruebas: Se aplicaron pruebas definidas para: (1) verificación del estado de las políticas de gobierno digital, (2) determinar el grado de madurez del sistema de seguridad y privacidad de la información, (3) determinar el estado de los controles de seguridad de la información, de acuerdo con la norma NTC-ISO 27002/27005, (4) determinar el estado de aseguramiento de las terminales financieras, (5) pruebas de campo con el fin de cotejar la información de indicadores y controles específicos del proceso.

3. Identificación de hallazgos y observaciones auditoría.

- Con la información analizada y verificada, junto con el resultado de las pruebas realizadas, se generaron una serie de hallazgos y recomendaciones resultantes de la comparación entre el criterio (ley, norma técnica, procedimiento, manual, instructivo, etc.) y el estado actual de la actividad/procedimiento.

4. Elaboración del Informe preliminar

- Teniendo en cuenta la identificación de hallazgos y observaciones, se procede con la elaboración del documento que sintetiza los resultados de la auditoría, mostrando los aspectos que fueron examinados, destacando las oportunidades de mejora y

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO	CÓDIGO: EV-EG-F-03-01
		VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN	PÁGINA: 6 DE 70
		FECHA: 03/05/2021

observaciones evidenciadas. Dicho informe es revisado y aprobado por el jefe de la Oficina de Control Interno.

5. Socialización del Informe

- Se realiza la socialización del informe con responsables y líderes del proceso, cuyo objetivo es informar acerca de las acciones de mejora, los hallazgos y observaciones evidenciadas durante el trabajo de auditoría, de manera que éstos puedan ser identificados por los líderes del proceso, y a su vez se realicen las aclaraciones que haya lugar.

5. CRITERIOS NORMATIVOS DEL PROCESO

A continuación, se enumeran los criterios normativos de verificación de cumplimiento:

- Ley 87 de 1993. Por medio de la cual se establecen normas para el ejercicio del Control Interno en las entidades y organismos del Estado.
- Ley 1474 de 2011. Estatuto Anticorrupción.
- Ley 1712 de 2014. Por la cual se crea la “Ley de Transparencia y del Derecho a la Información Pública Nacional”.
- Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 415 de 2016. Definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones.
- Decreto 1008 de 2018. Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
- Directiva 02 de 2019. Simplificación de la interacción digital ciudadanos y estado.
- Manual de implementación Política de Gobierno Digital. MINTIC, V.7 de abril de 2019.
- Manual operativo del Modelo Integrado de Planeación y Gestión. Dimensión Gestión con Valores para Resultados. numeral 3.2.1.2 Política Gobierno Digital. Versión 4 de 2021.
- Resolución MINTIC 001519 de 2020. Por la cual se definen estándares y directrices para publicar información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.
- Anexo A ISO 27001
- NTC-ISO 27002: Código de practica para la gestión de la seguridad de la información

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO	CÓDIGO: EV-EG-F-03-01
		VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN	PÁGINA: 7 DE 70
		FECHA: 03/05/2021

- NTC-ISO 27005: Gestión del riesgo en la seguridad de la información
- Instrumentos, manuales y guías de implementación Política de Gobierno y seguridad Digital - MINTIC
- Plan Estratégico de Tecnologías de la Información - PETI
- Procedimientos Gestión de la información y TICs.
- Mapa de Riesgos proceso Gestión de la información y TICs.
- Planes de mejoramiento proceso Gestión de la información y TICs.
- Indicadores proceso Gestión de la información y TIC'S
- Caracterización Gestión de la información y TICs
- Plan de seguridad y privacidad de la información

6. GENERALIDADES DEL PROCESO

La presente auditoría se realizó de acuerdo con la metodología, alcance y objetivos propuestos, así como el uso de las herramientas de auditoría presentadas en la reunión de apertura con los profesionales designados por la jefe de oficina de Tics.

6.1. Verificación de Documentación y Procedimientos

El proceso de Gestión de la Información y Tics se encuentra enmarcado dentro el macroproceso de apoyo y su caracterización se describe en el documento No. SI-C-01-01. Para la presente auditoría se priorizaron 33 de las 49 actividades descritas en la caracterización, como se muestra en la siguiente tabla:

CICLO	ACTIVIDAD DEL PROCESO
P	Identificar y actualizar periódicamente los lineamientos y directrices de Seguridad de la Información.
P	Elaborar cronogramas de desarrollo y mantenimiento de la plataforma informática y generación de copias de seguridad.
P	Elaborar y actualizar acorde a las necesidades institucionales el diagnóstico de necesidades de los sistemas de información.
P	Establecer el plan de formación y capacitación en relación con la seguridad de la información dirigido a todos los colaboradores articulado con Gestión de Talento Humano.
P	Identificar los riesgos de seguridad de la información.
P	Definir y actualizar el Plan Estratégico de Tecnologías de la Información y las comunicaciones, Plan de Contingencia de los Sistemas de Información, demás planes y programas.
P	Diseñar herramientas y elementos de Control de la información y de la arquitectura del sistema.
P	Definir el Plan Administrativo por Área.

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO	CÓDIGO: EV-EG-F-03-01
		VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN	PÁGINA: 8 DE 70
		FECHA: 03/05/2021

CICLO	ACTIVIDAD DEL PROCESO
H	Efectuar el monitoreo de las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas.
H	Apoyar la implementación de la estrategia de Gobierno en Línea y Anti trámites.
H	Implantar los controles que permitan una rápida detección y respuesta a los incidentes de seguridad.
H	Realizar el seguimiento a contratos afines al proceso.
H	Realizar la clasificación y control de activos de información.
H	Prevenir e impedir accesos no autorizados, daños e interferencias a las sedes, instalaciones e información de la Subred Integrada de Servicios de Salud Norte E.S.E.
H	Gestionar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y comunicaciones.
H	Minimizar los efectos de las posibles interrupciones de las actividades normales de la Unidad Integrada de Servicios de Salud Norte E.S.E. y proteger los procesos críticos mediante la combinación de controles preventivos y acciones de recuperación.
H	Realizar la capacitación, entrenamiento y evaluación de conocimiento y adherencia a los procesos de seguridad de la información.
H	Realizar la investigación de los incidentes de seguridad de la información cuando estos ocurran.
H	Implementar y gestionar las actividades, estrategias y proyectos del Plan Estratégico de Tecnologías de la Información y Comunicaciones.
H	Gestionar los requerimientos técnicos, de información y mantenimiento de equipos.
V	Hacer seguimiento a la ejecución del Plan Estratégico de Tecnologías de la Información y Comunicaciones, Plan de Contingencia de los Sistemas de Información, Plan Administrativo por Áreas.
V	Evaluar el cumplimiento de los estándares de seguridad de la información.
V	Analizar y hacer seguimiento de los Indicadores de gestión, cumplimiento del cronograma de actividades, monitorización periódica y sistemática de riesgos y de adherencia a la política y lineamientos de seguridad de la información.
V	Identificar oportunamente las brechas e incidentes de seguridad.
V	Evaluar la efectividad de los controles para verificar que se cumple con los requisitos de seguridad.
V	Revisar el SGSI por parte de la alta dirección.
V	Registrar acciones y eventos que puedan tener impacto sobre la efectividad o rendimientos del SGSI.
A	Ajustar el mapa de riesgo del proceso acorde a resultados.
A	Realizar acciones preventivas, correctivas y de mejora acordes a los análisis de resultado de indicadores, de las investigaciones de incidentes de seguridad de la información, seguimiento del proceso.
A	Seguridad de la Información en función de las conclusiones y hallazgos encontrados durante las actividades de monitorización y revisión.
A	Comunicar las acciones y mejoras a todas las partes interesadas.
A	Implantar en el SGSI las mejoras identificadas.
A	Documentar las acciones establecidas en la mejora de proceso.

Tabla No. 1: Actividades priorizadas del proceso de Gestión de la Información y Tics
Elaboración Oficina de Control Interno

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO	CÓDIGO: EV-EG-F-03-01
		VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN	PÁGINA: 9 DE 70
		FECHA: 03/05/2021

Al verificar la documentación obtenida de la Intranet y la página WEB de la Subred, se encontró que el proceso SI-C-01-01-Gestión de la Información y Tics, cuya fecha de versión es de abril de 2017, se encuentra desactualizado, toda vez que: (1) no obedece a políticas tales como las incorporadas por el MIPG (Gobierno Digital) y (Seguridad y Privacidad de la Información), (2) presenta una escasa caracterización de riesgos y activos de información, (3) procedimientos que no son ejecutados dentro del proceso - (Desarrollo y mantenimiento de la página WEB), (4) Documentos - (PESI) y (5) manuales desactualizados - (generación de copias de seguridad Backups), entre otros. La anterior situación evidencia una brecha entre lo documentado y lo ejecutado, motivo por el cual se presenta el hallazgo No. 01.

6.2. Verificación de Contratos de Servicios Tecnológicos

Durante la auditoría se realizó verificación de los contratos 056-2019 y 052-2022 que corresponden a contratar la prestación de los servicios de alquiler de equipos de cómputo, scanner, lectores y otros equipos para garantizar la adecuada prestación del servicio dentro de la subred norte celebrado con **NECSOFTPC LTDA** donde según manifiesta el proceso auditado, se presentan incumplimientos principalmente en los mantenimientos y visitas técnicas, entre otras clausulas, no obstante, esta oficina no logro corroborar dichos incumplimientos, toda vez que los informes de seguimiento y supervisión de contrato no los reflejaba.

Adicionalmente se revisó el contrato 143-2020 referente a contratar el servicio de impresión, fotocopiado y scanner para el desarrollo de las actividades operacionales de las diferentes dependencias de la Subred Norte celebrado con el proveedor **GRAN IMAGEN**, en el cual se pudo evidenciar que presentan incumplimiento en cuanto a: (1) falta de soporte técnico, (2) falta de cronograma de mantenimientos desde que inicio contrato a la fecha, (3) inoportunidad en la entrega de información de consumos, (4) falta de insumos de papel y demás suministros de impresoras. Dada la problemática anteriormente expuesta se han visto afectados los servicios asistenciales y administrativos por periodos prolongados de tiempo, adicionalmente la publicación de los soportes de seguimiento y ejecución del contrato en la plataforma SECOP por parte del supervisor es incompleta. Situación que genera el hallazgo No. 02, relacionado con la debilidad en la supervisión de los contratos.

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO	CÓDIGO: EV-EG-F-03-01
		VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN	PÁGINA: 10 DE 70
		FECHA: 03/05/2021

6.3. Verificación de Metas del POA

Para la oficina de Sistemas de información y TICs se tiene planteadas 4 metas directas dentro del Plan Operativo Anual para la vigencia 2022. A continuación, se muestran las observaciones y seguimiento de dichas metas para el periodo del primer semestre del 2022

TIPO DE METAS	METAS POA 2022	Propuesta de actividades
DIRECTAS	24. Disminuir el 10% del consumo de papel por dependencias, tomando como línea base la vigencia 2021.	• Elaboración de estrategias que incentiven la disminución del consumo del papel. • Realizar informe con medición por dependencia de la disminución por dependencias del consumo de papel (sistemas)
	5. Medir la oportunidad en la asignación de las salas de cirugía de urgencias	• Organizar una herramienta de tiempos y movimientos para las salas de cirugía (sistemas). • Realizar un informe trimestral con la descripción de la línea de tiempo de las salas y reporte de numero de procedimientos realizados
	64. Implementar al 100% la integración entre el sistema Radiologic information system - RIS- contratado por la Subred Norte para imágenes diagnósticas y el Sistema de información Servinte.	•Contratación del operador de sistemas para imágenes diagnosticas. (Subgerencia Corporativa). •Elaboración del plan de trabajo de integración entre el sistema RIS y Servinte. •Implementar al 100% el plan de trabajo propuesto para la integración. •Evaluar la integración entre el sistema RIS y Servinte. •Informe de resultados de la integración del sistema RIS y Servinte.
	65. Mapear o documentar las necesidades de tecnologías de información y comunicaciones de la Subred Norte, para el 100% de las unidades de servicios de salud, estableciendo los recursos técnicos, humanos y financieros requeridos.	•Elaboración de diagnóstico •Definir necesidades relacionadas con las tecnologías de la información y comunicaciones. •Realizar el documento del mapeo de necesidades el cual debe ser aprobado por el comité de Gestión y Desempeño.
APORTE OTRAS METAS	1. Desarrollar el 100% del plan de trabajo para la implementación de la herramienta de indicadores del Sistema de Gestión de Calidad ALMERA, para el seguimiento al sistema de información institucional.	•Definir Plan de trabajo y cronograma de implementación de la herramienta Almera, para el seguimiento al sistema de información. •Desarrollo del plan de trabajo para la implementación de la herramienta Almera. •Presentar informe trimestral del avance a las acciones propuestas
	Lograr un cumplimiento mayor o igual al 95% de las acciones del plan de mejoramiento del sistema único de acreditación - SUA	•1er trimestre. Participación en la autoevaluación de acreditación. •2do trimestre: Formulación del plan de mejoramiento del SUA por proceso. •3er y 4to trimestre: Seguimiento a los planes de mejoramiento del SUA por proceso.

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO	CÓDIGO: EV-EG-F-03-01
		VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN	PÁGINA: 11 DE 70
		FECHA: 03/05/2021

	Actualizar y monitorear de manera trimestral el mapa de riesgos por proceso de la Subred	•Proceso de capacitación en el módulo de Almera •Diligenciamiento del módulo de Almera por cada proceso •Seguimiento trimestral de resultados •Acompañamiento continuo durante el proceso •Informe semestral de seguimiento al mapa de procesos, Excel con seguimiento y listados de asistencia
--	--	---

Tabla No. 2: Seguimiento POA de 2022- Gestión de la Información y Tics
Fuente: Oficina de Desarrollo Institucional

De acuerdo con el seguimiento realizado, se pudo establecer el siguiente resultado con corte al segundo trimestre de 2022:

Para la **Meta 1.** relacionada con la disminución del 10% de consumo de papel por dependencias, se tuvieron los siguientes resultados comparativos de 2022 frente a la vigencia 2021.

No.	PROCESO	1er. Trimestre			2do. Trimestre		
		2.021	2022	Variación	2.021	2022	Variación
1	Control Interno	0	50.602	✗ 0%	27.839	36.819	✗ 32%
2	Subgerencia Corporativa	81.403	16.563	✓ -80%	87.371	18.748	✓ -79%
3	Comunicaciones	3.310	1.171	✓ -65%	3.241	2.664	✓ -18%
4	Dirección Administrativa	393.122	172.271	✓ -56%	308.004	148.250	✓ -52%
5	Mercadeo	3.833	1.727	✓ -55%	20.586	1.487	✓ -93%
6	Gestión de servicios complementarios	179.805	134.571	✓ -25%	272.440	235.888	✓ -13%
7	Dirección Gestión del Riesgo	1.033.630	922.225	✓ -11%	1.239.526	565.007	✓ -54%
8	Dirección de Urgencias	347.347	321.759	✗ -7%	438.882	346.336	✓ -21%
9	Gestión financiera	1.356.864	1.281.638	✗ -6%	1.349.542	1.544.683	✗ 14%
10	Oficina de Calidad	4.142	4.187	✗ 1%	4.604	4.041	✓ -12%
11	Gerencia	2.815	3.138	✗ 11%	2.700	4.235	✗ 57%
12	Participación social y atención al usuario	9.449	8.692	✗ -8%	41.152	9.695	✓ -76%
13	Dirección Servicios Ambulatorios	485.177	604.744	✗ 25%	601.810	627.708	✗ 4%
14	Dirección Hospitalarios	975.280	1.244.817	✗ 28%	1.229.696	1.318.287	✗ 7%
15	Dirección Talento Humano	4.587	6.121	✗ 33%	5.237	6.284	✗ 20%
16	Dirección Contratación	26.576	55.988	✗ 111%	26.375	74.810	✗ 184%
17	Oficina de Gestión del conocimiento	0	0	✗ 0%	-	1.722	✗ 0%
TOTAL		4.907.340	4.830.214	✗ -2%	5.659.005	4.946.664	✓ -13%

Tabla No. 3: Prueba de recalculation de disminución de consumo de papel
Fuente: Oficina de Control Interno

En la anterior tabla se puede observar que, aunque para el primer trimestre de la actual vigencia no se dio cumplimiento con lo propuesto; para el segundo trimestre la situación mejoró de manera significativa de tal forma que se dio cumplimiento a la meta. También se puede observar que el 53% de las dependencias evaluadas si están reduciendo notablemente el consumo.

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO	CÓDIGO: EV-EG-F-03-01
		VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN	PÁGINA: 13 DE 70 FECHA: 03/05/2021

Frente a la certificación y pago de las facturas del contrato se puede configurar un posible riesgo de corrupción toda vez que se certifican facturas sin cumplimiento pleno de las obligaciones, situación que reitera el hallazgo No. 02.

Frente a la Meta 2 del POA se pudo determinar que, durante el primer semestre de 2022 se han realizado mesas de trabajo para definir las mejores opciones de herramientas que permitan la medición de tiempos y movimientos, por lo anterior se realizó el instructivo de “medición de tiempos y movimientos quirúrgicos” el cual se encuentra en proceso de revisión por parte del líder del proceso.

En la reunión sostenida con la referente de salas de cirugía, se estableció incluir variables en las Plantilla de programación y cancelación de cirugías mensuales para que sean diligenciadas a partir de julio de 2022, con el fin de dar respuesta al requerimiento para la medición de la oportunidad de asignación de cirugías de urgencias. Las variables son:

- Fecha de entrega de boleta a salas de CX
- Hora de entrega de boleta a salas de CX
- Fecha de solicitud procedimiento (por el especialista)
- Hora de solicitud procedimiento (por el especialista)

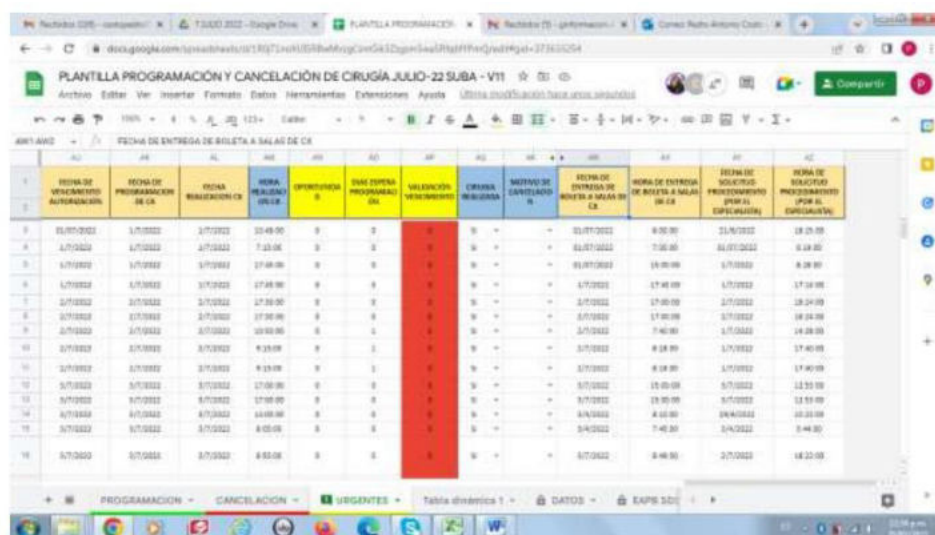


Imagen No. 2: Base de Drive de programación y cancelación de urgencias Julio
Fuente: Oficina de Sistemas de información y TICs.

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO	CÓDIGO: EV-EG-F-03-01
		VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN	PÁGINA: 14 DE 70
		FECHA: 03/05/2021

Teniendo en cuenta las actividades realizadas y los soportes aportados por el proceso la oficina de control interno considera que se está cumpliendo con esta meta.

Para la Meta 3 se tiene establecido Implementar al 100% la integración entre el sistema Radiologic information system - RIS- contratado por la Subred Norte para imágenes diagnósticas y el Sistema de información Servinte. Sobre este respecto se evidencia la suscripción del contrato 030-2022 de la Subred con la empresa EDX tecnología en salud S.A.S, cuyo objeto es “Contratar el servicio de alquiler del Sistema de Información Radiológico (RIS) y el sistema de almacenamiento y distribución de imagen de archivos DICOM (PACS) para el servicio de imágenes diagnosticas de las diferentes unidades de servicios de salud que conforman la Subred Norte”, al verificar la invitación a cotizar 009-2022 se observó que se presentaron 4 ofertas y se realizó la selección y adjudicación de la empresa EDX, que a respecto se tiene establecido un cronograma de actividades para la implementación del sistema RIS como se pudo evidenciar en reunión sostenida el 11 de mayo de 2022, entre el personal de la subred (Referente de imágenes Diagnosticas) y de la empresa EDX.

Con la realización de estas actividades se considera que la meta para este periodo se está cumpliendo adecuadamente.

Frente la Meta 4 de Mapear o documentar las necesidades de tecnologías de información y comunicaciones de la Subred Norte, para el 100% de las unidades de servicios de salud, estableciendo los recursos técnicos, humanos y financieros requeridos. Frente a esta meta no se tiene soporte documental que permita definir el porcentaje de avance de cumplimiento de la meta.

La oficina de sistemas realizó una encuesta en junio de 2022 a los líderes de los procesos de la subred, con el propósito de identificar las principales necesidades tecnológicas. A continuación, se muestra imagen de la encuesta.

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO	CÓDIGO: EV-EG-F-03-01
		VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN	PÁGINA: 15 DE 70
		FECHA: 03/05/2021



Imagen No. 3: Encuesta de necesidades de tecnologías de la información y comunicaciones

Fuente: Oficina de Sistemas de información y TICs

De la encuesta se recibieron 36 respuestas distribuidas como muestra la siguiente tabla:

Proceso	# de Respuestas	Unidad de servicio	# de Respuestas
Gestión de Hospitalización y cirugía	30	UMHES SIMON BOLIVAR	26
Participación social y Atención al Usuario	2	UMHES ENGATIVA CALLE 80	3
Gestión estrategica	1	UMHES CSE SUBA	3
Gestión de Servicios Complementarios	1	CAPS CHAPINERO	2
Gestión de la informacion y TICs	1	CAPS EMAUS	1
Gestion del ambiente Físico y Tecnológico	1	CAPS FRAY BARTOLOME DE LAS CASAS	1

Tabla No. 4: Acumulado de repuestas por proceso

Fuente: Oficina de Sistemas de información y TICs

Como se puede observar, no se está dando cubrimiento al 100% de las unidades ni procesos, por lo que esta oficina recomienda reforzar las actividades para lograr cumplir con la meta de establecer un documento o estrategia con las necesidades identificadas para todos los procesos de la subred.

7. RESULTADO DE LA AUDITORÍA

7.1. Resumen de hallazgos

En el siguiente cuadro se presenta un resumen de los hallazgos encontrados durante la auditoría:

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO	CÓDIGO: EV-EG-F-03-01
		VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN	PÁGINA: 16 DE 70
		FECHA: 03/05/2021

No.	HALLAZGO	PAG. INFORME
01	Debilidades en la documentación del proceso SI-C-01-01-Gestión de la Información y Tics	9
02	Supervisión ineficiente de los contratos a cargo del proceso de Sistemas de Información y TICs generando un posible riesgo de corrupción frente a la certificación y pago de las facturas de los contratos, dado que no se tiene un control adecuado sobre los incumplimientos reiterados de las obligaciones contractuales, adicionalmente no se están publicando los soportes de supervisión y ejecución de los contratos en la plataforma SECOP II	9
03	Deficiencias metodológicas en el diseño y redacción de los controles definidos para la mitigación de los riesgos del proceso. Adicionalmente el mapa de riesgos de gestión se encuentra desactualizado y no contempla posibles riesgos por actos de corrupción.	20
04	Las carpetas y archivo de los documentos del proceso, no cumplen con lo establecido y reglamentado en el acuerdo 042 del archivo general de la nación.	20
05	Incumplimiento en el plan de mantenimiento de equipos de cómputo y ausencia de mantenimiento en servidores, lo que genera una posible pérdida en la disponibilidad e integridad de la información ocasionada por daños en servidores y equipos de cómputo.	21
06	Incumplimiento al Acuerdo de Nivel de Servicios establecido en el documento AP-GI-I-19-01.	23
07	Ausencia de documentación y/o evidencias que soporten la totalidad de las respuestas, en términos de los requisitos técnicos relacionados con el objetivo de la pregunta del FURAG 2021, generando sobre calificación de las Políticas de Seguridad y Gobierno Digital.	34
08	Materialización del riesgo de daño en la base de datos de Orfeo, con pérdida en la disponibilidad de la información y posible compromiso de los datos, sin que mediara un procedimiento documentado sobre la gestión del incidente.	34
09	Exposición de la información almacenada en los equipos de cómputo y servidores a ataques informáticos causada por malware, debido al vencimiento del sistema antivirus.	34

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO	CÓDIGO: EV-EG-F-03-01
		VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN	PÁGINA: 17 DE 70
		FECHA: 03/05/2021

No.	HALLAZGO	PAG. INFORME
10	Falta de un plan de continuidad del negocio y ejercicios de simulación y respuesta ante el evento de que una amenaza explote una vulnerabilidad de un activo de información crítico.	35
11	El inventario de activos de información de la Entidad no contempla los inventarios de activos de información de Tics, ni la caracterización de los riesgos de seguridad y privacidad de la información de acuerdo con la metodología definida por el DAFP y MINTIC.	35
12	Fallas en los procedimientos y políticas de control de acceso a aplicaciones y servicios informáticos. Se debe evitar el acceso no autorizado a sistemas y servicios.	38
13	Desactualización de los procedimientos e inexistencia de esquemas de Backup sobre activos de información altamente críticos como son las bases de datos de sistemas en producción.	38
14	No se cuenta con un plan de concienciación enmarcado dentro de un proceso de mejora continua del SGSI, que dé cuenta del avance efectivo y de la importancia sobre la seguridad de la información en la Subred	39
15	La mayoría de centros de cableado y cuartos de comunicaciones presentan riesgo de pérdida en la disponibilidad y confidencialidad de la información, toda vez que existen deficiencias en cuanto a su restricción de acceso, organización interna de los dispositivos, documentación, planos, certificación y demás condiciones físicas.	40

Tabla No. 5: Resumen de hallazgos

Breve descripción de las pruebas de auditoría realizadas

Con el fin de evaluar la efectividad de los controles existentes en el proceso de Gestión de la información y TIC's diseñados para mitigar los riesgos más críticos, la auditoría aplicó algunas pruebas, las cuales se describen a continuación:

	INFORME FINAL		CÓDIGO: EV-EG-F-03-01
	AUDITORIAS DE CONTROL INTERNO		VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN		PÁGINA: 18 DE 70
			FECHA: 03/05/2021

7.2. Nivel de Aseguramiento de Controles y Gestión de Riesgo

Como insumo para la ejecución del trabajo de verificación, la Oficina de Control Interno tomó el mapa de **riesgos de gestión** del proceso publicado en la página WEB, el cual se encuentra desactualizado, toda vez que no cumple con lo definido en la política de riesgos y la metodología de desarrollo del Departamento Administrativo de la Función Pública DAFP, versión 4. Situación que genera el hallazgo No. 03.

El mapa muestra un total de 5 riesgos, clasificados de la siguiente manera: (3) riesgos en estado alto y (2) en estado moderado, luego de ser aplicados los controles planteados (13 en total), los riesgos pasaron a la siguiente clasificación; (1) riesgo en estado menor, (3) riesgos en estado moderado y (1) continua en estado alto manteniendo su criticidad.

La siguiente imagen muestra el mapa de riesgos para el proceso:

RIESGOS	No. DEL RIESGO	ZONA RIESGO	CONTROLES EXISTENTES/MEDIDA DE MITIGACIÓN	ZONA RIESGO RESIDUAL	SOPORTE
Fallas en las aplicaciones o sistemas de información que apoyen los procesos de la Subred.	R1	RIESGO MODERADO	El profesional asignado elabora anualmente el plan y cronograma de mantenimientos para revisión y aprobación por parte del Jefe de la Oficina y su correspondiente ejecución por parte del personal técnico de forma semestral	RIESGO MODERADO	Plan y cronograma de mantenimiento
			El profesional responsable de la administración del Sistema de Información Servinte realiza el reporte en la mesa de servicios de Carvajal SAS sobre los problemas presentados en el normal funcionamiento de este.		Registro en mesa de ayuda Servis - Servinte
			El profesional realiza la verificación de la falla presentada tanto en software o hardware y a través del aplicativo de mesa de ayuda realiza el registro para la asignación al técnico del área el cual realiza la revisión y brinda la respectiva solución		Registro en mesa de ayuda
Uso inadecuado de los activos de información (tipo servicios, hardware, software, talento humano, información física y digital)	R2	RIESGO MODERADO	El profesional del área de sistemas diseña estrategias para incentivar el uso y la apropiación de las TICs de la Subred Norte ESE.	RIESGO MENOR	Estrategias diseñadas
			El área de comunicaciones realiza la publicación de las piezas comunicativas diseñadas junto con el área de sistemas relacionadas con el uso de los activos de información con que cuenta la Subred Norte ESE.		Piezas comunicativas Registro del despliegue
Daño en equipos informáticos (equipos de cómputo, servidores, equipos de comunicaciones, seguridad)	R3	RIESGO ALTO	El profesional universitario designa a personal técnico a realizar la verificación de que los equipos de cómputo, servidores, equipos de comunicaciones, seguridad se encuentren a la red regulada	RIESGO MODERADO	Inventario
			Profesional Universitario entrega el cronograma de mantenimiento preventivo de los equipos de cómputo al personal técnico de la Subred por sedes para su correspondiente ejecución y diligenciamiento de los formatos respectivos.		Cronograma de mantenimientos Formato elaboración mantenimientos
Fuga, alteración, divulgación o pérdida de la información generada por cada uno de los procesos.	R4	RIESGO ALTO	El profesional del área de sistemas realiza la actualización del documento AP-GI-PL-02-01-PLAN-DE-GESTIÓN-DE-SEGURIDAD-DE-LA-INFORMACIÓN y diseña las estrategias para su socialización	RIESGO ALTO	Documento Plan de Gestión de Seguridad de la Información
			El profesional del área de sistemas realiza la actualización del documento AP-GI-I-03-01-INSTRUCTIVO-GENERACIÓN-COPIAS-DE-SEGURIDAD-(BACKUPS)		Documento generación copias de seguridad
			El profesional del área de sistemas diseña estrategias relacionadas con seguridad y uso adecuado de la información de la Subred Norte ESE.		Estrategias diseñadas
Software obsoleto o no licenciado.	R5	RIESGO ALTO	El profesional universitario designa al personal técnico para la revisión del software instalado en los equipos y desinstalación de software no autorizado ni autorizado por la jefatura del área de sistemas	RIESGO MODERADO	Listado equipos con software no licenciado
			El profesional del área de sistemas realiza el inventario del software obsoleto y se remite relación a la jefatura de la oficina de sistemas		Inventario equipos con software obsoleto
			El profesional del área designa al personal técnico para la realización del inventario de software institucional.		Inventario de software

Imagen No. 4: Mapa de Riesgos de gestión publicado en la WEB de la entidad.

	INFORME FINAL		CÓDIGO: EV-EG-F-03-01
	AUDITORIAS DE CONTROL INTERNO		VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN		PÁGINA: 19 DE 70
			FECHA: 03/05/2021

7.3. Verificación de Controles de los riesgos

Teniendo en cuenta los riesgos que apuntan al proceso y que pudieran afectar o impactar las actividades y objetivos del proceso auditado, se verificó el diseño y ejecución de los controles que se tiene establecidos para la mitigación y detección de la materialización de dichos riesgos. Para esta verificación se tuvo en cuenta la Guía para la administración del riesgo y el diseño de controles en entidades públicas emitida por la DAFP versiones 4 y 5, donde se especifican los 6 pasos para un diseño adecuado de los controles y que se pueden detallar a continuación:

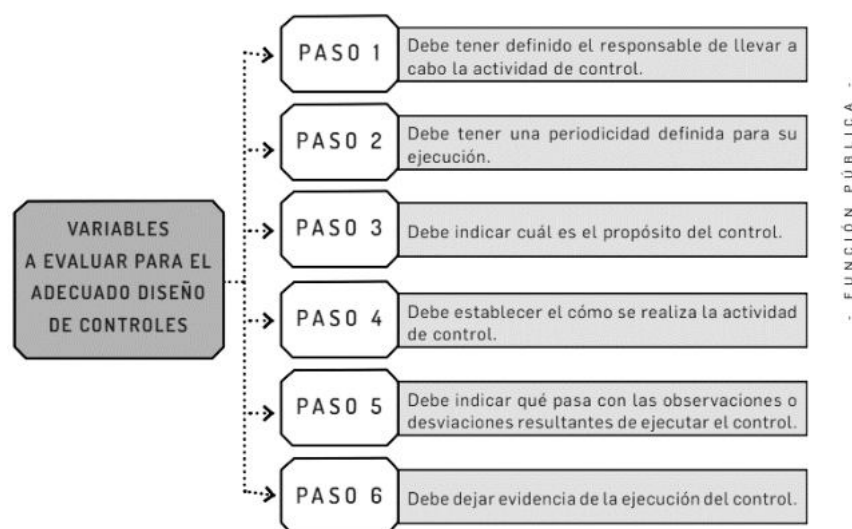


Imagen No. 5: Guía para la administración del riesgo y el diseño de controles en entidades públicas
Fuente: DAFP. Versión 4 de 2018

Luego de la verificación de los 13 controles establecidos para la mitigación de los riesgos del proceso, se identifica que en el diseño y redacción de los controles no cumplen completamente con todos los pasos recomendados por la Guía de la DAFP.

El anexo No.1 Resumen análisis de controles de los riesgos, del presente informe muestra el detalle de las observaciones sobre la evaluación de los riesgos del proceso, siendo evidente la ausencia de ejecución principalmente de la identificación específica del responsable del control pues está descrito globalmente, adicionalmente los pasos 3 y 5. deben revisarse, debido a que no se describe el propósito de algunos controles y adicionalmente no se explica qué se hace en las situaciones de desviación de las acciones del control.

Por otra parte, se verificó la valoración de los controles realizada por la oficina de desarrollo institucional al momento de la generación del mapa de riesgos de la entidad, identificándose

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO	CÓDIGO: EV-EG-F-03-01
		VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN	PÁGINA: 20 DE 70
		FECHA: 03/05/2021

la ejecución de los 6 pasos y la calificación de los controles de acuerdo con la guía de la función pública; sin embargo, esta oficina pudo constatar que los controles no son lo suficientemente fuertes para mitigar los riesgos motivando de esta manera el hallazgo No. 03.

Durante la revisión detallada de los controles se evidenciaron las siguientes situaciones:

1) Hojas de vida de equipos de computo

La oficina de control interno verificó que la manera como se almacenan y se mantienen las hojas de vida con las especificaciones técnicas, mantenimientos, responsables, registro de ubicación de los computadores de la subred, encontrando debilidades en cuanto a la organización, debido a la falta de expedientes individuales que mantengan la documentación suficiente de cada equipo; ya que las hojas de vida son guardadas en carpetas generales con todos los documentos de todos los equipos que se encuentran en cada una de las unidades de servicio, aumentando el riesgo de pérdida o archivado equivocado de los documentos. La siguiente imagen muestra donde se guardan estas carpetas.



Imagen No. 6: Medio de archivo de las hojas de vida de los equipos de computo

Adicionalmente se identificó que las carpetas y archivo no cumplen con lo establecido por las TRD de la Subred Norte e incumpliendo con lo establecido y reglamentado en el acuerdo 042 del archivo general de la nación, en lo relacionado con la información de expedientes y las TRD, situación que conlleva la formulación del hallazgo No. 04.

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO		CÓDIGO: EV-EG-F-03-01
			VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN		PÁGINA: 21 DE 70
			FECHA: 03/05/2021

2) Mantenimiento preventivo de equipos de computo

Se verificó que la programación del mantenimiento se inició con 2.159 equipos, no obstante a la fecha de esta auditoría el inventario reportado fue de 2.174. La siguiente tabla muestra el comportamiento de lo ejecutado versus lo programado.

Unidad de Servicio	#. Mantenimientos Proyectados		#. Mantenimientos Realizados						Total mantenimientos realizados hasta el mes según proyección	% de Cumplimiento vs. Proyectado	Total Mantenimientos Realizados en la Unidad hasta Julio	% de Avance en mantenimientos a Julio por unidad de servicio
	Mes Proyectado de Realización	TOTAL	feb	mar	abr	may	jun	jul				
CAPS CHAPINERO	Marzo	222	96	69	5	13	2	10	165	74%	195	88%
Salud Pública SUBA	Feb y Marzo	38	3	28			1	1	31	82%	33	87%
UMHES ENGATIVA	Abril y Mayo	399			46	137	183	5	183	46%	371	93%
CSE SUBA	Junio y Julio	333				1		83	84	25%	84	25%
CAPS Suba	Mayo	5							0	0%	0	0%
CAPS Prado Veraniego	Mayo	23							0	0%	0	0%
Gaitana	Junio	39							0	0%	0	0%
Rincon	Junio	17							0	0%	0	0%
Emaus	Mayo	38					37		0	0%	37	97%
Garces Nlvas	Junio	12					12		12	100%	12	100%
Ferías	Agosto	80			1		7	70	0	0%	78	98%
Bachue	Mayo	10					9	1	0	0%	10	100%
Quirigua	Mayo	9					9		0	0%	9	100%
Española	Mayo	10						10	0	0%	10	100%
Bellavista	Mayo	10					9		0	0%	9	90%
Boyaca Real	Mayo	18					18		0	0%	18	100%
Alamos	Mayo	8					8		0	0%	8	100%
FRAY	Nov - Dic	171					8	101	0	0%	109	64%
TOTALES		1191	99	97	52	151	303	281	475	40%	983	83%

Tabla No. 6: Prueba de recalcu de cumplimiento de mantenimiento de equipos de computo

Fuente: Oficina de Control Interno

Para el mes de julio se habían ejecutado 983 mantenimientos de los 1.191 programados, esto es un desfase de 208 equipos, es decir un 17% de atraso, también se observa que, en unidades como Ferías y Fray Bartolomé, se adelantó el mantenimiento sin que se ajustase el cronograma, ya sea por retrasos o anticipaciones, lo que dificulta la medición y el seguimiento de lo programado, situación que genera Incertidumbre por lo tanto riesgo de incumplimiento.

Por otra parte, solo se evidencia el plan de mantenimiento infraestructura de tecnología de la información código AP-GI-PI-13-01 pero no un cronograma de mantenimiento de servidores ni reporte de seguimiento, dicha situación supone un riesgo evidente dado la importancia de la ejecución de mantenimientos sobre uno de los activos de información más importantes de la Subred, lo que puede ocasionar perdida en la disponibilidad e integridad de la información. Dicha situación da lugar al hallazgo No. 05.

3) Mantenimiento correctivo de equipos de computo

Para programar el mantenimiento correctivo a los equipos de cómputo se tiene la herramienta de la mesa de ayuda de la oficina de sistemas de información y TICs. En esta herramienta se

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO	CÓDIGO: EV-EG-F-03-01
		VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN	PÁGINA: 22 DE 70
		FECHA: 03/05/2021

realiza la generación de los casos por parte de las áreas afectadas, la asignación de los técnicos o responsables de la solución y se registran las acciones y soluciones realizadas para cada uno de los casos generados.

A corte de junio de 2022 se tenía un total de 8.330 casos reportados en la herramienta, como se muestra en las siguientes tablas.

Unidad de Servicio Reportada	Promedio de	
	Numero de casos	Tiempo atencion
UMHES USS SUBA > SALUD Publica	105	12
USS CHAPINERO > USS Lorencita	26	10
USS CHAPINERO	1012	10
UMHES USS ENGATIVA > USS Ferias	198	9
UNIDAD NO REPORTADA	132	9
UMHES USS SUBA > CAPS Gaitana	134	8
USS CHAPINERO > USS San Luis	12	7
UMHES USS ENGATIVA > CAPS Emaus	94	6
USS USAQUEN > USS Santa Cecilia	58	6
UMHES USS SUBA	1649	5
UMHES USS SIMON > Servitá	30	5
UMHES USS ENGATIVA > USS Bachue	49	5
UMHES USS ENGATIVA > USS Quirigua	22	5
USS USAQUEN > USS Usaquén	154	4
UMHES USS ENGATIVA > USS Española	30	4
UMHES USS SUBA > CAPS Suba	44	4
USS USAQUEN > CAPS San Cristóbal	86	4
UMHES USS ENGATIVA > USS Alamos	21	4
USS USAQUEN > USS Orquideas	49	4
USS USAQUEN > USS Buenavista	10	4
UMHES USS SUBA > USS Rincón	52	4
UMHES USS SUBA > USS Prado Veraniego	62	3
USS CHAPINERO > Rionegro	161	3
UMHES USS ENGATIVA > USS Bellavista	27	3
UMHES USS SIMON > UMHES USS Fray	709	3
USS USAQUEN > SEDE Administrativa	5	2
UMHES USS ENGATIVA > USS Garcés Navas	38	2
UMHES USS SIMON	1414	2
USS USAQUEN > USS Codito	27	2
UMHES USS ENGATIVA	1873	2
UMHES USS ENGATIVA > USS Boyaca Real	45	2
USS CHAPINERO > Juan XXIII	2	0
Total general	8330	4

Tabla No. 7: Promedio de atención por unidad de servicio
Fuente: Oficina de Sistemas de Información

Se puede evidenciar que, en unidades como Chapinero, Salud Publica Suba, USS ferias y USS Lorencita el tiempo promedio de atención es de 10 o más días. En 21 de los 32 puntos que reportaron casos, los tiempos de atención en promedio superaron los 3 días que corresponde al ANS establecido para los requerimientos de más baja prioridad según el instructivo de acuerdo de niveles de servicio AP-GI-I-19-01 en su numeral 5.4.3.2. Los puntos donde se presentó el mejor tiempo atención promedio fueron: UMHES Simón Bolívar, Engativá, Usaquén, Garcés Navas, Codito, Boyacá Real y Juan XXIII, con menos de 3 días.

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO		CÓDIGO: EV-EG-F-03-01
			VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN		PÁGINA: 23 DE 70
			FECHA: 03/05/2021

Categoría del requerimiento	Numero de casos	Promedio de Tiempo atención
SISTEMAS > Impresoras	440	7
SISTEMAS > Solicitudes de Información > Salud pública	4	6
SISTEMAS	12	6
SISTEMAS > Equipos de cómputo	4474	6
SISTEMAS > Solicitudes de Información > Investigación.	1	5
SISTEMAS > Solicitudes de Información > Direccionamiento y planeación de la organización	2	4
SISTEMAS > Solicitudes de Información > Asignación de recursos.	38	4
SISTEMAS > Solicitudes de Información > Promoción y prevención.	1	3
SISTEMAS > Aplicativos institucionales	1208	3
SISTEMAS > Solicitudes de Información > Docencia-servicio.	3	3
SISTEMAS > Servinte (HIS)	1535	2
SISTEMAS > Solicitudes de Información > Mejoramiento de la calidad	4	2
SISTEMAS > Red Voz – Datos	598	1
SISTEMAS > Solicitudes de Información > Del paciente y su familia durante su atención.	10	1
Total general	8330	4

Tabla No. 8: Promedio de atención por categoría de requerimiento
Fuente: Oficina de Sistemas de Información

Como se muestra en la tabla, los servicios que más tiempo consumen para la realización de las actividades son los requerimientos por Impresoras, Solicitudes de Información de Salud pública y Equipos de Cómputo, mientras que las solicitudes que se atienden más rápidamente son las relacionadas con Red Voz - Datos y las de solicitudes de información del paciente y su familia durante la atención. Cabe anotar que esta es la categorización de los casos que entran por la mesa de servicio y que son registrados en el módulo de sistemas.

Adicionalmente se evidencia que hay casos que según el instructivo de acuerdo de niveles de servicio AP-GI-I-19-01 están por encima de lo establecido con el numeral 5.4.3.2.

En la siguiente tabla se muestra que en el 19.4 % de los casos reportados, se les dio solución por fuera de los tiempos, incumpliendo así el Acuerdo de Nivel de Servicio (ANS). Motivo por el cual se genera el hallazgo No. 06.

Tiempo de días de respuesta	No. de casos	% Participación
<= 3	6714	80,61%
4-30	1376	16,52%
31-60	79	0,95%
61-100	21	0,25%
> 100	139	1,67%
Total	8329	100,00%

Tabla No. 9: Tiempos de atención de casos reportados a mesa de servicios
Fuente: Oficina de Sistemas de Información

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO	CÓDIGO: EV-EG-F-03-01
		VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN	PÁGINA: 24 DE 70
		FECHA: 03/05/2021

Cabe mencionar también que del 19.4%, el 1.67% corresponden a 139 requerimientos que se solucionaron después de 100 días. Al solicitar información sobre los casos, la oficina de sistemas confirmó que correspondían a actualización del sistema operativo y la demora fue debido a problemas logísticos y fue imposible realizar la actividad programada en menos tiempo.

7.4. Riesgos relacionados con la seguridad y privacidad de la Información - Evaluación de la Política de Seguridad Digital

Para la evaluación de esta política se tuvieron en cuenta dos herramientas:

1. Revisión del auto diagnóstico de seguridad de la información: De acuerdo con este instrumento, se revisó la información correspondiente a políticas, planes, procedimientos e instrumentos relacionados con seguridad de la información y de acuerdo con el anexo A de la ISO 27001.

En el siguiente cuadro se muestra el listado de los documentos solicitados y la evaluación de cumplimiento de dichos documentos.

ID	SOLICITUD DE INFORMACIÓN	DOCUMENTOS ENTREGADOS	OBSERVACIONES OCI
1	Documento de análisis de contexto: aspectos externos e internos que son necesarios para cumplir su propósito y que afectan su capacidad para lograr los resultados previstos en el MSPI.	Inexistente	No se evidencia
2	Mapa de Procesos	Manual de Procesos y Procedimientos - ES-GC-M-01-02 de 31 de mayo de 2017	Documento desactualizado y/o en proceso de actualización
3	Organigrama de la entidad, detallando el área de seguridad de la información o quien haga sus veces	Acuerdo 008 de 5 de abril de 2017 - Por el cual se establece la estructura organizacional de la Subred Integrada de Servicios de Salud Norte ESE.	No se cuenta con organigrama de seguridad ni roles ni responsabilidades
4	Políticas de seguridad de la información formalizada y firmada	P-GI-M-02-02-Manual de políticas de seguridad y privacidad de la información	En el manual de seguridad no se evidencia el acto administrativo de aprobación
5	Organigrama, roles y responsabilidades de seguridad de la información, asignación del recurso humano y comunicación de roles y responsabilidades.	Documento AP-GI-PL-02-03-Plan de seguridad y privacidad de la información	No se cuenta con organigrama de seguridad ni roles y responsabilidades.

	INFORME FINAL		CÓDIGO: EV-EG-F-03-01
	AUDITORIAS DE CONTROL INTERNO		VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN		PÁGINA: 25 DE 70
			FECHA: 03/05/2021

ID	SOLICITUD DE INFORMACIÓN	DOCUMENTOS ENTREGADOS	OBSERVACIONES OCI
6	Documento con el resultado de la autoevaluación realizada a la Entidad, de la gestión de la seguridad y privacidad de la información e infraestructura de red de comunicaciones (IPv4/IPv6), revisado y aprobado por la alta dirección	Inexistente	No se evidencia
7	Documento con el resultado de la herramienta de la encuesta de diagnóstico de seguridad y privacidad de la información, revisado, aprobado y aceptado por la alta dirección	Instrumento de evaluación MSPI	Documento vigente
8	Documento con el resultado de la estratificación de la entidad, aceptado y aprobado por la alta dirección	Inexistente	No se evidencia
9	Objetivo, alcance y límites del MSPI (Modelo de Seguridad y Privacidad de la Información)	AP-GI-PL-02-03-Plan de seguridad y privacidad de la información	Documento vigente
10	Procedimientos de control documental del MSPI	AP-GI-I-02-02-INSTRUCTIVO ADMINISTRACIÓN DE CUENTAS DE USUARIO AP-GI-PL-12-02-Contingencia de los sistemas de información AP-GI-PL-03-02-PLAN DE TRATAMIENTO DEL RIESGO DE LA INFORMACIÓN AP-GI-I-03-01-INSTRUCTIVO GENERACIÓN COPIAS DE SEGURIDAD (BACKUPS) AP-GI-I-04-01-INSTRUCTIVO USO RECURSOS TECNOLÓGICOS AP-GI-PL-09-01-PLAN DE COMUNICACIÓN Y DIVULGACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN AP-GI-I-16-01-Gestión de Incidentes de Seguridad de la Información AP-GI-I-17-01-Identificación de Infraestructura Crítica Cibernética	* AP-GI-I-02-02-INSTRUCTIVO ADMINISTRACIÓN DE CUENTAS DE USUARIO: Desactualizado, no contempla todos los servicios y/o aplicaciones, no se cumplen los controles. * AP-GI-PL-12-02-Contingencia de los sistemas de información: No se cuenta con la aprobación ni con pruebas. * AP-GI-PL-03-02-PLAN DE TRATAMIENTO DEL RIESGO DE LA INFORMACIÓN: Desactualizado, no se da cumplimiento y no acorde con la metodología * AP-GI-I-03-01-INSTRUCTIVO GENERACIÓN COPIAS DE SEGURIDAD (BACKUPS): desactualizado y no se da cumplimiento *AP-GI-I-04-01-INSTRUCTIVO USO RECURSOS TECNOLÓGICOS:

	INFORME FINAL		CÓDIGO: EV-EG-F-03-01
	AUDITORIAS DE CONTROL INTERNO		VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN		PÁGINA: 26 DE 70
			FECHA: 03/05/2021

ID	SOLICITUD DE INFORMACIÓN	DOCUMENTOS ENTREGADOS	OBSERVACIONES OCI
		AP-GI-M-02-02-Manual de políticas de seguridad y privacidad de la información. Otros documentos: Listados de cuentas inactivas de red y aplicaciones Acto de aprobación y actas de pruebas del plan de contingencia. Registro de copias de seguridad y de restauración. Listado de incidentes de seguridad e informe final del tratamiento.	Desactualizado, no se da cumplimiento *AP-GI-PL-09-01-PLAN DE COMUNICACIÓN Y DIVULGACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN: Tiene características de manual, no contempla un plan.
11	Metodología de Gestión de riesgos	ES-GC-M-01-02-MANUAL DE PROCESOS Y PROCEDIMIENTOS ES-GE-M-02-01-MANUAL DE GESTIÓN Y ADMINISTRACIÓN DEL RIESGO	Inexistente para riesgos de seguridad de la información
12	Riesgos identificados y valorados de acuerdo a la metodología	ES-GE-F-09-03-Mapa de Riesgos Institucional 2020 ES-GE-M-02-02-Gestión y administración del riesgo	Documento desactualizado, no da cumplimiento ni acorde con la metodología.
13	Planes de tratamiento de los riesgos	AP-GI-PL-03-02-Tratamiento del riesgo de la información	Documento desactualizado, no da cumplimiento ni acorde con la metodología.
14	Formatos de acuerdos contractuales con empleados y contratistas para establecer responsabilidades de las partes en seguridad de la información	Contrato OPS contiene cláusula de confidencialidad	Documento vigente
15	Procedimiento de verificación de antecedentes para candidatos a un empleo en la entidad	TH-P-01-01-PROCEDIMIENTO IDENTIFICACION SELECCION Y RECLUTAMIENTO DEL TALENTO HUMANO AP-TH-I-13-01-INSTRUCTIVO VERIFICACIÓN DE LA INFORMACIÓN DE LA HOJA DE VIDA	Documento vigente
16	Documento con el plan de comunicación, sensibilización y capacitación en seguridad de la información, revisado y aprobado por la alta Dirección, con sus respectivos soportes.	AP-GI-PL-09-01-PLAN DE COMUNICACIÓN Y DIVULGACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	El documento presentado no es un plan, las características son de un manual

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO		CÓDIGO: EV-EG-F-03-01
			VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN		PÁGINA: 27 DE 70
			FECHA: 03/05/2021

ID	SOLICITUD DE INFORMACIÓN	DOCUMENTOS ENTREGADOS	OBSERVACIONES OCI
17	Documento que haga claridad sobre el proceso disciplinario en caso de incumplimiento de las políticas de seguridad de la información	Inexistente	No se evidencia
18	Inventario de activos de información clasificados, de la entidad, revisado y aprobado por la alta dirección	AP-GI-F-25-02-CUADRO DE CARACTERIZACIÓN DOCUMENTAL-REGISTRO DE ACTIVOS INFORMACIÓN	El formato de caracterización está incompleto y no cumple con los requerimientos mínimos de la Guía para la Gestión y Clasificación de Activos de Información de MINTIC
19	Inventario de áreas de procesamiento de información y telecomunicaciones	Inexistente	No se cuenta con el inventario
20	Diagrama de red de alto nivel o arquitectura de TI	Inexistente	No se evidencia
21	Inclusión de la seguridad de la información en la gestión de proyectos	Inexistente	No se evidencia
22	Inventario de partes externas o terceros a los que se transfiere información de la entidad	Inexistente	No se evidencia
23	Formato de acuerdo de transferencia de información	Inexistente	No se evidencia
24	Inventario de proveedores que tengan acceso a los activos de información, indicando el servicio que prestan o bienes que venden	Inexistente	No se evidencia
25	Reporte de eventos e incidentes de seguridad de la información de los últimos 12 meses.	Inexistente	No se evidencia
26	Plan de continuidad de la Entidad aprobado	AP-GI-PL-04-01-PLAN DE CONTINUIDAD DEL NEGOCIO	Documento presentado no cumple con las características del plan de continuidad
27	Inventario de obligaciones legales, estatutarias, reglamentarias, normativas relacionadas con seguridad de la información	Inexistente	No se evidencia
28	Listado de auditorías relacionadas con seguridad de la información realizadas en la entidad	Inexistente	No se evidencia
29	Procedimientos, manuales, guías, directrices, lineamientos, estándares, instructivos relacionados con seguridad de la información, el modelo de	Los entregados en el numeral 12	La mayoría de los documentos suministrados se encuentran desactualizados y/o no se da cumplimiento.

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO	CÓDIGO: EV-EG-F-03-01
		VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN	PÁGINA: 28 DE 70
		FECHA: 03/05/2021

ID	SOLICITUD DE INFORMACIÓN	DOCUMENTOS ENTREGADOS	OBSERVACIONES OCI
	seguridad y privacidad de la información de Min Tic.		
30	Indicadores y métricas de seguridad de la información definidos.	Inexistente	No se evidencia
31	Declaración de aplicabilidad	Documento preliminar de declaración y aplicabilidad controles	cumple parcial
32	Aceptación de los riesgos residuales por parte de los dueños de los riesgos	Inexistente	No se evidencia
33	Avance en la ejecución del plan de tratamiento de riesgos de seguridad	Inexistente	No se evidencia
34	Documento con el consolidado de las auditorías realizadas de acuerdo con el plan de auditorías, revisado y aprobado por la alta dirección y verifique como se asegura que los hallazgos, brechas, debilidades y oportunidades de mejora se subsanen, para asegurar la mejora continua.	Inexistente	No se evidencia

Tabla No. 10: Evaluación de cumplimiento sobre la documentación relacionada

Se puede observar que falta documentar gran parte de los instrumentos que darían soporte al MSPI, y adicionalmente buena parte la documentación existente se encuentra Desactualizada o no da cuenta de la realidad, por lo que se reitera el hallazgo No. 01.

EVALUACIÓN DE EFECTIVIDAD DE CONTROLES - ISO 27001:2013 ANEXO A

Teniendo en cuenta los criterios de valoración de controles descritos en la siguiente tabla y la verificación de la documentación y el uso de la herramienta de **identificación de la línea base de seguridad** de MINTIC.

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO	CÓDIGO: EV-EG-F-03-01
		VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN	PÁGINA: 29 DE 70
		FECHA: 03/05/2021

ATRIBUTO	CRITERIO
Inexistente	Falta de cualquier proceso reconocible. La Organización ni siquiera ha reconocido que hay un problema a tratar. No se aplican controles.
Inicial	Hay una evidencia de que la Organización ha reconocido que existe un problema y que hay que tratarlo. No hay procesos estandarizados. La implementación de un control depende de cada individuo y es principalmente reactiva, y se cuenta con procedimientos documentados pero no son conocidos y/o no se aplican y/o están obsoletos.
Repetible	Los procesos y los controles siguen un patrón regular. Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. No hay formación ni comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores.
Efectivo	Los procesos y los controles se documentan y se comunican. Los controles son efectivos y se aplican casi siempre. Sin embargo, es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo no es la indicada.
Gestionado	Los controles se monitorean y se miden. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente.
Optimizado	Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores prácticas, basándose en los resultados de una mejora continua.

Tabla No. 11: Escala de Valoración de Controles ISO 27001:2013 ANEXO A

Se determinaron los siguientes resultados:

- Detalle de evaluación de controles: El anexo No. 2 del presente informe muestra el detalle de la evaluación de cada uno de los controles del estándar.
- Resumen de evaluación de controles: a continuación se muestra de manera resumida el resultado de la evaluación de los controles del estándar

No.	DOMINIO	Calf. Actual	Calf. Objetivo	Eval efectividad de control
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	30	100	REPETIBLE
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	16	100	INICIAL
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	9	100	INICIAL

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO	CÓDIGO: EV-EG-F-03-01
		VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN	PÁGINA: 30 DE 70
		FECHA: 03/05/2021

No.	DOMINIO	Calf. Actual	Calf. Objetivo	Eval efectividad de control
A.8	GESTIÓN DE ACTIVOS	23	100	REPETIBLE
A.9	CONTROL DE ACCESO	14	100	INICIAL
A.10	CRIPTOGRAFÍA	0	100	INEXISTENTE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	25	100	REPETIBLE
A.12	SEGURIDAD DE LAS OPERACIONES	16	100	INICIAL
A.13	SEGURIDAD DE LAS COMUNICACIONES	20	100	INICIAL
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	1	100	INEXISTENTE
A.15	RELACIONES CON LOS PROVEEDORES	10	100	INICIAL
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	3	100	INICIAL
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	7	100	INICIAL
A.18	CUMPLIMIENTO	19	100	INICIAL
PROMEDIO EVALUACIÓN DE CONTROLES		16	100	INICIAL

Tabla No. 12: Resultado evaluación efectividad de controles Anexo A ISO 27001:2013



Gráfico No. 1: Brecha evaluación de controles Anexo A ISO 27001:2013

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO	CÓDIGO: EV-EG-F-03-01
		VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN	PÁGINA: 31 DE 70
		FECHA: 03/05/2021

Teniendo en cuenta la tabla de evaluación de efectividad de los controles y de acuerdo con el estándar ISO 27001, se puede evidenciar que la Subred Norte se encuentra en un estado INICIAL y como muestra la siguiente tabla, dicho estado hace referencia principalmente a que **no hay procesos estandarizados**, que los procedimientos están documentados **pero no se aplican y/o están obsoletos**. No obstante, se ha logrado avanzar en ciertos grupos de controles que se encuentran en estado REPETIBLE, lo cual indica que existen controles y procedimientos, pero estos no han sido comunicados y la seguridad se basa en los conocimientos y experticia de quienes ejecutan los controles.

La siguiente tabla y gráfico muestran el avance del Sistema de Gestión de Seguridad y Privacidad de la Información con relación al ciclo PHVA. Se puede evidenciar un avance total del 18%, lo que es consecuente con el avance de implementación de controles.

COMPONENTE	% Avance	% Esperado
Planificación	15%	40%
Implementación	3%	20%
Evaluación de desempeño	0%	20%
Mejora continua	0%	20%
Total	18%	100%

Tabla No. 13: Avance ciclo de funcionamiento del modelo de operación (PHVA)

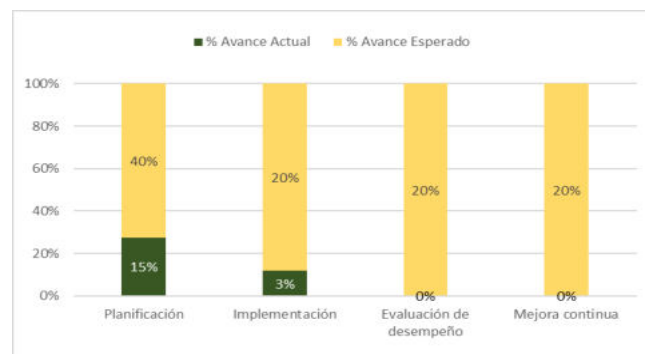


Gráfico No. 2: Avance ciclo de funcionamiento del modelo de operación (PHVA)

De acuerdo con el instrumento de evaluación del MSPI del ministerio de TICS, se puede evidenciar que la Subred Norte se encuentra en un nivel de madurez **Inicial**, tal como lo muestra el siguiente cuadro

Inicial: En este nivel se encuentran las entidades que aún no cuentan con una identificación clara de activos ni gestión de riesgos de seguridad y privacidad de la información, que permita determinar el grado de criticidad de información respecto a la seguridad y privacidad de la misma. Por lo tanto, los controles no están alineados con la preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información.

Repetible: En este nivel se encuentran las entidades en las cuales existen procesos básicos de gestión de seguridad y privacidad de la información. De igual forma existen controles que permiten detectar posibles incidentes de seguridad, pero no se encuentran gestionados dentro del componente planificación del MSPI.

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO	CÓDIGO: EV-EG-F-03-01
		VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN	PÁGINA: 32 DE 70
		FECHA: 03/05/2021

Definido: En este nivel se encuentran las entidades que tienen documentado, estandarizado y aprobado por la alta dirección, el modelo de seguridad y privacidad de la información. Todos los controles se encuentran debidamente documentados, aprobados, implementados, probados y actualizados.

Administrado: En este nivel se encuentran las entidades que cuentan con métricas, indicadores y realizan auditorías al MSPI, recolectando información para establecer la efectividad de los controles.

Optimizado: En este nivel se encuentran las entidades en donde existe un mejoramiento continuo del MSPI, retroalimentando cualitativamente el modelo.

Tabla No. 14: Niveles de madurez Instrumento de evaluación MSPI MINTIC

- Revisión del resultado de la Medición del Desempeño Institucional 2021 de la política 07 Seguridad Digital: para la ejecución de esta actividad, además de la información solicitada en el punto 1, también se revisó el cuestionario del Formulario Único de Reporte de Avance de la Gestión - FURAG y el resultado de publicado en la página de la función pública.



Al comparar los resultados de las evaluaciones del FURAG (80.4) y la de controles del MSPI (16), se puede concluir que los patrones de medición no son equiparables, no obstante la documentación soporte del MSPI aplica completamente para la política de seguridad digital.

Teniendo en cuenta esta premisa, se revisaron los soportes de las respuestas consignadas en el FURAG a la luz de los soportes de los controles de la ISO 27001:2013 anexo A. En dicha comparación se logró determinar que controles o parte de estos se tuvieron en cuenta en la encuesta de la política de seguridad digital FURAG 2021.

Imagen No. 7: Resultado FURAG
Política Seguridad Digital - 2021

GRUPO DE CONTROLES	EVALUACIÓN	PREGUNTA FURAG
CUMPLIMIENTO	Parcial	SDI14
GESTIÓN DE ACTIVOS	Parcial	SDI16
GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	Parcial	SDI15

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO	CÓDIGO: EV-EG-F-03-01
		VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN	PÁGINA: 33 DE 70
		FECHA: 03/05/2021

GRUPO DE CONTROLES	EVALUACIÓN	PREGUNTA FURAG
GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	Parcial	SDI17, SDI18
ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	Parcial	SDI01, SDI05, SDI07, SDI08, SDI10, SDI11, SDI19
POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	Parcial	SDI09
RELACIONES CON LOS PROVEEDORES	Parcial	SDI20
SEGURIDAD DE LAS OPERACIONES	Parcial	SDI21, SDI23
SEGURIDAD DE LOS RECURSOS HUMANOS	Parcial	SDI12, SDI13, SDI22
SEGURIDAD FÍSICA Y DEL ENTORNO	Parcial	SDI06

Tabla No. 15: Comparativo controles Anexo A ISO 27001 VS Política de Seguridad Digital FURAG 2021

En la anterior tabla se muestra la relación entre el grupo de controles y las preguntas del FURAG, se puede observar que las preguntas dan un cumplimiento parcial sobre cada control, esto nos permite concluir que la rigurosidad y el alcance de los controles ISO es mucho más amplio, lo que explica en parte la diferencia de los puntajes obtenidos entre el auto diagnóstico y el resultado FURAG.

No obstante, al comparar las respuestas del FURAG versus la documentación del autodiagnóstico, esta oficina logro determinar la presencia de respuestas que no cuentan con bases documentales y/o procedimentales que las soporte. A continuación, se muestra los resultados de la prueba.

GRUPO	CUMPLIMIENTO
PREGUNTA	¿La alta dirección de la entidad realiza la revisión del Sistema de Gestión de Seguridad de la Información (SGSI)?
RESPUESTA	Se realizan revisiones esporádicamente
OBSERVACIÓN OCI	La subred no tiene definido un SGSI, por lo tanto no puede hacer revisiones a dicho sistema. La anterior situación genera una sobre calificación y por supuesto una falsa expectativa sobre el estado de la seguridad de la

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO	CÓDIGO: EV-EG-F-03-01
		VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN	PÁGINA: 34 DE 70
		FECHA: 03/05/2021

	información en la Subred, adicionalmente existe la posibilidad de riesgo legal dado que se emite una respuesta positiva sin contar con los soportes de la misma, situación que genera el hallazgo No. 07.
--	---

GRUPO	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN
PREGUNTA	¿La entidad ha establecido un procedimiento de gestión de incidentes de seguridad de la información?
RESPUESTA	Se ha establecido un procedimiento y está formalizado, pero no se ha implementado
OBSERVACIÓN OCI	No se evidencia procedimiento de gestión de incidentes de seguridad, se desconoce el tratamiento de los mismos. Durante la ejecución de esta auditoría se presentaron dos incidentes de seguridad considerables (caída del servidor de ORFEO y vencimiento de antivirus) sobre los cuales no se evidenció planes de continuidad o contingencia, ni controles de mitigación del riesgo. Hallazgo No. 08: se materializó el riesgo de daño en la base de datos de Orfeo con pérdida en la disponibilidad de la información por fallas en el hardware y en los controles de Backup, sin que mediara un procedimiento documentado sobre la gestión del incidente. Por otra parte se presenta el hallazgo No. 09, dado que los equipos de cómputo y servidores quedaron vulnerables y expuestos a ataques informáticos y pérdida total y/o parcial de la información causada por malware, debido al vencimiento del sistema antivirus.

GRUPO	GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO
PREGUNTA	¿La entidad efectúa ejercicios de simulación y respuesta a ataques cibernéticos?
RESPUESTA	Si, y cuenta con las evidencias
OBSERVACIÓN OCI	Esta oficina no encontró evidencias de simulacros ni respuestas a ataques cibernéticos, por lo tanto la respuesta dada no refleja la realidad de la situación de la Subred.

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO	CÓDIGO: EV-EG-F-03-01
		VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN	PÁGINA: 35 DE 70 FECHA: 03/05/2021

	Frente a la gestión de continuidad del negocio, en los casos anteriores no se evidenció la puesta en marcha de un plan de contingencia ni la comunicación sobre las situaciones presentadas, donde se informe sobre las actividades y el tiempo estimado de recuperación de los servicios RTO (Recovery Time Objective), ni el tiempo estimado de recuperación de la data RPO (Recovery Point Objective). La anterior situación genera dos hallazgos: se reitera el hallazgo No. 07 y se genera el hallazgo No. 10: como una posible pérdida de la disponibilidad de los servicios informáticos al no contar con un plan de continuidad del negocio con ejercicios y simulacros.
PREGUNTA	¿La entidad efectúa evaluaciones de vulnerabilidades informáticas?
RESPUESTA	Si, y cuenta con las evidencias
OBSERVACIÓN OCI	No se evidencia evaluación de vulnerabilidades sobre los activos de información. Tampoco se evidencia el plan de tratamiento de riesgos de seguridad. La evaluación de las vulnerabilidades frente a las amenazas, son las que permiten definir el riesgo de un activo de información. La subred no tiene un inventario de activos de información actualizado (solo cuenta con inventario documental). Hallazgo No. 11: La falta de un inventario de activos de información y la evaluación de vulnerabilidades sobre los activos, genera un posible riesgo de falla en la caracterización de los riesgos de seguridad y privacidad de la información.

GRUPO	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
PREGUNTA	¿La entidad ha establecido roles y responsabilidades específicos respecto a la seguridad de la información?

	INFORME FINAL		CÓDIGO: EV-EG-F-03-01
	AUDITORIAS DE CONTROL INTERNO		VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN		PÁGINA: 36 DE 70
			FECHA: 03/05/2021

RESPUESTA	Los ha establecido, incluyendo el rol de responsable de seguridad de la información de la entidad, estos roles están aprobados y satisfacen las necesidades de la entidad
OBSERVACIÓN OCI	No se evidencia la definición de roles ni responsables de seguridad de la información. Adicionalmente se controvierte en las preguntas SDI11 y SDI19, ya que se afirma que la alta dirección no destina recursos para la seguridad de la información ni se caracterizan los riesgos de seguridad. Se reitera el hallazgo No. 07.

GRUPO	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN
PREGUNTA	Con respecto a los objetivos específicos de seguridad de la información, la entidad:
RESPUESTA	Los ha establecido, han sido aprobados por la alta dirección y se han definido indicadores para medir su nivel de cumplimiento, pero no se cuenta con resultados históricos
OBSERVACIÓN OCI	Se evidencia un documento preliminar de manual de políticas de seguridad de la información, no obstante dicho documento no muestra definición de roles y responsabilidades, no se evidencia métrica ni instrumentos de medición de cumplimiento. No se evidencia revisión y aprobación por la alta Dirección. Se reitera el hallazgo No. 07

GRUPO	SEGURIDAD DE LAS OPERACIONES
PREGUNTA	Con respecto a la gestión de las vulnerabilidades de los sistemas de información de la entidad:
RESPUESTA	La entidad identifica periódicamente vulnerabilidades técnicas, pero no cuenta con procedimientos formales para la actualización y la colocación de parches en los sistemas de información
OBSERVACIÓN OCI	No se evidencia procedimientos ni informes de identificación de vulnerabilidades a los sistemas de información de la subred. No existe

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO	CÓDIGO: EV-EG-F-03-01
		VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN	PÁGINA: 37 DE 70
		FECHA: 03/05/2021

caracterización de riesgos de seguridad y privacidad de la subred, por lo que se reitera el hallazgo No. 11.

Adicionalmente, al revisar la seguridad lógica del acceso al sistema Servinte, se encontró que 171 funcionarios que se retiraron de la Subred, continúan con acceso vigente a dicho sistema, como muestra la siguiente tabla.

TOTAL PERSONAS RETIRADAS	1262
TOTAL PERSONAS CON CLAVE AUN ACTIVA	171
Clave Servinte	Vigente ☒
Etiquetas de fila	☒ Cuenta
DIRECCIÓN DE GESTIÓN DEL RIESGO EN SALUD	63
DIRECCIÓN DE SERVICIOS HOSPITALARIOS	50
DIRECCIÓN DE SERVICIOS DE URGENCIAS	24
DIRECCIÓN DE SERVICIOS COMPLEMENTARIOS	19
DIRECCIÓN FINANCIERA	9
DIRECCIÓN DE SERVICIOS AMBULATORIOS	3
DIRECCIÓN ADMINISTRATIVA	1
OFICINA DE PARTICIPACIÓN COMUNITARIA Y SERVICIO AL CIUDADANO	1
DIRECCIÓN DE GESTIÓN DE TALENTO HUMANO	1
Total general	171

Tabla No. 16: Accesos vigentes de personal retirado

En este mismo sentido, se evidenció que 116 de los 3962 usuarios activos, presentan errores en el número de documento o dicho dato se encuentra vacío, por ejemplo (12345,99999,1, 2, 44444, etc.).

Finalmente al revisar los roles de usuarios se encontró que existen 7 usuarios administradores y que dos de éstos corresponden a funcionarios que ya no laboran para la Subred.

idecod	idenom	ideap1	ideap2	idel	ideide	ideeadg	ideeade	grunom
ADMINISTRADOR	[REDACTED]			CC	99999999	9999	N	ADMINISTRADORES
ADMINISTRADOR	[REDACTED]			CC	999999	9999	N	ADMINISTRADORES
ADMINISTRADOR	[REDACTED]			CC	99999999	9999	N	ADMINISTRADORES
ADMINISTRADOR	[REDACTED]			CC	99999999	9999	N	ADMINISTRADORES
ADMINISTRADOR	[REDACTED]			CC	999999	9999	N	ADMINISTRADORES
ADMINISTRADOR	[REDACTED]			CC	99999999	9999	N	ADMINISTRADORES
ADMINISTRADOR	[REDACTED]			CC	99999999	9999	N	ADMINISTRADORES

Tabla 17: Accesos vigentes de administradores

	INFORME FINAL		CÓDIGO: EV-EG-F-03-01
	AUDITORIAS DE CONTROL INTERNO		VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN		PÁGINA: 38 DE 70
			FECHA: 03/05/2021

	La anterior circunstancia evidencia una grave falla en el control de acceso a los sistemas, servicios y aplicaciones, toda vez que: (1) no se retiran o deshabilitan de manera inmediata las identificaciones de los usuarios que han dejado la organización, (2) no se identifican, eliminan o deshabilitan periódicamente las identificaciones de usuario redundantes. Por lo que se genera el hallazgo No. 12 Se reitera el hallazgo No. 07
PREGUNTA	Con respecto a las copias de respaldo de información de la entidad:
RESPUESTA	La entidad realiza copias de respaldo con una periodicidad definida con los usuarios de la información y realiza pruebas de restauración de las copias para garantizar su correcto funcionamiento en caso de que sean requeridas
OBSERVACIÓN OCI	El procedimiento e instructivo de copias de seguridad está desactualizado, no se hacen pruebas a las copias de respaldo ni se tiene definido un esquema de copias de seguridad. Las copias de la base de datos del sistema SERVINTE se realizan de manera semanal con igual tiempo de retención. De acuerdo con informe presentado por el responsable de dicho activo, se evidenció que la última prueba de restore fue realizada fue el 24 de agosto del 2021. Hallazgo No. 13: no contar con procedimientos actualizados ni esquemas de Backup sobre activos de información altamente críticos como son las bases de datos de sistemas en producción, la Subred corre con un alto riesgo de experimentar un desastre informático de consecuencias catastróficas. Se reitera el hallazgo No. 07

GRUPO	SEGURIDAD DE LOS RECURSOS HUMANOS
PREGUNTA	¿La entidad ha realizado campañas de concientización en temas de seguridad de la información?

	INFORME FINAL		CÓDIGO: EV-EG-F-03-01
	AUDITORIAS DE CONTROL INTERNO		VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN		PÁGINA: 39 DE 70
			FECHA: 03/05/2021

RESPUESTA	Se realizan campañas de seguridad específicas para los diferentes roles dentro de la entidad, y se actualizan mediante un proceso de mejora continua
OBSERVACIÓN OCI	Se evidencia el envío esporádico de piezas comunicativas con temas relacionados sobre seguridad de la información.
PREGUNTA	Con respecto a la toma de conciencia sobre seguridad de información en la entidad:
RESPUESTA	La entidad realiza ocasionalmente ejercicios simulados de ingeniería social al personal de la entidad incluyendo campañas de phishing y smishing, analiza los resultados obtenidos, pero no realiza retroalimentación al personal para generar conciencia sobre la seguridad de la información
OBSERVACIÓN OCI	Se evidencian ocasionalmente piezas comunicativas sobre seguridad de la información, sin embargo, estas no obedecen a un plan de concienciación ni se informan los resultados sobre la comunicación de dichos elementos. Hallazgo No. 14: No se evidencia un plan de concienciación enmarcado dentro de un proceso de mejora continua del SGSI, de tal manera que dé cuenta del avance efectivo de la toma de conciencia sobre seguridad. La anterior situación genera desgaste y reproceso con poca reciprocidad en los resultados. Se reitera el hallazgo No. 07

GRUPO	SEGURIDAD FÍSICA Y DEL ENTORNO
PREGUNTA	¿La entidad ha identificado factores externos e internos (contexto) que puedan afectar la seguridad de su información?
RESPUESTA	Ha identificado los factores, pero no han sido aprobados por la alta dirección
OBSERVACIÓN OCI	Durante la auditoría se realizaron visitas a varios puntos de servicios donde se verificaron los centros de cableado y el Data Center, de acuerdo con el anexo No. 3 (Visita de campo y verificación de controles de la red), esta

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO	CÓDIGO: EV-EG-F-03-01
		VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN	PÁGINA: 40 DE 70
		FECHA: 03/05/2021

	oficina encontró evidencias de riesgos en seguridad física y lógica en las redes, dispositivos de comunicación y centros de cableado. Hallazgo No. 15: la mayoría de centros de cableado y cuartos de comunicaciones presentan riesgo de pérdida en la disponibilidad y confidencialidad de la información, toda vez existen deficiencias en cuanto a su restricción de acceso, organización interna de los dispositivos, documentación, planos, certificación y demás condiciones físicas. Cabe destacar que algunos centros de cableado presentan condiciones aceptables de organización y estado físico como en el caso de la UMHES de Engativá y el laboratorio en Simón Bolívar Se reitera el hallazgo No. 07
--	--

7.5. Evaluación de la Política de Gobierno Digital

El seguimiento de esta política se hizo con base en el resultado del cuestionario FURAG publicado en la página de la función pública.



Imagen No. 8 Resultado de la Política de Gobierno Digital FURAG 2021

Para la ejecución de esta actividad se revisaron cada una de las respuestas dadas por el líder de política de la entidad a la luz de la documentación presentada y/o publicadas por la oficina de Sistemas de Información y TICS

De acuerdo con lo anterior y dado que no se cuenta con la escala de medición usada en FURAG, fue necesario determinar atributos de cumplimiento, relacionados con completitud, disponibilidad y calidad de la información requerida y/o que soporta la respuesta dada por la entidad. La siguiente tabla muestra la escala de cumplimiento

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO		CÓDIGO: EV-EG-F-03-01
			VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN		PÁGINA: 41 DE 70
			FECHA: 03/05/2021

Atributo	Convención	Descripción	%
Cumplimiento Total	CT	La totalidad de la documentación que soporta la respuesta, da cumplimiento en términos de los requisitos técnicos relacionados con el objetivo de la pregunta y alcanzan la meta propuesta.	100
Cumplimiento Parcial aumentado	CP+	La mayoría de la documentación que soporta la respuesta, se relaciona con los productos, objetivos y/o servicios requeridos en términos de los requisitos técnicos y de calidad y se evidencia un avance significativo.	75
Cumplimiento Parcial	CP	Parte de la documentación que soporta la respuesta, se relaciona con los productos, objetivos y/o servicios requeridos en términos de los requisitos técnicos y de calidad y se evidencia un avance importante.	50
Cumplimiento Parcial disminuido	CP-	Muy poca documentación que soporta la respuesta se relaciona con los productos, objetivos y/o servicios requeridos en términos de los requisitos técnicos y de calidad, se evidencia un avance mínimo.	25
No cumple	NC	No se cuenta con documentación y/o el procedimiento no se encuentra establecido.	0

Tabla No. 18: Escala de valoración de cumplimiento de requisitos documentales.
Elaboración propia

A continuación se presenta de manera resumida la evaluación realizada por la OCI al cuestionario FURAG de la política de Gobierno Digital. La prueba de evaluación detallada con respuestas del líder de política se muestra en el anexo No. 4 (FURAG Respuestas detallado).

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO		CÓDIGO: EV-EG-F-03-01
			VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN		PÁGINA: 42 DE 70
			FECHA: 03/05/2021

COD PRE	Pregunta	NCL	NCO	Observaciones OCI
GDI01	Señale los criterios de accesibilidad web, del anexo 1 de la Resolución MinTIC 1519 de 2020 que cumple la entidad en todas las secciones de su portal Web oficial:	CT	CP	De acuerdo con la auditoría realizada en la vigencia 2021 por la OCI a la implementación de la resolución 1519 de 2020 y su plan de mejora, todos los hallazgos formulados quedarían subsanados al terminar la actual vigencia. Sin embargo, al hacer una prueba sobre la página principal de la subred, se encuentra que "falta texto alternativo en la imagen vinculada" como muestra la imagen del anexo No. 3 Evaluación detallada Política de Gobierno Digital – FURAG 2021 Dicha situación permite concluir que a la fecha de esta auditoría no se ha completado el plan de mejora y por lo tanto la actual página web no da cumplimiento total con la norma 1519; circunstancia que genera el hallazgo puntual No. 10.
GDI02	Señale los criterios de usabilidad web que cumple la entidad en todas las secciones de su portal Web oficial:	CT	CP	De acuerdo con la auditoría realizada en la vigencia 2021 por la OCI a la implementación de la resolución 1519 de 2020 y su plan de mejora, el cumplimiento de los hallazgos formulados se encuentra en desarrollo y para ser ejecutados en la actual vigencia, por lo tanto la página WEB no da cumplimiento con la norma. En la página "Participa" se evidencian 9 errores de "falta texto alternativo en la imagen vinculada", dicha situación origina que "una imagen sin texto alternativo da como resultado un enlace vacío." Por esta situación se genera el hallazgo puntual No. 10.
GDI03	Con respecto al Plan Estratégico de Tecnologías de la Información (PETI) para esta vigencia, la entidad:	CT	CP +	Esta oficina evidenció que el PETI está formulado pero no ha sido aprobado por el comité de gestión y desempeño institucional. Por lo tanto, la respuesta consignada en FURAG no tiene soporte documental.
GDI04	El Plan Estratégico de Tecnologías de la Información (PETI) incluye:	CT	CP +	El PETI presenta deficiencias en los temas de presupuesto, portafolio de proyectos e indicadores, por lo tanto no cumple con la calificación dada en FURAG.
GDI05	Con respecto a los proyectos de TI definidos en el PETI para la vigencia 2021:	CT	CT	El indicador de avance de los proyectos es de 0% Numero de proyectos ejecutados / Numero de proyectos formulados

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO		CÓDIGO: EV-EG-F-03-01
			VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN		PÁGINA: 43 DE 70
			FECHA: 03/05/2021

COD PRE	Pregunta	NCL	NCO	Observaciones OCI
GDI06	Para la gestión de tecnologías de la información (TI), la entidad cuenta con:	CT	CT	Se evidencia el cumplimiento de los documentos para la gestión de tecnologías de información.
GDI07	Señale los aspectos incorporados en el esquema de gobierno de tecnologías de la información (TI) de la entidad:	CT	CP-	No se evidencian: Manual de políticas de TI definidas, el proceso y procedimientos se encuentran desactualizados, al igual que los indicadores.
GDI08	Para la optimización de las compras de tecnologías de información (TI), la entidad:	CT	CT	Se evidencia que en las compras de TI se utilizan mecanismos o contratos de agregación
GDI09	Respecto a la gestión de proyectos de tecnologías de la información (TI), la entidad:	CP	CP	Se evidencia el cumplimiento parcial de las actividades y opciones de la respuesta en la gestión de proyectos de TI
GDI10	Con relación a la planeación y gestión de los componentes de información, la entidad:	CT	CP-	No se evidencia el cumplimiento de procesos de calidad de datos y no existe un MSPI en la entidad.
GDI11	Con relación a la planeación y gestión de los sistemas de información, la entidad:	CP +	CP-	Esta auditoría no evidencia el cumplimiento de funcionalidades de trazabilidad, log de auditoría en los sistemas de información implementados.
GDI12	Con relación al esquema de soporte y mantenimiento de los sistemas de información, la entidad:	CT	CP-	Se cuenta con un esquema de soporte, pero no se evidencia la aprobación ni la mejora continua
GDI13	Con respecto al ciclo de vida de los sistemas de información, la entidad:	CP +	CP-	No se evidencia el cumplimiento de implementación de un plan de aseguramiento de la calidad. Solo se evidencia el uso de la guía de estilo en la página WEB.
GDI14	Con relación al soporte y operación de la infraestructura de TI (o servicios tecnológicos), la entidad:	CT	CP	Solo se cuenta con plan de mantenimiento de equipos de cómputo, no se evidencia planes de mantenimiento a servidores, redes y equipos activos de comunicación. No se evidencia el uso de computación en la nube, el plan de continuidad de los servicios tecnológicos se encuentra en elaboración. El monitoreo se realiza sobre la disponibilidad de canales y actividad de servidores.
GDI15	¿En qué fase de la adopción de IPv6 se encuentra actualmente la entidad?	CP-	CP-	Se evidencia plan de transición de IPV4 a IPV6

	INFORME FINAL		CÓDIGO: EV-EG-F-03-01
	AUDITORIAS DE CONTROL INTERNO		VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN		PÁGINA: 44 DE 70
			FECHA: 03/05/2021

COD PRE	Pregunta	NCL	NCO	Observaciones OCI
GDI16	Con respecto a la adopción de IPv6, la entidad cuenta con:	CP	CP-	No se evidencia diagnóstico, plan detallado, plan de direccionamiento ni plan de contingencia.
GDI17	Frente a la estrategia para el uso y apropiación de tecnologías de la información (TI), la entidad:	CP +	NC	No se evidencia estrategia implementada de uso y apropiación de tecnología con formación y/o capacitación de servidores.
GDI18	¿La entidad cuenta con un diagnóstico de seguridad y privacidad de la información para la vigencia, construido a través de la herramienta de autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI)?	CT	CT	Se evidencia el diagnóstico de la seguridad y privacidad de la información
GDI19	La política de seguridad y privacidad de la información de la entidad:	CT	CP-	El manual de políticas de seguridad de la información no ha sido implementado, ni aprobado por la alta gerencia, ni se gestiona con mejora continua.
GDI20	¿La entidad cuenta con procedimientos de seguridad y privacidad de la información?	CP +	CP-	Solo se evidencia el procedimiento de gestión de incidentes en una versión preliminar
GDI21	Con respecto al inventario de activos de seguridad y privacidad de la información de la entidad:	CT	NC	Se evidencia una versión preliminar de inventario de activos de información. Pero no se encuentra clasificado, ni se actualiza mediante mejora continua
GDI22	Con respecto a los riesgos de seguridad y privacidad de la información de la entidad:	CP	NC	No se evidencia caracterización de riesgos de seguridad y privacidad de la información
GDI23	¿La entidad implementó el plan de tratamiento de riesgos de seguridad de la información?	CP-	NC	No se evidencia plan de tratamiento de riesgos de seguridad de la información
GDI24	Con respecto al plan operacional de seguridad y privacidad de la información, la entidad:	CT	CP-	La entidad cuenta con un plan de seguridad de la información que no ha sido aprobado
GDI25	Con respecto a los indicadores de implementación del Modelo de Seguridad y Privacidad de la	CP +	NC	No se evidencian indicadores definidos, aprobados e implementados

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO		CÓDIGO: EV-EG-F-03-01
			VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN		PÁGINA: 45 DE 70
			FECHA: 03/05/2021

COD PRE	Pregunta	NCL	NCO	Observaciones OCI
	Información (MSPI) en la entidad:			
GDI27	Con respecto a los procesos, trámites o servicios de la entidad que requieren interoperabilidad:	CT	CP-	Se evidencia un proceso parcial de identificación
GDI28	Con respecto al Marco de Interoperabilidad para realizar intercambio de información con otras entidades:	CT	CP	Existe evidencia parcial del uso del marco de interoperabilidad.
GDI29	Con respecto a los servicios de intercambio de información de la entidad:	CP	CP	Se evidencian servicios de interoperabilidad de la historia clínica
GDI30	Con respecto a los datos abiertos indique:	CP +	CP-	Se evidencian conjuntos de datos abiertos publicados, sin evidencia proceso de identificación de datos abiertos estratégicos.
GDI31	Para el tema de datos abiertos de la entidad, especifique:	CP	NC	No se evidencia el contacto con usuarios de datos abiertos
GDI32	Con respecto al plan de apertura, mejora y uso de datos abiertos para esta vigencia, la entidad:	CT	CP	Se evidencia un instructivo para la apertura, mejora y uso de datos abiertos; pero este no soporta la respuesta de que fue aprobado y que se integra al plan de acción anual.
GDI33	Con respecto a la ejecución del plan de apertura, mejora y uso de datos abiertos para esta vigencia, indique:	CT	NC	En el documento: instructivo para la apertura, mejora y uso de datos abiertos, no se evidencia un plan de apertura de datos con actividades programadas
GDI34	Con respecto a los procesos de la entidad, indique:	NC	NC	No se evidencian ejercicios de arquitectura empresarial de TI
GDI35	La automatización o mejora de los procesos le ha permitido a la entidad:	NC	NC	No se evidencian ejercicios de arquitectura empresarial de TI
GDI36	¿La entidad ha implementado iniciativas de ciudades y territorios inteligentes?	CT	CT	Se evidencia la participación activa de la subred en la construcción de la plataforma Bogotá Salud Digital
GDI37	En cuáles instrumentos de planeación de la entidad se contemplaron las iniciativas o	CT	CT	Se evidencia la participación activa de la subred en la construcción de la plataforma Bogotá Salud Digital

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO		CÓDIGO: EV-EG-F-03-01
			VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN		PÁGINA: 46 DE 70
			FECHA: 03/05/2021

COD PRE	Pregunta	NCL	NCO	Observaciones OCI
	proyectos de ciudad o territorio inteligente:			
GDI38	Para el despliegue y operación de servicios relacionados con iniciativas de ciudad o territorio inteligente, la entidad utiliza algunos de los siguientes servicios de computación en la nube:	NC	CP-	Se evidencia el uso de SAS en el correo electrónico.
GDI39	Con respecto al uso de internet de las cosas (IoT), la entidad ha realizado:	NC	NC	Sobre IoT, la entidad no ha realizado ejercicios
GDI40	¿La entidad hace uso de los instrumentos de agregación de demanda y priorización de los servicios de nube (como Acuerdos Marco de precios) para la gestión de recursos públicos en proyectos de Tecnologías de la Información?	NC	CP-	La entidad solo cuenta con servicio de correo como SaaS
GDI41	¿La entidad hace uso de tecnologías basadas en software libre o código abierto?	CT	CT	Se evidencia el uso de plataformas de software libre
GDI42	Cuáles de las siguientes tecnologías emergentes de la Cuarta Revolución Industrial que facilitan la prestación de servicios del Estado utiliza la entidad:	CP	CP-	No se evidencia el uso de inteligencia artificial en los procesos de prestación de servicios
GDI43	¿La entidad aplica programas de uso de tecnología para participación ciudadana y Gobierno abierto en sus procesos misionales?	CT	NC	En los procesos misionales no se evidencia el uso de tecnología para la participación ciudadana y gobierno abierto. Adicionalmente la evidencia enviada no es accesible
GDI44	¿La entidad hace uso de estrategias público-privadas que propendan por el uso de medios de pago electrónico?	CT	CT	Se evidencia el uso de estrategias para el fomento de pago electrónico

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO		CÓDIGO: EV-EG-F-03-01
			VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN		PÁGINA: 47 DE 70
			FECHA: 03/05/2021

COD PRE	Pregunta	NCL	NCO	Observaciones OCI
GDI45	¿La entidad cuenta con programas de capacitación que permitan a sus servidores públicos apropiarse de capacidades para conocer tecnologías de la cuarta revolución industrial?	NC	NC	No se evidencia el fomento de conocimiento de tecnologías de la 4ta revolución industrial
GDI46	¿La entidad hace uso de contratos de Asociaciones Público Privadas (APP) relacionados con Tecnologías de la Información y las Comunicaciones?	NC	NC	La entidad no hace uso de asociaciones público privadas relacionadas con TI
GDI47	La entidad hace uso del machine learning para:	NC	NC	La subred no hace uso de Machine Learning
GDI48	¿En cuál de los siguientes niveles la entidad hace uso de la Inteligencia Artificial –IA?	NC	NC	En concordancia con la pregunta No. 42. La entidad no hace uso de inteligencia artificial
GDI49	Con respecto al Plan de Transformación Digital (entendido en los términos del artículo 147 del PND y bajo los lineamientos del Marco de Transformación Digital) para la vigencia 2021, la entidad:	CT	CP +	De acuerdo con la pregunta 03. Esta oficina evidenció que el PETI está formulado pero no ha sido aprobado por el comité de gestión y desempeño institucional.
GDI50	Con respecto al uso de tecnologías DTL (Distribute Ledger Technologies) como Blockchain, la entidad:	NC	NC	La entidad no ha desarrollado proyectos o aplicaciones de DLT
GDI51	¿Existe en la entidad un equipo dedicado exclusivamente a la explotación de datos mediante la aplicación de técnicas y métodos de analítica de datos y Big Data?	CT	NC	Se evidencia que la entidad cuenta con un equipo de estadística, no con un equipo de explotación de datos.
GDI52	Con respecto a la capacitación que brinda la entidad en analítica de datos y Big Data:	NC	NC	La entidad no usa técnicas de explotación de datos. Adicionalmente esta respuesta controvierte la respuesta de la pregunta 51

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO		CÓDIGO: EV-EG-F-03-01
			VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN		PÁGINA: 48 DE 70
			FECHA: 03/05/2021

COD PRE	Pregunta	NCL	NCO	Observaciones OCI
GDI53	¿Durante los últimos cinco años la entidad ha destinado un presupuesto específico a la explotación de datos?	NC	NC	La entidad no usa técnicas de explotación de datos. Adicionalmente esta respuesta controvierte la respuesta de la pregunta 51
GDI54	A la hora de priorizar inversiones y distribuir el presupuesto de la entidad:	NC	NC	La entidad no usa técnicas de explotación de datos.
GDI55	¿La entidad ha implementado alguna iniciativa, proyecto o prueba de concepto de explotación de datos y Big Data?	CT	CP	Se evidencia la participación de la subred en la construcción de la plataforma Bogotá Salud Digital. No se evidencia iniciativa, proyecto de explotación de datos.
GDI56	Con respecto a la calidad de los conjuntos de datos de la entidad:	CP	CP-	Se evidencia un instructivo para la apertura, mejora y uso de datos abiertos. Sin embargo su procesamiento se realiza manual y con el uso de herramientas ofimáticas
GDI57	En el contexto de la explotación de datos y Big Data, ¿La entidad ha aplicado alguna técnica de anonimización que preserve la privacidad de los datos?	NC	NC	No se evidencian técnicas ni herramientas de anonimización de datos.
GDI58	¿La entidad define métricas para medir la calidad de los datos?	CT	NC	No se evidencian métricas de (DQA) Data Quality Assessment
GDI59	¿La entidad cuenta con un protocolo estandarizado para la anonimización y protección de datos personales (seguridad y privacidad)?	CT	NC	No se evidencia protocolo estandarizado para la anonimización y protección de datos. Adicionalmente esta respuesta controvierte la respuesta de la pregunta 51
GDI60	¿La entidad tiene definida una política de gobernanza de datos?	CP-	NC	No se evidencia el proceso de construcción de una política de gobernanza de datos en la entidad
GDI61	¿La entidad ha desarrollado iniciativas o proyectos basados en el uso de tecnologías emergentes (Inteligencia artificial, Internet de las cosas,	CT	NC	No se evidencia el desarrollo de iniciativas o proyectos basados en uso de tecnologías emergentes. Adicionalmente la evidencia enviada no es accesible

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO		CÓDIGO: EV-EG-F-03-01
			VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN		PÁGINA: 49 DE 70
			FECHA: 03/05/2021

COD PRE	Pregunta	NCL	NCO	Observaciones OCI
	Blockchain, Big Data, Robótica, entre otros)?			
GDI62	Con respecto a los servicios de la entidad:	CT	ND	Esta auditoría no pudo confirmar el dato aquí consignado
GDI63	Con respecto a los trámites de la entidad:	CT	ND	Esta auditoría no pudo confirmar el dato aquí consignado

NCL: Nivel de Cumplimiento Líder de política

NCO: Nivel de Cumplimiento Oficina Control Interno

Tabla No. 19: Resumen de evaluación de cumplimiento de la PGDI 2021
Elaboración propia

En la siguiente tabla permite ver las diferencias porcentuales entre la evaluación OCI y la evaluación del líder de política.

	Nivel de cumplimiento					
	CT	CP+	CP	CP-	NC	ND
Evaluación cumplimiento Líder Política	52%	10%	11%	5%	23%	0%
Evaluación cumplimiento OCI	13%	5%	13%	26%	40%	3%
Diferencia	39%	5%	2%	21%	18%	3%

Tabla No. 20: Diferencias porcentuales evaluación de cumplimiento de la PGDI 2021
Elaboración propia

Se puede constatar en la anterior tabla y en los instrumentos de las pruebas (tabla resumen de cumplimiento y anexo No. 4), que se dio respuesta de cumplimiento total al 39% de las preguntas de la PGDI, sin que se evidencie la totalidad de la documentación que soporta la respuesta, en términos de los requisitos técnicos relacionados con el objetivo de la pregunta. La anterior situación reitera el hallazgo No. 07.

La causa es una falta de objetividad en las respuestas del FURAG consignadas por el líder de la política y fallas en la primera y segunda línea de defensa.

Riesgo: un posible riesgo legal debido a la sobre calificación y la dificultad para soportar la respuesta ante los entes de control. Adicionalmente se genera una falsa expectativa sobre la política.

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO	CÓDIGO: EV-EG-F-03-01
		VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN	PÁGINA: 50 DE 70
		FECHA: 03/05/2021

7.6. Riesgos de corrupción

Durante la auditoría realizada por la oficina de control interno se pudo evidenciar que el proceso no tiene identificados riesgos en el mapa de riesgos de corrupción, por este motivo se sugiere realizar un análisis profundo de los procedimientos y actividades que se realizan dentro del área para lograr identificar este tipo de riesgos, ya que se pudo establecer que hay puntos sensibles donde podrían presentarse temas relacionados con corrupción, principalmente con la certificación de facturas sin cumplimiento pleno de las obligaciones, situación que reitera el hallazgo No. 02.

7.7. Descripción de hallazgos generados

Hallazgo No. 01 Debilidades en la documentación del proceso SI-C-01-01-Gestión de la Información y Tics
Posibles causas identificadas por la Oficina de Control Interno: • Se realizan modificaciones a las actividades del proceso sin tener en cuenta realizar dichos cambios en los formatos, procedimientos o instructivos relacionados con las acciones que se ejecutan. • Falta de seguimiento y verificación por parte del área de calidad en el control de documentos que son normalizados. • Fallas en la depuración de los documentos del proceso por parte de las áreas relacionadas, en cuanto a que se dejan de utilizar, se modifican o simplemente se adaptan a los nuevos requerimientos de las actividades. • Falta de personal capacitado que esté encargado de la actualización de la documentación para que se ajuste a lo requerido.
Descripción del riesgo: Uso de procedimientos no adecuados y que no garantizan la efectividad de las acciones que se requieran para el seguimiento y control del proceso.
Descripción del impacto: • Posible información errada sobre las actividades realizadas por el proceso. • Realización de actividades innecesarias o reprocesos que disminuyan la optimización de los recursos con los que cuenta el proceso. • Pérdida de tiempo en la realización de actividades inadecuadas u omisión de otras, en el desarrollo del procedimiento.

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO	CÓDIGO: EV-EG-F-03-01
		VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN	PÁGINA: 51 DE 70
		FECHA: 03/05/2021

- Desinformación en el proceso de inducción de nuevos colaboradores del área.

Recomendaciones:

- Revisar y actualizar los documentos vigentes del proceso para que sean acorde con las actividades que deben realizarse según las necesidades de cada área.
- Coordinar con el área de normalización de Calidad para realizar la depuración de los documentos desactualizados dejando solo documentos vigentes.
- Revisar la normatividad aplicable para garantizar la documentación requerida para el adecuado desarrollo del proceso.

ANÁLISIS A LA RESPUESTA DADA AL INFORME PRELIMINAR SOBRE EL HALLAZGO No. 01

El proceso auditado en comunicación del 11 de noviembre de 2022 según radicado 20221900032913 presenta la siguiente observación:

En la vigencia actual 2022 la Oficina de Sistemas TIC ha realizado mesas de trabajo con la Oficina de Desarrollo Institucional con el fin de actualizar la documentación referente al proceso gestión de información y Tics, para lo cual se han realizado las siguientes actividades:

- 1. Actualización de la caracterización del proceso de gestión de la información y Tics, el cual ya se encuentra en normalización.*
- 2. Revisión y actualización de los procedimientos:*
 - Procedimiento identificación, consolidación, disposición y publicación de la información*
 - Procedimiento de gestión de incidentes y mesa de servicios Nota: La caracterización del proceso y los procedimientos se encuentran en proceso de envío a normalización por parte de la Oficina de Desarrollo Institucional.*
- 3. Revisión y actualización del instructivo de gestión de incidentes de seguridad de la información*
- 4. Creación de la política de gobernanza de datos.*
- 5. Creación del plan de continuidad de los servicios tecnológicos.*
- 6. Se encuentra en proceso de documentación el inventario de activos de información, matriz de riesgos de seguridad digital y plan de tratamiento de riesgos de seguridad digital.*

Dado a lo anterior, se observa que la Oficina de Sistemas con su recurso humano actual, ha logrado mantener la revisión y actualización de documentación vital para el proceso enmarcado para el cumplimiento de las diferentes políticas de gobierno digital y seguridad digital.

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO	CÓDIGO: EV-EG-F-03-01
		VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN	PÁGINA: 52 DE 70
		FECHA: 03/05/2021

Es de aclarar que para la caracterización de los procesos se tiene como marco de referencia el Modelo de Gestión IT4+ emanado por el Ministerio de la Información y las comunicaciones en los componentes Estrategia de TI Gobierno de TI, Gestión de información, Sistemas de Servicios tecnológicos y Uso y Apropiación de TI.

Luego de evaluar la respuesta dada por el proceso auditado, la oficina de control interno no encuentra justificación suficiente para retirar el hallazgo del informe final, debido a: (1). Los documentos entregados se encuentran en una fase preliminar, y no han sido normalizados, validados y socializados. (2) Faltan procedimientos importantes dentro de la caracterización, tal es el caso de: “*administración y rotación de copias de seguridad*”. (3) El plan de continuidad de servicios informáticos debe ser probado, aprobado y socializado, documentación que no se evidencia. (4) Los activos de información aún se encuentran en proceso de caracterización, por lo tanto, (5) El mapa de riesgos de seguridad digital no cumple con los requerimientos metodológicos definidos por el DAFP y MINTIC.

HALLAZGO No. 02

Supervisión ineficiente de los contratos a cargo del proceso de Sistemas de Información y TICs generando un posible riesgo de corrupción frente a la certificación y pago de las facturas de los contratos, dado que no se tiene un control adecuado sobre los incumplimientos reiterados de las obligaciones contractuales, adicionalmente no se están publicando los soportes de supervisión y ejecución de los contratos en la plataforma SECOP

Posibles causas identificadas por la Oficina de Control Interno:

- Desconocimiento de las obligaciones referidas en el manual de supervisión de contratos establecido por la Subred Norte.
- Falta de capacitación de las personas que realizan el proceso de supervisión de los contratos sobre manejo de la plataforma del SECOP y sobre la totalidad de las obligaciones precontractuales y contractuales requeridas sobre los soportes a cargar en la plataforma.
- Posible sobrecarga laboral del personal de la Oficina de sistemas y TICs que no permita mantener actualizada la información de cumplimiento de los contratos.

Descripción del riesgo:

- Posible afectación de los servicios asistenciales y administrativos por periodos prolongados de tiempo, por incumplimiento de las obligaciones contractuales de los proveedores debido a un seguimiento inadecuado por parte de los supervisores de contrato.
- Incumplimiento normativo

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO	CÓDIGO: EV-EG-F-03-01
		VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN	PÁGINA: 53 DE 70
		FECHA: 03/05/2021

Descripción del impacto:

- Retraso en actividades de los procesos de la subred que son soportados mediante la contratación de servicios a proveedores externos, por incumplimiento de las obligaciones contractuales.
- Posibles hallazgos por parte de los entes de control cuando realicen sus evaluaciones.
- Investigaciones, multas y sanciones debido a la falta de seguimiento o aplicación de la normatividad vigente.
- Pago de facturas de los contratos a pesar de los incumplimientos.
- Incumplimiento de los principios de transparencia y pérdida de confianza y credibilidad de la entidad.

Recomendaciones:

- Realizar capacitaciones a los supervisores de los contratos sobre el manual de supervisión de la subred, así, como sobre el manejo y cargue de la información contractual requerida en la Plataforma SECOP II
- Efectuar verificaciones periódicas a las obligaciones contractuales de los proveedores de los servicios contratados por el proceso, para tomar decisiones sobre el pago de las facturas.
- Cumplir las disposiciones de la Circular Externa 01 de 2021 de Colombia Compra Eficiente, relacionada con la publicación de la totalidad de documentos del proceso de seguimiento Contractual en la plataforma SECOP II.

Hallazgo No. 03

Deficiencias metodológicas en el diseño y redacción de los controles definidos para la mitigación de los riesgos del proceso. Adicionalmente el mapa de riesgos se encuentra desactualizado y no contempla posibles riesgos por actos de corrupción.

Posibles causas identificadas por la Oficina de Control Interno:

- Falta de claridad o capacitación sobre la metodología a utilizar en la subred norte para la formulación de los riesgos y sus controles.
- Se evidencia que el mapa de riesgos que está implementado para subred no se ha actualizado desde el 2020 es decir hace 2 años
- Falta de conocimiento en materia de riesgos por parte de las personas que participan en el proceso de gestión de la información y TICs de la Subred Norte.

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO	CÓDIGO: EV-EG-F-03-01
		VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN	PÁGINA: 54 DE 70
		FECHA: 03/05/2021

Descripción del riesgo:

Posible materialización los riesgos del proceso por falta de controles y su mitigación la cual no es efectiva.

Descripción del impacto:

- Incumplimiento a normatividad y recomendaciones de la DAFP en relación a la identificación, clasificación y controles de los riesgos reconocidos para el proceso de gestión de la información y TIC
- Posibles inconvenientes jurídicos, fiscales, económicos y hasta disciplinarios en razón de falta de controles de riesgos o asignación inadecuada de los mismos.
- Investigaciones, multas y sanciones debido a la falta de aplicación de la normatividad

Recomendaciones:

- Trabajar en conjunto con la Oficina de Desarrollo institucional la capacitación sobre el manejo e implementación de la metodología para la administración de Riesgos según el DAFP.
- Gestionar en coordinación con la Oficina de Desarrollo Institucional, la actualización del mapa de riesgos del proceso de gestión de la información y TIC, reforzando la identificación de causas, descripción y redacción de riesgos y controles, metas e indicadores de acuerdo a la metodología institucional que sea definida.
- Evaluar la implementación del mapa de riesgos de corrupción del proceso

Hallazgo No. 04

Las carpetas y archivo de los documentos del proceso, no cumplen con lo establecido y reglamentado en el acuerdo 042 del archivo general de la nación.

Posibles causas identificadas por la Oficina de Control Interno:

- Desconocimiento de los criterios para la organización de los archivos de gestión según las TRD, por parte de las personas que realizan el archivo de los soportes físicos de las hojas de vida de los equipos de cómputo.
- Ausencia de carpetas membretadas con las caratulas estandarizadas para la Subred que son entregadas por gestión documental para el archivo de documentos de gestión y hojas de vida de los equipos.

Descripción del riesgo:

- Incumplimiento de normatividad establecida en el acuerdo 042 del Archivo General de la Nación

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO	CÓDIGO: EV-EG-F-03-01
		VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN	PÁGINA: 55 DE 70
		FECHA: 03/05/2021

- Inadecuado seguimiento sobre el estado de gestión que se tiene sobre cada uno de los equipos de cómputo, en cuanto a los mantenimientos, repuestos y Software instalado.

Descripción del impacto:

- Generación de activos de información mal gestionados; posible pérdida de información, falencias en la disponibilidad de la información y reprocesos en la gestión documental.
- Ausencia de certeza de la completa información que se mantiene en las hojas de vida de los equipos con los que cuenta la subred.
- Posibles hallazgos por parte de los entes de control cuando realicen sus evaluaciones.
- Incumplimiento de los principios de transparencia y pérdida de confianza y credibilidad de la entidad.

Recomendaciones:

- Realizar verificación de lo establecido por las TRD establecidas para la oficina de sistemas de información y TICs código AP-GI-T-20-01 y del acuerdo 042 del Archivo General de la Nación.
- Mantener un expediente individual de los equipos de cómputo con todo lo relacionado con hoja de vida, mantenimientos, repuestos, software y licencias para garantizar la información de estos activos.
- Debido a que los equipos son trasladados entre unidades de servicio según las necesidades de la entidad no es recomendable tener los archivos agrupados por punto de atención.

Hallazgo No. 05

Incumplimiento en el plan de mantenimiento de equipos de cómputo y ausencia de mantenimiento en servidores, lo que genera una posible pérdida en la disponibilidad e integridad de la información ocasionada por daños en servidores y equipos de cómputo.

Posibles causas identificadas por la Oficina de Control Interno:

- Falta de planeación para la elaboración de los cronogramas de mantenimientos.
- Alta rotación o traslado de los equipos de cómputo entre puntos de atención, sin un control eficiente, lo que no permite tener certeza de la ubicación de los equipos actualizada, dificultando la programación de los mantenimientos.
- Escasez de personal o alta rotación de los técnicos encargados de realizar los mantenimientos que genera atrasos en esta actividad.
- Falta de recursos económicos disponibles para la realización adecuada de los mantenimientos

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO	CÓDIGO: EV-EG-F-03-01
		VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN	PÁGINA: 56 DE 70
		FECHA: 03/05/2021

Descripción del riesgo:

Posible daño en los activos de información y equipos de cómputo generando inconvenientes en las actividades normales de los procesos tanto asistenciales como administrativos y de las demás consecuencias que conlleven los daños físicos de los equipos y servidores.

Descripción del impacto:

- Pérdida en la disponibilidad e integridad de la información necesaria para el normal funcionamiento de la entidad.
- Incumplimiento de los compromisos adquiridos por los procesos de la subred generando pérdida de confianza y credibilidad de la entidad.
- Inoportunidad en la entrega de información solicitada por los entes de control en caso que lo requieran.
- Posibles pérdidas económicas por fallas en el servicio.

Recomendaciones:

- Realizar ajustes necesarios al cronograma de mantenimientos teniendo en cuenta las modificaciones que se van presentando por traslados de equipos, con el propósito de velar por el cumplimiento de las fechas establecidas y evitar daños.
- Fortalecer el trabajo en conjunto con el área de activos fijos para mantener un inventario actualizado de los equipos, que permita tener claridad sobre el estado de estos por unidad, reduciendo el número de traslados sin confirmación adecuada.
- Buscar estrategias para disminuir la rotación del personal encargado de la realización de los mantenimientos, para garantizar el recurso suficiente para poder dar cumplimiento a los cronogramas de mantenimiento.
- Realizar seguimientos periódicos al cumplimiento del cronograma y/o plan de mantenimiento.

Hallazgo No. 06

Incumplimiento al Acuerdo de Nivel de Servicios establecido en el documento AP-GI-I-19-01

Posibles causas identificadas por la Oficina de Control Interno:

- Escasez de personal o alta rotación de los técnicos encargados de realizar los mantenimientos correctivos que genera retrasos en los requerimientos de la mesa de servicios.
- Posible desconocimiento del Instructivo Acuerdos de Niveles de Servicio por parte del personal de la oficina de sistemas de información y TICs, encargada de la solución de los requerimientos de la mesa de servicios.

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO	CÓDIGO: EV-EG-F-03-01
		VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN	PÁGINA: 57 DE 70
		FECHA: 03/05/2021

- Posible incremento del número de solicitudes a la mesa de servicio por falta de mantenimiento.

Descripción del riesgo:

La falta de cumplimiento de los Acuerdos de Niveles de Servicio ocasiona incertidumbre dentro de los procesos de la subred generando pérdida de confianza y daño reputacional y en casos extremos hasta pérdidas económicas por fallas en el servicio.

Riesgo de pérdida de tiempo del personal administrativo por reprocesos y demora en la solución de las solicitudes de mesa de servicio.

Descripción del impacto:

- Incumplimiento de los compromisos adquiridos por los procesos internos de la subred generando pérdida de confianza y credibilidad de la entidad.
- Generación de reprocesos o desviación de los recursos con los que cuenta la entidad para mantener el servicio de manera óptima mientras se solucionan los requerimientos que presentan retrasos en la solución por parte de la mesa de servicios.
- Pérdidas económicas por tiempo inoficioso del personal administrativo y/o reprocesos.

Recomendaciones:

- Tomar medidas efectivas para lograr el ajuste de los tiempos de atención de la mesa de servicio para garantizar el cumplimiento de los ANS
- Fomentar estrategias que permitan reducir la alta rotación del personal encargado de dar solución de los requerimientos registrados en la mesa de servicio.
- Hacer seguimiento periódico sobre los tiempos de atención que se estén presentado en la solución de los requerimientos y así tomar decisiones oportunas para mejorar el nivel de satisfacción de los procesos internos que hacen uso de la mesa de servicios.

Hallazgo No. 07

Ausencia de documentación y/o evidencias que soporten la totalidad de las respuestas, en términos de los requisitos técnicos relacionados con el objetivo de la pregunta del FURAG 2021, generando sobre calificación de las Políticas de Seguridad y Gobierno Digital.

Posibles causas identificadas por la Oficina de Control Interno:

- Diligenciamiento del formulario sin el debido seguimiento y verificación de los soportes necesarios, que garanticen el cumplimiento los requerimientos y gestión de las políticas de Seguridad y Gobierno Digital.

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO	CÓDIGO: EV-EG-F-03-01
		VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN	PÁGINA: 58 DE 70
		FECHA: 03/05/2021

- Falta de objetividad en las respuestas del FURAG consignadas por el líder de la política y/o fallas en la primera y segunda línea de defensa.
- Falta de conocimiento sobre los insumos documentales por la primera línea de defensa.
- Gran densidad documental técnica requerida.
- Desconocimiento y falta de uso de las metodologías dispuestas por MINTIC.
- Falta de personal técnico especializado.
- Desconocimiento de la PGDI por parte de la primera línea de defensa y líder de política.
- Presión para obtener alta calificación en el IDI.

Descripción del riesgo:

Posibles implicaciones disciplinarias debidas a la sobre calificación y a la dificultad para soportar la respuesta ante los entes de control. Adicionalmente se genera una falsa expectativa sobre la valoración de las políticas que impiden visibilizar plenamente los avances y necesidades de mejora en la gestión.

Descripción del impacto:

- Mostrar un nivel de desempeño que no está acorde con la realidad de la entidad.
- Posibles hallazgos por parte de los entes de control, ante la incapacidad de soportar las respuestas cuando se realicen las evaluaciones.
- Posibles sanciones debido a la falta de seguimiento de los requerimientos de la política y la no aplicación de la normatividad vigente.
- Falsa expectativa sobre el estado de la seguridad de la información en la Subred.
- Reputacional por pérdida de credibilidad e imagen institucional.
- Dificultad para emprender acciones correctivas y preventivas sobre las debilidades presentadas.

Recomendaciones:

- Fortalecer el proceso de diligenciamiento del instrumento de evaluación de las políticas y realizar seguimiento adecuado a las respuestas que son entregadas durante el diligenciamiento del FURAG
- Es importante que los funcionarios que den respuesta a la evaluación FURAG, tengan el conocimiento y la capacitación, además que la segunda línea de defensa y/o el dueño de la política realice la revisión de la totalidad de la información, antes de ser enviada.
- Propender el cumplimiento adecuado de los lineamientos establecidos dentro de la política de Seguridad digital y el SGSI.
- Responder los cuestionarios de manera objetiva, evidenciando que se cuenten con los documentos idóneos para soportar las respuestas.

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO	CÓDIGO: EV-EG-F-03-01
		VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN	PÁGINA: 59 DE 70
		FECHA: 03/05/2021

- Afinamiento de información: manuales, procedimientos, políticas e instructivos que permitan el logro esperado del enfoque de la política.
- Atender las 9 y 28 recomendaciones realizadas por la medición de desempeño institucional 2021 sobre las Política de Seguridad y Gobierno Digital respectivamente.

Hallazgo No. 08

Materialización del riesgo de daño en la base de datos de Orfeo, con pérdida en la disponibilidad de la información y posible compromiso de los datos, sin que mediara un procedimiento documentado sobre la gestión del incidente.

Posibles causas identificadas por la Oficina de Control Interno:

- Fallas en la estabilidad del sistema o del servidor de apoyo del aplicativo por vulnerabilidades de seguridad.
- Falta de una herramienta de respaldo o de una copia de seguridad de la información de la base de datos del aplicativo Orfeo.

Descripción del riesgo:

Pérdida parcial o definitiva en la disponibilidad e integridad de la información y posible compromiso de los datos que afectan los objetivos institucionales y el funcionamiento normal de la institución.

Descripción del impacto:

- Pérdida de información necesaria para gestión y toma de decisiones dentro de los procesos internos de la Subred.
- Generación de reprocesos dentro de las actividades de las áreas afectadas para lograr la recuperación de la información mientras se restaura la disponibilidad del sistema.
- Inicio de acciones por no atender requerimientos de entes de control o pérdidas de la trazabilidad en la correspondencia interna y externa

Recomendaciones:

- Tener implementado un plan de contingencia para situaciones en las que se presenten fallas de los aplicativos que soportan los procesos internos de la institución para mitigar los impactos por pérdida de información.
- Contar con una copia de seguridad de la información más sensible de la institución o contar con herramientas informáticas para la recuperación de esta.
- Presentar un informe sobre el resultado de la evaluación del incidente sobre el aplicativo Orfeo, con el fin de adelantar acciones al respecto.

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO	CÓDIGO: EV-EG-F-03-01
		VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN	PÁGINA: 60 DE 70
		FECHA: 03/05/2021

Hallazgo No. 09

Exposición de la información almacenada en los equipos de cómputo y servidores a ataques informáticos causados por malware, debidos al vencimiento del sistema antivirus.

Posibles causas identificadas por la Oficina de Control Interno:

- Falta de planeación o seguimiento a las fechas de vencimiento de las licencias y/o permisos de los aplicativos con los que cuenta la subred.
- Demora en los procesos de contratación para la adquisición de bienes y servicios.
- Falta de recursos financieros o proyectados dentro del presupuesto asignado para la oficina de sistemas de información y TICs.
- Falta de utilización de los acuerdos marco de plataforma de Colombia compra eficiente.

Descripción del riesgo:

- Posible pérdida parcial o definitiva en la disponibilidad de la información y compromiso de los datos que forman parte del inventario de activos de información de la subred.
- Posibilidad de ataques informáticos que pongan en riesgo la integridad de la información con la que cuenta la subred.
- Posibilidad de sufrir secuestro de información o ransomware.

Descripción del impacto:

- Vulnerabilidad del sistema de información por ataques causados por Malware o delincuentes informáticos
- Daños en el hardware y software de los equipos de cómputo con los que cuenta la subred produciendo inconvenientes en el funcionamiento general de la entidad.
- Pérdidas económicas por reprocesos y/o perturbaciones en las operaciones.
- Daño reputacional y pérdida de confianza de terceros.

Recomendaciones:

- Hacer seguimiento frecuente de las fechas de vencimiento de las licencias y permisos de los programas que son requeridos por la institución para su normal funcionamiento y de esta manera anticiparse para tomar decisiones y agilizar los procesos de adquisición de los bienes y servicios requeridos.
- Reforzar el proceso de planeación contractual para la renovación de los antivirus.

ANÁLISIS A LA RESPUESTA DADA AL INFORME PRELIMINAR SOBRE EL HALLAZGO No. 09

El proceso auditado en comunicación del 11 de noviembre de 2022 según radicado 20221900032913 presenta la siguiente observación:

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO	CÓDIGO: EV-EG-F-03-01
		VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN	PÁGINA: 61 DE 70
		FECHA: 03/05/2021

La oficina de sistemas suscribió contrato No. 121 de 2021, cuyo objeto es “Contratar la renovación y / o actualización del antivirus ESET Endpoint Security Protection Avanced incluye la consola (esta está separada en cinco sedes), servidores y computadores de la subred norte ese el cual consta de licencia y soporte e instalación”, con la empresa Redcomputo para lo cual el proveedor suministra licencia con fecha de expiración 30 de julio de 2022.

Teniendo en cuenta lo anterior la Oficina de Sistemas de Información – TIC inicia proceso de contratación a través de la solicitud de estudios de mercado de fecha 21 de junio de 2022.

Producto de lo anterior la Subred Norte ESE publica en la plataforma SECOP el estudio de mercado No. 174-2022 ANTIVIRUS, al cual se presentan cinco (5) proponentes. Basado en lo anterior se solicita CDP y se expide el No. 1734 de 28 de junio de 2022 y estudios previos de fecha 28 de junio de 2022 el cual es radicado ante la Dirección de Contratación el 29 de junio de 2022.

Se da inicio el proceso de contratación para la adquisición del licenciamiento del antivirus para la Subred Norte ESE ante el SECOP. Producto de lo anterior y surtidos todos los procesos se suscribe contrato de compraventa No. BYS 120 – 2022 con fecha inicio de contrato 09/09/2022 con la empresa CLUSTER DE SERVICIOS S.A.S.

La oficina de control interno considera que la suscripción del contrato de BYS 120-2022 es una corrección, sin embargo no incide directamente sobre la causa del hallazgo toda vez que faltó planeación y gestión para evitar que los sistemas quedaran desprotegidos por un tiempo considerable (mayor a 60 días), dando la posibilidad de la materialización del riesgo de ataques informáticos, situación que mantiene vigente el hallazgo. Es importante se tomen medidas preventivas para mitigar el riesgo de ataques informativos por vencimiento del antimalware, razón por la cual se requiere plan de mejora y se diseñen los controles adecuados.

Hallazgo No. 10

Falta de un plan de continuidad del negocio y ejercicios de simulación y respuesta ante el evento de que una amenaza explote una vulnerabilidad de un activo de información crítico.

Posibles causas identificadas por la Oficina de Control Interno:

- Falta de lineamientos desde la línea estratégica sobre continuidad del negocio (política de continuidad de negocio)
- Falta de recursos económicos para su implementación.

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO	CÓDIGO: EV-EG-F-03-01
		VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN	PÁGINA: 62 DE 70
		FECHA: 03/05/2021

- Falta de conocimiento en la normatividad relacionada con la continuidad del negocio.
- Falta de talento humano y de interrelación con las demás dependencias de la Subred.

Descripción del riesgo:

No contar con un plan que mitigue y permita reaccionar de manera eficiente sobre una posible falla en la disponibilidad de la información y/o denegación de servicios, ocasionada por la amenaza de ataque informático.

Descripción del impacto:

- No contar con un plan de continuidad del negocio puede ocasionar pérdidas económicas por la falta de disponibilidad de los servicios informáticos que soportan el negocio.
- Pérdidas económicas por falta de control en procesos críticos, como facturación e historia clínica.
- Reputacional: por la pérdida de confianza de los clientes y terceros.
- Pérdida de vidas o degradación de la salud de los pacientes, por inoperatividad de sistemas de información de apoyo a procedimientos médicos.

Recomendaciones:

Implementar un plan de continuidad de negocio para el proceso debidamente estructurado, que cuente con puntos de control y que cubra procesos y servicios críticos, estableciendo la estrategia, desarrollo e implementación de la respuesta, el mantenimiento y prueba entre otros.

Hallazgo No. 11

El inventario de activos de información de la Entidad no contempla los inventarios de activos de información de Tics, ni la caracterización de los riesgos de seguridad y privacidad de la información de acuerdo con la metodología definida por el DAFP y MINTIC.

Posibles causas identificadas por la Oficina de Control Interno:

- No existe procedimiento específico para la identificación de riesgos de SI.
- Falta de capacitación sobre la caracterización y gestión de riesgos de SI.
- El inventario de activos de información está enfocado solo a documentos.
- No se da cumplimiento al plan de seguridad y privacidad de la información.
- Falta de una gestión real de riesgos tecnológicos y de seguridad alineados con los activos críticos de la subred.
- No contar con los recursos necesarios para la caracterización de activos de información.

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO	CÓDIGO: EV-EG-F-03-01
		VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN	PÁGINA: 63 DE 70
		FECHA: 03/05/2021

Descripción del riesgo:

Inadecuada gestión de los riesgos de seguridad y privacidad de la información.

Descripción del impacto:

- Legal por incumplimiento de la ley transparencia 1712 de 2014.
- Dificultad para la acreditación de la Subred, por incumplimiento de los estándares 144 y 145 de la norma de acreditación.
- Deficiencias en la valoración y gestión de los riesgos de Seguridad de la información y de TI
- Deficiencias en la gestión de planes de continuidad.

Recomendaciones:

- Definir el procedimiento de levantamiento y actualización de activos de información, estableciendo las directrices y actividades generales para identificar, clasificar y valorar los activos de información de la Subred.
- Incluir los activos de Tics dentro del inventario de de activos de información en conformidad con lo determinado por la guía de MINTIC, incluyendo los activos de SI.
- Efectuar el análisis de vulnerabilidades sobre los activos críticos de SI
- Realizar el análisis y gestión de riesgos sobre los activos de SI de acuerdo con la metodología de gestión de riesgos de Seguridad de la Información del DAFP y MINTIC.

Hallazgo No. 12

Fallas en los procedimientos y políticas de control de acceso a las aplicaciones y servicios informáticos. Se debe evitar el acceso no autorizado a sistemas y servicios

Posibles causas identificadas por la Oficina de Control Interno:

- Fallas en las políticas de control de acceso a los recursos informáticos.
- Fallas en las políticas de talento humano con relación al momento de terminar el contrato.
- Falta de control por parte de los administradores de los sistemas, al momento de establecer o denegar privilegios dentro de los sistemas.
- Falta de procedimientos de control y de comunicación entre el área de Tics y las demás áreas con relación a los funcionarios con permisos dentro del sistema.

Descripción del riesgo:

Alteración, manipulación o divulgación de información sensible por fallas en la limitación del acceso a la información, a los sistemas informáticos e instalaciones de procesamiento de información.

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO	CÓDIGO: EV-EG-F-03-01
		VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN	PÁGINA: 64 DE 70
		FECHA: 03/05/2021

Descripción del impacto:

- Pérdida de la disponibilidad de los recursos informáticos
- Propensión a ataques informáticos
- Denegación de servicios por abuso de autoridad sobre los recursos informáticos.
- Errores de autenticación.
- Fuga de información sensible.

Recomendaciones:

- Ajustar la política de control de acceso.
- Revisar el proceso para la gestión y la identificación de los usuarios.
- Deshabilitar o retirar inmediatamente las identificaciones de los usuarios que han dejado la Subred, y los que se encuentran en situaciones administrativas (vacaciones, licencias, incapacidad)
- Revisar la asignación de derechos de acceso privilegiado a través de un proceso de autorización formal de acuerdo con la política de control de acceso

Hallazgo No. 13

Desactualización de los procedimientos e inexistencia de esquemas de Backup sobre activos de información altamente críticos como son las bases de datos de sistemas en producción.

Posibles causas identificadas por la Oficina de Control Interno:

- Falta de recursos tecnológicos para la ejecución de Backups
- Falta de procedimientos e instructivos claros para la ejecución de Backups.
- Falta de controles efectivos que permitan hacer seguimiento sobre la ejecución y calidad de las copias de seguridad.
- Falla en la política de copias de seguridad.

Descripción del riesgo:

Desastre informático de consecuencias catastróficas por la falta de implementación de procedimientos y esquemas de backups sobre las bases de datos de activos de información de misión crítica.

Descripción del impacto:

- Caos y pérdidas económicas incalculables.
- Pérdida económica por la destinación de recursos en la recuperación de la información.
- Pérdida reputacional y pérdida de confianza

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO	CÓDIGO: EV-EG-F-03-01
		VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN	PÁGINA: 65 DE 70
		FECHA: 03/05/2021

- Impacto legal por la pérdida de información clasificada como privada reservada
- Sanciones económicas por parte de terceros dueños de la información
- Sanciones legales por parte de las autoridades regulatorias, de vigilancia y control
- Pérdida de capacidad productiva.

Recomendaciones:

- Adquirir las herramientas necesarias para la toma y almacenamiento de copias de seguridad y recuperación de las mismas.
- Actualizar e implementar los procedimientos e instructivos de copias de seguridad.
- Asignar responsabilidades sobre los custodios de las bases de datos.
- Estudiar la estrategia de alojamiento en la nube con el fin de hacer una transferencia del riesgo a terceros

Hallazgo No. 14

No se cuenta con un plan de concienciación enmarcado dentro de un proceso de mejora continua del SGSI, que dé cuenta del avance efectivo y de la importancia sobre la seguridad de la información en la Subred.

Posibles causas identificadas por la Oficina de Control Interno:

- Falla en la organización y ejecución del plan de seguridad y privacidad de la información.
- Falta de personal especializado y equipo de seguridad
- Falta definición de roles y funciones de seguridad
- Falla en la aplicación de políticas.
- Mecanismos de capacitación insuficiente o poco eficiente sobre seguridad de la información.

Descripción del riesgo:

La falta de una cultura de seguridad de la información en la Subred, facilita la pérdida de integridad, disponibilidad y confidencialidad de los activos de información, ya sea por errores y/o desconocimiento de funcionarios y colaboradores, o por la explotación de dicha vulnerabilidad por parte de delincuentes informáticos.

Descripción del impacto:

- Pérdida económica causada por reprocesos y recuperación de información
- Daño reputacional por la pérdida de confianza de terceras partes
- Daño legal por compromiso de información clasificada reservada y/o privada.

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO	CÓDIGO: EV-EG-F-03-01
		VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN	PÁGINA: 66 DE 70
		FECHA: 03/05/2021

Recomendaciones:

- Establecer planes y mecanismos para la toma de conciencia que contribuyan con la formación y el desarrollo de funcionarios y colaboradores de la subred.
- identificar las principales amenazas de seguridad de la información que involucra a las personas y el efecto sobre las mismas.
- Identificar patrones de comportamiento en donde las personas se vuelven vulnerables frente a amenazas de delitos informáticos.
- Fomentar la cultura del autocontrol en funcionarios y colaboradores de la Subred, relacionada con Seguridad de la Información, convirtiéndola en una práctica del día a día.
- Identificar desde la ingeniería social, técnicas de persuasión inversa, para que contribuyan en la toma de conciencia del personal frente a la seguridad de la información.

Hallazgo No. 15

La mayoría de centros de cableado y cuartos de comunicaciones presentan riesgo de pérdida en la disponibilidad y confidencialidad de la información, toda vez que existen deficiencias en cuanto a su restricción de acceso, organización interna de los dispositivos, documentación, planos, certificación y demás condiciones físicas.

Posibles causas identificadas por la Oficina de Control Interno:

- Falta de planes de mantenimiento preventivo y/o correctivo.
- Falta de recursos técnicos y financieros.
- Falta de personal técnico para atención de los incidentes.
- Falta de documentación en los activos de información (centros de cableado)
- Falta de coordinación entre Tics e Ingeniería.
- Falta de condiciones de seguridad que impidan el acceso a los centros de cableado, tales como: (Avisos disuasivos y restrictivos, cerraduras de seguridad, etc.)

Descripción del riesgo:

Pérdida en la disponibilidad y confidencialidad de la información, por fallas en la seguridad física, restricción de acceso, organización interna de los dispositivos, documentación, planos, certificación y demás condiciones físicas.

Descripción del impacto:

- Económico por daño permanente de los equipos.
- Reputacional por fuga de información

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO	CÓDIGO: EV-EG-F-03-01
		VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN	PÁGINA: 67 DE 70
		FECHA: 03/05/2021

- Fallas en la disponibilidad de los servicios informáticos en caso de daños de equipos de interconexión y componentes activos de las redes.
- Económico por Incremento en gastos de reparación de equipos
- Reputacional por insatisfacción de usuarios.

Recomendaciones:

- Establecer y ejecutar planes de mantenimiento preventivo y correctivo.
- Coordinar con el área de mantenimiento de instalaciones, el mejoramiento y la seguridad de los cuartos de comunicaciones.
- Elaborar y ejecutar proyectos de mejora de infraestructura de redes y comunicaciones.
- Implementar medidas de seguridad y acceso a los cuartos de comunicaciones.

8. CONCLUSIONES

- Con relación al Índice de Desempeño Institucional (IDI) 2021, la Subred presenta una sobrevaloración en FURAG de las políticas de Gobierno Digital (85.9) y Seguridad y Privacidad de la Información (80.4). Esta auditoría evidenció que gran parte de las respuestas entregadas no cuentan con la totalidad de los requisitos técnicos relacionados con el objetivo de la pregunta. En este sentido es importante que tanto los líderes de política como la primera y segunda línea de defensa, realicen una evaluación y análisis al nivel de implementación de las políticas, teniendo en cuenta las recomendaciones de mejora dadas por la medición del FURAG.
- Teniendo en cuenta la tabla de evaluación de efectividad de los controles y de acuerdo con el estándar ISO 27001, se puede evidenciar que la Subred Norte se encuentra en un estado INICIAL, dicho estado hace referencia principalmente a que **no hay procesos estandarizados**, que los procedimientos están documentados, **pero no se aplican y/o están desactualizados**. No obstante, se ha logrado avanzar en ciertos grupos de controles que se encuentran en estado REPETIBLE, lo cual indica que existen controles y procedimientos, pero estos no han sido comunicados y la seguridad se basa en los conocimientos y experticia de quienes ejecutan los controles.
- La documentación en la que se basa el proceso se encuentra desactualizada, principalmente la caracterización que es la guía para la adecuada gestión de las

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO	CÓDIGO: EV-EG-F-03-01
		VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN	PÁGINA: 68 DE 70
		FECHA: 03/05/2021

actividades, generando reprocesos y/o desaprovechamiento de recursos por parte de los colaboradores del proceso.

- Con la exposición a ataques informáticos sobre equipos de cómputo y servidores causada por malware, más la falta de esquemas y controles de backup sobre activos de información de bases de datos de sistemas de misión crítica, la Subred corre con un altísimo riesgo de experimentar un desastre informático de consecuencias catastróficas.
- La oficina de control interno evaluó el diseño y efectividad de los controles internos en las diferentes etapas del proceso de Sistemas de información y Tic's, evidenciándose debilidades en las actividades de control de acuerdo a lo recomendado por la metodología del DAFP, al no describir claramente el propósito y las acciones a tomar en cuanto se presenten desviaciones que puedan impactar al proceso.
- La Subred Norte, en el proceso de gestión de la información y TICs en términos generales, presenta debilidades en el cumplimiento de los lineamientos y requisitos de seguimiento y controles que tiene establecidos en el mapa de riesgos y la normatividad. Teniendo en cuenta los hallazgos y oportunidades de mejora evidenciadas, es necesario que se tomen acciones correctivas con el propósito de reducir los riesgos que puedan impactar el proceso.

FORTALEZAS

- Es importante destacar que algunos centros de cableado presentan condiciones aceptables de organización y estado físico como en el caso de la UMHES de Engativá y el laboratorio en Simón Bolívar.
- A pesar del reducido número de funcionarios en el proceso de Gestión de la Información y TIC's, se han estructurado y presentado algunos instrumentos en aras de llevar control de la gestión, buscar mejorar los servicios tecnológicos y avanzar en la implementación del Modelo Integrado de Planeación y Gestión.
- Se resalta el trabajo realizado por la oficina de sistemas de información y TIC's con la búsqueda de estrategias para la reducción del consumo de papel y el seguimiento a las impresiones que realizan las dependencias de la subred, según se pudo evidenciar el valor de la factura por concepto de impresiones a partir de Julio ha venido reduciéndose notablemente.

	INFORME FINAL AUDITORIAS DE CONTROL INTERNO	CÓDIGO: EV-EG-F-03-01
		VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN	PÁGINA: 69 DE 70
		FECHA: 03/05/2021

OPORTUNIDADES DE MEJORA

- Realizar un análisis para determinar una solución que respalde la actual infraestructura tecnológica y software de gestión de backup, que le permita a la Subred, la recuperación ante desastres y continuidad de la operación.
- Mejorar las competencias técnicas de los funcionarios de primera línea de defensa que dan respuesta a la evaluación FURAG. Adicionalmente, que la segunda línea de defensa y/o el dueño de la política realice la revisión de la totalidad de la información antes de ser enviada.
- Mejorar la comunicación y coordinación con el proceso de activos fijos e infraestructura, en cuanto a labores compartidas de traslado de equipos de cómputo sin registro oportuno y mantenimiento de cuartos de cableado.
- Realizar un análisis de integración entre el sistema de gestión de calidad y el sistema de gestión de seguridad de la información que apoye efectivamente al Sistema Único de Acreditación en Salud SUA.
- Reforzar las acciones tendientes a lograr el mapeo y la generación del documento de las necesidades de tecnologías de información y comunicaciones de la Subred Norte, para el 100% de las unidades de servicios de salud de la subred y así dar cumplimiento a la 4ta. meta del POA.
- Mejorar la documentación que soporta el MSPI con el fin de lograr el enfoque requerido por el Sistema de Gestión de Seguridad de la Información.
- Para la implementación del MSPI, se sugiere que los roles y responsabilidades asignadas de cada perfil, sean incorporados en los manuales de funciones de la entidad, de acuerdo al cargo desempeñado.
- Actualizar la documentación que se considere necesaria para el desarrollo del proceso Gestión de la información y TICs, incorporando puntos de control, responsables e indicadores, teniendo en cuenta las debilidades identificadas, y de conformidad con las directrices, lineamientos, componentes, habilitadores y dominios del Modelo de Gestión y Gobierno TI.

	INFORME FINAL		CÓDIGO: EV-EG-F-03-01
	AUDITORIAS DE CONTROL INTERNO		VERSIÓN :1
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E EVALUACIÓN DE GESTIÓN		PÁGINA: 70 DE 70
			FECHA: 03/05/2021

- Gestionar oportunamente incidentes de Seguridad de la Información que impacten negativamente en las operaciones de la Subred, con cabal cumplimiento de los procedimientos de reporte, análisis, contención, aprendizaje y mejora de los controles.

SOLICITUD DE PLAN DE MEJORAMIENTO

De acuerdo con lo establecido en el instructivo EV-EG-I-01-01 "Seguimiento a Planes de Mejora de Auditorías Internas" de mayo de 2021 el líder de proceso auditado, Directores, Jefes de Oficina, y/o asesores de procesos involucrados en las áreas involucradas deberán, para cada uno de los hallazgos reportados, concertar, elaborar y diligenciar el formato ES-GC-F-10-04 "Plan de mejoramiento institucional" en los campos correspondientes (identificación causa principal del Hallazgo, Acciones de mejora, persona responsable de la acción, fechas de inicio y finalización de la acción) dentro de los 5 días hábiles siguientes a la recepción del informe final de la auditoría. Las acciones plasmadas en el formato deberán tener como objetivo la eliminación y/o mitigación de las causas de los hallazgos.

Los resultados de la auditoría fueron socializados el 21 de noviembre con el acta 08 de 2022 la cual forma parte de los papeles de trabajo.

ANEXOS

Anexo No. 1 Resumen análisis de controles de riesgos

Anexo No. 2 Detalle evaluación de controles - ISO 27001:2013 Anexo A

Anexo No. 3 Visita de campo a los puntos y evaluación de los controles

Anexo No. 4 Detalle de evaluación Política de Gobierno Digital FURAG 2021


LUIS ANTONIO RODRIGUEZ OROZCO
Jefe Oficina de Control Interno


OSCAR IVAN VERGARA MEDINA
Profesional Universitario. Control interno


LUIS ANTONIO TRISTANCHO ROBLES
Profesional Universitario. Control interno

PROC	RIESGOS	No. DEL RIESGO	ANALISIS RIESGO OFICINA CONTROL INTERNO	CAUSAS	ANALISIS DE LA CAUSA DEL RIESGO OFICINA CONTROL INTERNO	CONTROLES EXISTENTES/MEDIDA DE MITIGACIÓN	SOPORTE	ANALISIS DEL CONTROL OFICINA CONTROL INTERNO	ANALISIS DEL CONTENIDO DE LOS CONTROLES OFICINA CONTROL INTERNO	INDICADOR	ANALISIS INDICADOR OFICINA CONTROL INTERNO	META	ANALISIS DE LA META OFICINA CONTROL INTERNO
APOYO Gestión de la información -TICS	Fallas en las aplicaciones o sistemas de información que apoyen los procesos de la Subred.	R1	La definición del riesgo se considera inadecuada es muy general porque no especifica que tipos de fallas e impactos pueden presentarse, para así poder implementar acciones mas acordes y efectivas para evitar su materialización, mas bien podría relacionarse con una causa de un riesgo de pérdida de información o falta de integridad de la misma.	Infraestructura insuficiente u obsoleta.	La causa esta relacionada con el riesgo frente a las aplicaciones obsoletas con las que cuenta la entidad y que pueden producir las fallas	El profesional asignado elabora anualmente el plan y cronograma de mantenimientos para revisión y aprobación por parte del Jefe de la Oficina y su correspondiente ejecución por parte del personal técnico de forma semestral	Plan y cronograma de mantenimiento	El control como esta definido no esta atacando directamente a la causa del riesgo, se debe revisar a durante los mantenimientos se evalua la obsolescencia de la infraestructura y si la cantidad de equipos es suficiente para brindar el apoyo necesario a los procesos, estas variables hacen que el control no sea efectivo en su totalidad.	Durante la verificación de la redacción del control se puede evidenciar que no hay un responsable claro, no se especifica el proposito claramente , ni tampoco se tiene evidencia de que se hace cuando hay variaciones en el control o simplemente no se esta cumpliendo con el coronograma o si hay planes de contingencia.	Numero de equipos con mantenimiento / Total de equipos*100	la formula del indicador muestra el porcentaje de cubrimiento del mantenimiento de los equipos de la subred, sin embargo no se puede determinar con esta formula cual es el cumplimiento o seguimiento del cronograma de mantenimiento.	90 % equipos con mantenimiento realizado	El porcentaje de meta que se tiene es aceptable, sin embargo es importante revisar si se esta cumpliendo efectivamente y si se realizó seguimiento al cumplimiento real del cronograma.
				Mantenimiento insuficiente instalación fallida de los medios de procesamiento de información (Computadores).	La causa es pertinente con la posible materialización del riesgo.	El profesional responsable de la administración del Sistema de Información Servinte realiza el reporte en la mesa de servicios de Carvajal SAS sobre los problemas presentados en el normal funcionamiento de este.	Registro en mesa de ayuda Servis Servinte	El control esta enfocado solo atoseguimiento de fallas en el aplicativo de servinte , pero no esta relacionado con a causa mencionada fallas en otros aplicativos relacionados con los medios de procesamiento de información y/o otros aplicativos que se tiene en la institución.	Durante la verificación de la redacción del control se puede evidenciar que, no se especifica la frecuencia del control, el proposito de su realización, ni se tiene evidencia que se hace cuando hay variaciones en el control o el procedimiento que se sigue con los casos abiertos sin solución por parte del proveedor.	Numero de incidencias efectivamente gestionadas / número de incidencias reportadas por la Subred.	El indicador esta definido adecuadamente para el seguimiento del control sin embargo como el control no mitiga completamente la causa no se considera efectiva la medición	Solución del 90% de las solicitudes interpuestas por la Subred.	* La programación de la meta es poco retadora, porque si bien es cierto que se solicita un alto porcentaje de cumplimiento deberia ser del 100% porque si los fallos en el programa no se solucionan completamente se pueden presentar inconvenientes en la gestion de apoyo que debe garantizar el proceso de Sitemas y TICS a las demas áreas de la institución.
				Mantenimiento insuficiente instalación fallida de los medios de procesamiento de información (Computadores). -- Fallas en software y hardware	La causa es pertinente con la posible materialización del riesgo.	El profesional realiza la verificación de la falla presentada tanto en software o hardware y a través del aplicativo de mesa de ayuda realiza el registro para la asignación al tecnico del area el cual realiza la revisión y brinda la respectiva solución	Registro en mesa de ayuda	El control esta bien definido según la causa a la que se requiere reducir	Durante la verificación de la redacción del control se puede evidenciar que no hay un responsable claro del control , no se especifica la frecuencia de realización, además que se hace cuando hay variaciones en el control o el procedimiento que se desarrolla con los casos que no son solucionados efectivamente dentro del tiempo adecuado.	Numero de incidencias efectivamente gestionadas / número de incidencias recibidas	El indicador esta definido adecuadamente para el seguimiento del control sin embargo como el control no mitiga completamente la causa no se considera efectiva la medición	Responder el 90% de los requerimientos de soporte técnico	* La programación de la meta es poco retadora, porque si bien es cierto que se solicita un alto porcentaje de cumplimiento deberia ser del 100% porque si los fallos en el programa no se solucionan completamente se pueden presentar inconvenientes en la gestion de apoyo que debe garantizar el proceso de Sitemas y TICS a las demas áreas de la institución.
	Uso inadecuado de los activos de información (tipo servicios, hardware, software, talento humano, información física y digital)	R2	Aunque esto puede ser un riesgo podría plantearse de otra manera para identificar posibles riesgos mas globales o impactos que pueden presentarse por esta situación que mas parece una causa que un riesgo mayor como Fugas o perdidas de información, posibles actos de corrupción por divulgación de información confidencial	Falta de sensibilización en el uso adecuado de los activos de información.	La causa es pertinente con la posible materialización del riesgo.	El profesional del area de sistemas diseña semestralmente estrategias para incentivar el uso y la apropiación de las Tics de la Subred Norte ESE.	Estrategias diseñadas	El control esta bien definido según la causa a la que se requiere reducir, sin embargo es importante identificar la manera como se medirá la efectividad del control.	Durante la verificación de la redacción del control se puede evidenciar que no hay un responsable claro, no se tiene evidencia de que se hace cuando hay variaciones en el control o no se identifica si se hace un seguimiento a la estrategia o si se mide la adherencia de la estrategia.	Total de estrategias implementadas/ Total de estrategias diseñadas	El indicador tiene una formulación basica y efectiva , sin embargo para poder tener éxito en la mitigación del riesgo se deberia incorporar una medida de seguimiento o de adherencia de las estrategias para asi asegurar su efectividad	1 estrategia diseñada por semestre.	El cumplimiento de la meta es poco retadora, para poder tener éxito en la mitigación del riesgo se deberia incorporar una meta especifica de seguimiento o de adherencia de las estrategias para asi asegurar su efectividad
				Capacitaciones para incentivar el uso y la apropiación de TIC	La causa es pertinente con la posible materialización del riesgo.	El area de comunicaciones realiza mensual la publicacion de las piezas comunicativas diseñadas junto con el area de sistemas relacionadas con el uso de los activos de informacion con que cuenta la Subred Norte ESE.	Piezas comunicativas Registro del despliegue	El control está bien definido según la causa a la que se requiere reducir, sin embargo es importante identificar la manera como se medirá la efectividad del control.	Durante la verificación de la redacción del control se puede evidenciar que no hay un responsable claro del control, no se especifica la frecuencia de realización, además que se hace cuando hay variaciones en el control o el procedimiento que se desarrolla con los casos que no son solucionados efectivamente dentro del tiempo adecuado.	Publicaciones realizadas/ total de piezas comunicativas elaboradas	El indicador tiene una formulación basica y efectiva , sin embargo para poder tener éxito en la mitigación del riesgo se deberia incorporar una medida de seguimiento o de adherencia de las campañas o piezas publicadas para evaluar la efectividad	1 publicacion realizada por semestre	El cumplimiento de la meta es poco retadora, para poder tener éxito en la mitigación del riesgo se deberia incorporar una meta especifica de seguimiento o de adherencia de las campañas o piezas informativas para asegurar la efectividad de estos medios.
	Daño en equipos informáticos (equipos de cómputo, servidores, equipos de comunicaciones , seguridad)	R3	Aunque esto puede ser un riesgo podría plantearse de otra manera para identificar posibles riesgos mas globales o impactos que pueden presentarse por el daño en los equipos de computo, servidores y demas equipos de tecnologicos.	Conexión de equipos a corriente no regulada	La causa es pertinente con la posible materialización del riesgo.	El profesional universitario designa semestralmente el personal tecnico a realizar la verificación de que los equipos de cómputo, servidores, equipos de comunicaciones, seguridad se encuentren a la red regulada	Inventario	El control está bien definido según la causa a la que se requiere reducir, sin embargo es anecdótico porque se observa que los soportes del control no de fácil obtención porque durante las verificaciones se pueden presentar muchas desviaciones.	Durante la verificación de la redacción del control se puede evidenciar que no hay un responsable claro del control , no se identifica que se hace cuando hay variaciones en el control o el procedimiento que se desarrolla con los casos en que se encuentran equipos fuera de la red regulada.	Numero de equipos no conectados a la red regulada / total de equipos	la formula del indicador muestra el porcentaje de cubrimiento de las revisiones realizadas a los equipos de la subred.	90 % del total de los equipos conectado a la red regulada.	El porcentaje de meta que se tiene es aceptable, sin embargo es importante revisar si se esta cumpliendo efectivamente y si se realizó seguimiento al cumplimiento en los equipos que no estan conectados correctamente.
				Equipos si mantenimiento preventivo	La causa es pertinente con la posible materialización del riesgo.	Profesional Universitario entrega semestralmente el cronograma de mantenimiento preventivo de los equipos de computo al personal tecnico de la Subred por sedes para su correspondiente ejecución y diligenciamiento de los formatos respectivos.	Cronograma de mantenimientos Formato elaboracion mantenimientos	El control como está definido está atacando directamente a la causa del riesgo, se debe revisar los punto de control que se realizan durante los mantenimientos preventivos para garantizar que se esta mitigando el riesgo.	Durante la verificación de la redacción del control se puede evidenciar que no hay un responsable claro, ni tampoco se tiene evidencia de que se hace cuando hay variaciones en el control o simplemente no se esta cumpliendo con el coronograma o si hay planes de contingencia.	Numero de equipos con mantenimiento / Total de equipos*100	la formula del indicador muestra el porcentaje de cubrimiento del mantenimiento de los equipos de la subred, sin embargo no se puede determinar con esta formula cual es el cumplimiento o seguimiento del cronograma de mantenimiento.	90 % equipos con mantenimiento realizado	El porcentaje de meta que se tiene es aceptable, sin embargo es importante revisar si se esta cumpliendo efectivamente y si se realizó seguimiento al cumplimiento real del cronograma.

PROC	RIESGOS	No. DEL RIESGO	ANALISIS RIESGO OFICINA CONTROL INTERNO	CAUSAS	ANALISIS DE LA CAUSA DEL RIESGO OFICINA CONTROL INTERNO	CONTROLES EXISTENTES/MEDIDA DE MITIGACIÓN	SOPORTE	ANALISIS DEL CONTROL OFICINA CONTROL INTERNO	ANALISIS DEL CONTENIDO DE LOS CONTROLES OFICINA CONTROL INTERNO	INDICADOR	ANALISIS INDICADOR OFICINA CONTROL INTERNO	META	ANALISIS DE LA META OFICINA CONTROL INTERNO
APOYO Gestión de la información -TICS	Fuga, alteración, divulgación o pérdida de la información generada por cada uno de los procesos.	R4	Si se puede considerar como un riesgo, sin embargo hay que dar claridad sobre que tipo de información hay que controlar porque hay información publica que no sería necesario controlar su fuga.	Falta de capacitación en seguridad y privacidad de la información	Aunque la falta de conocimiento en seguridad y privacidad de la información puede aportar al riesgo, no necesariamente teniendo personal capacitado se garantiza que no se presente el riesgo, se requiere identificar las amenazas reales a la información que debe protegerse para tomar medidas claras.	El profesional del area de sistemas realiza anualmente la actualización del documento AP-GI-PL-02-01-PLAN+DE+GESTIÓN++DE+SEGURIDAD+DE+LA+INFORMACIÓN y diseña las estrategias para su socialización	Documento de Gestión de Seguridad de la Información	El control debe estar acompañado de una serie de actividades de seguimiento al plan para reducir las posibles falencias que se presenten, no basta con publicar el plan y socializarlo al interior de la empresa.	Durante la verificación de la redacción del control se puede evidenciar que no hay un responsable claro, ni tampoco se tiene evidencia de que se hace cuando hay variaciones en el control o si se realiza seguimiento al cumplimiento del plan.	Plan de gestión de seguridad de la información.	El indicador no esta directamente relacionado con la causa, porque si la causa es falta de capacitación debería es medirse es la adherencia del plan y/ o cantidad de personas capacitadas en seguridad y privacidad de la información.	Plan de seguridad de la información	la meta no es retardadora, como se menciona si el indicador no esta bien diseñado porque no ataca la causa directamente, la meta no esta alineada con el objetivo de reducir la causa del riesgo , debería esta enfocada a un porcentaje de adherencia del plan o de numero de personas efectivamente capacitadas en la seguridad y privacidad de la información.
				No contar con controles adecuados para proteger la información	La presencia de esta causa efectivamente puede permitir la materialización del riesgo, pero debería ser mas especifica en la clase de controles que son considerados como adecuados para conservar la información o describir amenazas claras que puedan colaborar para la materialización del riesgo.	El profesional del area de sistemas realiza anualmente la actualización del documento AP-GI-03-01-INSTRUCTIVO+GENERACIÓN+COPIAS+DE+SEGURIDAD+(BACKUPS)	Documento de generación de copias de seguridad	El control debe estar acompañado de una serie de actividades de seguimiento a la generación de las copias de seguridad, sin embargo esto solo esta atacando la posibilidad de perdida de información , pero no ayuda a controlar la fuga o divulgación de información que debe ser controlada. No basta con actualizar el documento debe haber un plan de seguimiento de la generación de las copias de seguridad y demas controles al interior de la empresa.	Durante la verificación de la redacción del control se puede evidenciar que no hay un responsable claro, ni tampoco se tiene evidencia de que se hace cuando hay variaciones en el control o si se realiza seguimiento al cumplimiento la generación de las copias de seguridad.	Instructivo generacion copias de seguridad	El indicador no esta directamente relacionado con la causa, porque si la causa es falta de controles debería es medirse es seguimiento y cumplimiento de la generación de las copias de seguridad entre otros controles para evitar la fuga, o divulgación de información controlada.	Instructivo generacion copias de seguridad	la meta no es retardadora, Debido a que el indicador no esta bien diseñado porque no ataca completamente la causa, la meta debería estar alineada al seguimiento de las copias de seguridad y de implementación de controles para reducir el riesgo en la seguridad y privacidad de la información.
				No aplicación correcta del procedimiento para la generación de respaldos.	La causa es pertinente con la posible materialización del riesgo.	El profesional del area de sistemas diseña semestralmente estrategias relacionadas con seguridad y uso adecuado de la información de la Subred Norte ESE.	Estrategias diseñadas	El control esta bien definido según la causa a la que se requiere reducir, sin embargo es importante identificar la manera como se medirá la efectividad del control.	Durante la verificación de la redacción del control se puede evidenciar que no hay un responsable claro, no se tiene evidencia de que se hace cuando hay variaciones en el control o no se identifica si se hace un seguimiento a la estrategia o si se mide la adherencia de la estrategia.	Total de estrategias implementadas/ Total de estrategias diseñadas	El indicador tiene una formulación basica y efectiva , sin embargo para poder tener éxito en la mitigación del riesgo se debería incorporar una medida de seguimiento o de adherencia de las estrategias para asi asegurar su efectividad	1 estrategia diseñada por semestre.	El cumplimiento de la meta es poco retardadora, para poder tener éxito en la mitigación del riesgo se debería incorporar una meta especifica de seguimiento o de adherencia de las estrategias para asi asegurar su efectividad
	Software obsoleto o no licenciado.	R5	No es un riesgo es una causa posible de un riesgo que puede ser de multas, calculo o estadísticas erradas o incumplimiento de servicios	No existencia de soporte ni soporte técnico por parte de la casa matriz	La causa puede considerarse como factor para que se vuelva obsoleto o no se obtenga las licencias requeridas, sin embargo esta causa esta mas relacionada con daños o fallas del software.	El profesional universitario designa anualmente el personal tecnico para la revisión del software instalado en los equipos y desinstalación de software no autorizado ni autorizado por la jefatura del area de sistemas	Listado equipos con software no licenciado	El control no tiene nada que ver con la causa, este control esta mas enfocado a que no se tenga claro el estado y seguimiento del software con el que cuenta la entidad.	Durante la verificación de la redacción del control se puede evidenciar que no hay un responsable claro, ni tampoco se tiene evidencia de que se hace cuando hay variaciones en el control o si se realiza seguimiento al cumplimiento de las condiciones del software instalado.	Equipos con software no licenciado / Total de equipos	El indicador tiene una formulación basica y efectiva para medir el porcentaje de equipos con software no licenciado, sin embargo al no tener relación directa con la causa no esta midiendo el impacto del control, y la mitigación del riesgo.	95% equipos identificados	El porcentaje de meta que se tiene es aceptable, a modo de información para la institución sin embargo el cumplimiento de la meta, no mide realmente el impacto en la disminución de la causa.
				Falta de recursos para suplir el software obsoleto o no licenciado	La causa es pertinente con la posible materialización del riesgo.	El profesional del area de sistemas realiza anualmente el inventario del software obsoleto y se remite relacion a la jefatura de la oficina de sistemas	Inventario equipos con software obsoleto	El control no tiene nada que ver con la causa, debiera estar enfocado a conseguir recursos para reducir el software obsoleto o la falta de licencias, este control como esta definido esta mas enfocado a reconocer y llevar registro de los programas y el seguimiento del software de la subred.	Durante la verificación de la redacción del control se puede evidenciar que no hay un responsable claro, ni tampoco se tiene evidencia de que se hace cuando hay variaciones en el control o si se realiza alguna accion con los programas obsoletos.	Equipos con software obsoleto / Total de equipos	El indicador tiene una formulación basica y efectiva para medir el porcentaje de equipos con software obsoleto, sin embargo al no tener relación directa con la causa no esta midiendo el impacto del control, y la mitigación del riesgo.	95% de equipos identificados con software obsoleto	El porcentaje de meta que se tiene es aceptable, a modo de información para la institución sin embargo el cumplimiento de la meta, no mide realmente el impacto en la disminución de la causa.
				No funcionamiento correcto del software	La causa como esta definida, es mas un impacto o efecto del riesgo, no como como factor para que se vuelva obsoleto el software.	El profesional del area designa anualmente el personal técnico para la realización del inventario de software institucional.	Inventario de software	El control no tiene nada que ver con la causa, debiera estar enfocado a la verificación del funcionamiento de los programas, este control como esta definido esta mas enfocado a reconocer y llevar registro de los programas y el seguimiento del software de la subred.	Durante la verificación de la redacción del control se puede evidenciar que no hay un responsable claro, ni tampoco se tiene evidencia de que se hace cuando hay variaciones en el control o si se realiza acciones sobre los inventarios que son registrados.	Listado de software institucional	El indicador no tiene una formulación clara y no se compara por ejemplo con el inventario de activos fijos para hacer una conciliación e identificar diferencias, adicionalmente no mide la disminución de la causa. Ni hay mitigación del riesgo.	95% del software identificado	El porcentaje de meta que se tiene es aceptable, a modo de información para la institución sin embargo el cumplimiento de la meta, no mide realmente el impacto en la disminución de la causa.

GRUPO CONTROL	TEMA CONTROL	ID_ISO	ITEM_ISO	CRITERIOS PRUEBA	CAL	OBSERVACIÓN OFICINA CONTROL INTERNO
POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Documentación	A.5.1.1	Documento de la política de seguridad y privacidad de la Información	Se debe definir un conjunto de políticas para la seguridad de la información aprobada por la dirección, publicada y comunicada a los empleados y a la partes externas pertinentes	40	El manual de políticas no cumple: La definición de seguridad de la información es muy básica, al igual que los objetivos, no tiene definición de roles y responsabilidades, no se evidencia métrica ni instrumentos de medición de cumplimiento.
		A.5.1.2	Revisión y evaluación	Las políticas para seguridad de la información se deberían revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.	20	No se evidencia la periodicidad de revisión de política No se evidencia revisión y aprobación por la alta Dirección.
ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	Organización Interna	A.6.1.1	Roles y responsabilidades para la seguridad de la información	Se deben definir y asignar todas las responsabilidades de la seguridad de la información	0	No se encuentran definida ni asignadas los roles y responsabilidades de la seguridad de la información
		A.6.1.2	Separación de deberes / tareas	Los deberes y áreas de responsabilidad en conflicto se debe separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.	20	Se evidencia una política de control de Acceso, sin definición de roles ni responsabilidades, ni instrumentos de medición.
		A.6.1.3	Contacto con las autoridades.	Las organizaciones deben tener procedimientos establecidos que especifiquen cuándo y a través de que autoridades se debe contactar a las autoridades (por ejemplo, las encargadas de hacer cumplir la ley, los organismos de reglamentación y las autoridades de supervisión), y cómo se debe reportar de una manera oportuna los incidentes de seguridad de la información identificados (por ejemplo, si se sospecha una violación de la ley)	20	Se evidencia en el documento: AP-GI-I-16-01 un procedimiento de reporte a autoridades, sin embargo no se da cumplimiento.
		A.6.1.4	Contacto con grupos de interés especiales	Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad. Por ejemplo a través de una membresía	20	Se evidencia el registro del jefe de la oficina de Tics en el grupo de seguridad de la información del Distrito.
		A.6.1.5	Seguridad de la información en la gestión de proyectos	La seguridad de la información se debe integrar al(los) método(s) de gestión de proyectos de la organización, para asegurar que los riesgos de seguridad de la información se identifiquen y traten como parte de un proyecto. Esto se aplica generalmente a cualquier proyecto, independientemente de su naturaleza, por ejemplo, un proyecto para un proceso del negocio principal, TI, gestión de instalaciones y otros procesos de soporte.	0	No se evidencia que los objetivos de la seguridad de la información se incluyan en los objetivos y fases de los proyectos, ni la valoración de los riesgos de seguridad de la información.
	Dispositivos Móviles y Teletrabajo	A.6.2.1	Política para dispositivos móviles	Se deberían adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	20	En el manual de políticas de seguridad de la información se presenta la política de dispositivos móviles, no obstante la política no da cumplimiento con los requisitos de: 1) registro de los dispositivos móviles, (2) requisitos de la protección física, (3) restricciones para la instalación de software, (4) requisitos para las versiones de software de dispositivos móviles y para aplicar parches, (5) restricción de la conexión a servicios de información, (6) técnicas criptográficas, (7) protección contra software malicioso, (8) des habilitación remota, borrado o cierre, (9) copias de respaldo, (10) dispositivos móviles de propiedad personal, (11) acuerdos de usuario final

GRUPO CONTROL	TEMA CONTROL	ID_ISO	ITEM_ISO	CRITERIOS PRUEBA	CAL	OBSERVACIÓN OFICINA CONTROL INTERNO
	Dispositivos Móviles y Teletrabajo	A.6.2.2	Teletrabajo	Se deberían implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	20	En el manual de políticas de seguridad de la información se presenta la política de teletrabajo, sin embargo la política no da cuenta con los requisitos de: 1) la seguridad física existente en el sitio del teletrabajo 2) los requisitos de seguridad de las comunicaciones 3) acceso no autorizado a información o a recursos, por parte de terceros. 4) acuerdos de licenciamiento de software 5) protección contra software malicioso. 6) revocación de la autoridad y de los derechos de acceso. 7) dispositivos de propiedad personal.
SEGURIDAD DE LOS RECURSOS HUMANOS	Antes de asumir el empleo	A.7.1.1	Selección e investigación de antecedentes	Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.	20	Se evidencia el procedimiento de TH-P-01-01-PROCEDIMIENTO IDENTIFICACION SELECCION Y RECLUTAMIENTO DEL TALENTO HUMANO, que solo aplica para reclutamiento de empleados de planta.
		A.7.1.2	Términos y condiciones del empleo	Los acuerdos contractuales con empleados y contratistas, deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	20	Se evidencia en contratos para personal contratista, cláusulas de confidencialidad.
	Durante la ejecución del empleo	A.7.2.1	Responsabilidades de la dirección	La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	0	No se evidencia que los contratistas y empleados se encuentren: 1) debidamente informados sobre sus roles y responsabilidades de seguridad de la información y, 2) logren un nivel de toma de conciencia sobre la misma. 3) fortalezcan sus habilidades y reciban capacitación en forma regular. 4) Cuenten con un canal para reporte anónimo de incumplimiento de las políticas o procedimientos de seguridad de la información ("denuncias internas").
		A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	Todos los empleados de la Entidad, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.	20	El documento AP-GI-PL-09-01-PLAN DE COMUNICACIÓN Y DIVULGACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN no muestra: 1) la planeación y el desarrollo campañas de sensibilización de seguridad y privacidad de la información. 2) planes de toma de conciencia y comunicación de las políticas de seguridad y privacidad de la información. 3) sensibilización para nuevos empleados y contratistas. 4) La periodicidad de los programas de toma de conciencia. 5) La medición del avance del plan y el impacto de mismo.
		A.7.2.3	Proceso disciplinario	Se debe contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	0	No se evidencia un proceso disciplinario formal contra funcionarios que hayan cometido una violación a la seguridad de la información.
	Terminación y cambio de empleo	A.7.3.1	Terminación o cambio de responsabilidades de empleo	Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de contrato se deberían definir, comunicar al empleado o contratista y se deberían hacer cumplir.	0	Los acuerdos de confidencialidad sobre los contratos, solo hacen referencia durante la ejecución del contrato, mas no al terminar la relación laboral.

GRUPO CONTROL	TEMA CONTROL	ID_ISO	ITEM_ISO	CRITERIOS PRUEBA	CAL	OBSERVACIÓN OFICINA CONTROL INTERNO
GESTIÓN DE ACTIVOS	Responsabilidad de los activos	A.8.1.1	Inventario de activos	Se deben identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	40	El inventario de activos de información se encuentra desactualizado y no se da cumplimiento con los requerimientos mínimos de la Guía para la Gestión y Clasificación de Activos de Información de MINTIC. Falta incluir el inventario de activos de seguridad de la información.
		A.8.1.2	Propiedad de los activos	Los activos mantenidos en el inventario deben tener un propietario.	20	El documento: AP-GI-O-03-03-Registro de activos de información, no cumple con las especificaciones mínimas de clasificación del activo (custodio, dueño, clasificación sobre integridad, disponibilidad y confidencialidad), además se encuentra desactualizado
		A.8.1.3	Uso aceptable de los activos	Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	20	El manual de políticas no ha sido socializada y no contiene declaración de uso aceptable de los activos de información.
		A.8.1.4	Devolución de activos	Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	20	En el formato TH-F-04-01-FORMATO PAZ Y SALVO, no se evidencia la entrega de los activos de información de los cuales es dueño o custodio. No se evidencia el retiro de accesos a los principales activos de información (correo, erp, software de gestión documental, dominio, etc.) No se evidencia la transferencia de conocimientos cuando el activo de información es una persona.
	Clasificación de información	A.8.2.1	Clasificación de la información	La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	20	Existen dos formatos de registro de activos de información, el primero AP-GI-O-03-03-REGISTRO DE ACTIVOS DE INFORMACIÓN, no cumple con las condiciones de clasificación de integridad, confidencialidad y disponibilidad, custodio, dueño, frecuencia, etc. El segundo AP-GI-F-59-01-REGISTRO DE ACTIVOS DE INFORMACIÓN, se encuentra vacío y no tiene información de dueño ni custodio. No se evidencia procedimiento para la clasificación de los activos de información.
		A.8.2.2	Etiquetado de la información	Se debe contar con procedimientos o manuales de etiquetado de los activos.	20	Se cuenta con procedimiento de etiquetado de activos fijos tipo hardware. No se tiene procedimiento de etiquetado de información
		A.8.2.3	Manejo de activos	Se debe contar con procedimientos o manuales de etiquetado de los activos.	20	Los procedimientos con que cuenta la entidad para manejo, procesamiento, almacenamiento y comunicación de información de conformidad con su clasificación, son limitados y están desactualizados.
	Manejo de medios	A.8.3.1	Gestión de medios removibles	Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de la información almacenada en los medios.	0	No se cuenta con directrices, guías, lineamientos ni procedimientos para la gestión de medios removibles.
		A.8.3.2	Disposición de los medios		0	El documento AP-GI-PL-05-01-PLAN DE DISPOSICIÓN FINAL DE RESIDUOS TECNOLÓGICOS DE TI-RAEE, no contempla procedimientos de borrado seguro.
		A.8.3.3	Transferencia de medios físicos		0	La subred no dispone de directrices para la protección de medios que contienen información durante el transporte.

GRUPO CONTROL	TEMA CONTROL	ID_ISO	ITEM_ISO	CRITERIOS PRUEBA	CAL	OBSERVACIÓN OFICINA CONTROL INTERNO
ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	Continuidad de la seguridad de la información	A.17.1.1	Planificación de la continuidad de la seguridad de la información	La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para garantizar el nivel necesario de continuidad para la seguridad de la información durante una situación adversa.	20	La subred cuenta con el documento AP-GI-PL-04-01 como plan de continuidad del negocio, no obstante para el desarrollo de dicho plan se hace referencia al PETI y en el PETI no se desarrolla el Plan de continuidad. Situación que debe ser contraria, es decir desde el PETI referenciar el desarrollo del plan.
		A.17.1.2	Implementación de la continuidad de la seguridad de la información		0	La entidad no cuenta con: (1) estructura organizacional adecuada para mitigar y responder a un evento contingente. (2) personal formalmente asignado de respuesta a incidentes de seguridad de la información. (3) controles de seguridad de la información implementados.
		A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.		0	No se hacer revisión ni evaluación al plan de continuidad del negocio.
	Redundancias	A.17.2.1	Disponibilidad de instalaciones de procesamiento de información		0	En el plan de continuidad no se define la infraestructura redundante.
CUMPLIMIENTO	Cumplimiento de requisitos legales y contractuales	A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales.	Se deben proteger los registros importantes de una organización de pérdida, destrucción y falsificación, en concordancia con los requerimientos estatutarios, reguladores, contractuales y comerciales.	0	No existe normograma asociado a la seguridad y privacidad de la información
		A.18.1.2	Derechos de propiedad intelectual.		40	No se cuenta con política publicada sobre derechos de propiedad intelectual. La OCI realiza anualmente auditoría sobre derechos de autor y se tiene un plan de mejora vigente sobre el tema.
		A.18.1.3	Protección de registros.		40	Se cuenta con TRD de registros físicos
		A.18.1.4	Protección de los datos y privacidad de la información relacionada con los datos personales.	Se deben asegurar la protección y privacidad de la información personal tal como se requiere en la legislación relevante, las regulaciones y, si fuese aplicable, las cláusulas contractuales.	20	Se cuenta con política de tratamiento de datos personales, no se tiene definidos los responsables, ni los repositorios de datos personales, no se cuenta con registro de consentimientos de tratamiento, no se definen las técnicas de almacenamiento de las bases de datos de datos personales.
		A.18.1.5	Reglamentación de controles criptográficos.		0	No se tiene contemplado en la declaración de controles. No obstante debe contemplarse toda vez que la el principal documento de misionalidad es la historia clinica la cual debe cumplir con reglamentación de controles criptográficos
	Revisiones de seguridad de la información	A.18.2.1	Revisión independiente de la seguridad de la información	La organización en lo posible debe asegurarla revisión independiente de la seguridad de la información	20	Se realiza la verificación a través del furag. Las revisiones independientes son realizadas por la oficina de control interno
		A.18.2.2	Cumplimiento con las políticas y normas de seguridad.	Asegurar el cumplimiento de los sistemas con las políticas y estándares de seguridad organizacional.	0	No se realiza la revisión y medición del estado de las políticas
		A.18.2.3	Revisión de cumplimiento técnico.	Los sistemas de información deben chequearse regularmente para el cumplimiento con los estándares de implementación de la seguridad.	20	Se realizó un trabajo de detección de vulnerabilidades, como ejercicio de cumplimiento. No se evidencia procedimientos de hardening a servidores
RELACIONES CON LOS PROVEEDORES	Revisión de la seguridad con relación a los proveedores tanto de servicios como de tecnología	A.15.1	Seguridad de la información en las relaciones con los proveedores	Asegurar la protección de los activos de la entidad que sean accesibles para los proveedores	20	No se evidencia acuerdos con los proveedores para el tratamiento de riesgos de SI. No se cuenta con procedimiento de borrado seguro ni con política de confidencialidad con los proveedores.
		A.15.2	Gestión de la prestación de servicios de proveedores	Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores	0	No se evidencia despliegue de política de tratamiento y transferencia de datos.

GRUPO CONTROL	TEMA CONTROL	ID_ISO	ITEM_ISO	CRITERIOS PRUEBA	CAL	OBSERVACIÓN OFICINA CONTROL INTERNO
CONTROL DE ACCESO	REQUISITOS DEL NEGOCIO PARA CONTROL DE ACCESO	A.9.1.1	Política de control de acceso	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	20	Se cuenta con declaración de la política de control de acceso. No se evidencia el despliegue.
		A.9.1.2	Acceso a redes y a servicios en red	Se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	0	No se cuenta con procedimiento formal para otorgar los permisos de acceso.
	GESTIÓN DE ACCESO DE USUARIOS	A.9.2.1	Registro y cancelación del registro de usuarios	Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	20	No se cuenta con identificaciones únicas para los usuarios. La inactivación de usuarios que se retiran de la institución no es inmediata.
		A.9.2.2	Suministro de acceso de usuarios	Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.	0	No se cuenta con procedimiento asociado con la asignación y/o revocación de los derechos de acceso.
		A.9.2.3	Gestión de derechos de acceso privilegiado	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.	0	No se cuenta con procedimiento asociado con la asignación y/o revocación de los derechos de acceso.
		A.9.2.4	Gestión de información de autenticación secreta de usuarios	La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	0	No se cuenta con procedimiento asociado con la asignación y/o revocación de los derechos de acceso.
		A.9.2.5	Revisión de los derechos de acceso de usuarios	Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	0	No se realiza la revisión periódica de los derechos de acceso
		A.9.2.6	Retiro o ajuste de los derechos de acceso	Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	20	El formato de paz y salvo no da cuenta de entrega de activos de información. No se retiran los accesos a tiempo en la base de datos.
	RESPONSABILIDADES DE LOS USUARIOS	A.9.3.1	Uso de información de autenticación secreta	Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	20	No se evidencia socialización del documento AP-GI-I-02-02 ni seguimiento al mismo. Las políticas de grupo del directorio activo no tienen incorporadas las exigencias requeridas por el estandar.
	CONTROL DE ACCESO A SISTEMAS Y APLICACIONES	A.9.4.1	Restricción de acceso a la información	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debería restringir de acuerdo con la política de control de acceso.	40	Las herramientas auxiliares no responden a la política de control de acceso. En el directorio activo no se evidencia la inclusión de políticas de rotación de claves, tamaño ni nivel de seguridad.
		A.9.4.2	Procedimiento de ingreso seguro	Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.	20	Las herramientas existentes no aplican la totalidad de las buenas prácticas con relación al control de acceso.
		A.9.4.3	Sistema de gestión de contraseñas	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	20	Las herramientas existentes no aplican la totalidad de las buenas prácticas con relación al control de acceso.
		A.9.4.4	Uso de programas utilitarios privilegiados	Se debe restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.	20	No se cuenta con política y/o restricciones sobre programas utilitarios
		A.9.4.5	Control de acceso a códigos fuente de programas	Se debe restringir el acceso a los códigos fuente de los programas.	0	La subred no tiene un proceso formal de desarrollo

GRUPO CONTROL	TEMA CONTROL	ID_ISO	ITEM_ISO	CRITERIOS PRUEBA	CAL	OBSERVACIÓN OFICINA CONTROL INTERNO
CRYPTOGRAFIA	CONTROLES CRIPTOGRAFICOS	A.10.1.1	Política sobre el uso de controles criptográficos	Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	0	No se tiene política sobre controles criptográficos
		A.10.1.2	Gestión de llaves	Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.	0	No se cuenta con procedimientos de gestión de llaves criptográficas
SEGURIDAD FÍSICA Y DEL ENTORNO	ÁREAS SEGURAS	A.11.1.1	Perímetro de seguridad física	Se debe definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o crítica, e instalaciones de manejo de información.	40	Se cuenta con un area de recepcion y vigilancia para acceso a la edificacion y al area administrativa. Se cuenta con señalización para el centro de computo y cuartos de cableado auxiliar. La seguridad de los centros de cableado es deficiente con exección del datacenter.
		A.11.1.2	Controles físicos de entrada	Las áreas seguras se deben proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.	40	Se cuenta con registro de visitantes al centro de computo principal y acceso biometrico para lo funcionarios.
		A.11.1.3	Seguridad de oficinas, recintos e instalaciones	Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.	40	La seguridad impide el acceso al publico, pero no se identifica al visitante. El datacenter esta rotulado como tal, siendo una mala práctica dado que se identifica como centro de procesamiento de datos.
		A.11.1.4	Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	20	En el datacenter se evidencian elementos de protección contra incendios
		A.11.1.5	Trabajo en áreas seguras	Se debe diseñar y aplicar procedimientos para trabajo en áreas seguras.	0	No se cuenta con directrices de área segura
		A.11.1.6	Áreas de despacho y carga	Se debe controlar los puntos de acceso tales como áreas de despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	20	El area de despacho se encuentra restringido desde el exterior y se cuenta con registro de ingreso al almacen en el sistema de informacion
	EQUIPOS	A.11.2.1	Ubicación y protección de los equipos	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado.	40	Se evidencian directrices de uso seguro de equipos de computo
		A.11.2.2	Servicios de suministro	Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	40	Se evidencian directrices de uso seguro de equipos de computo
		A.11.2.3	Seguridad del cableado	El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información deben estar protegido contra interceptación, interferencia o daño.	20	No se cuentan con certificación de cableado
		A.11.2.4	Mantenimiento de equipos	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	40	Se tiene plan de mantenimiento de equipos de computo. No se cuenta con mabtenimiento de servidores y datacenter.
		A.11.2.5	Retiro de activos	Los equipos, información o software no se deben retirar de su sitio sin autorización previa.	20	Se cuenta con procedimiento de traslado de equipos, sin embargo no se da cumplimiento.
		A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Se debe aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.	0	No se evidencia la aplicación de medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la subred.

GRUPO CONTROL	TEMA CONTROL	ID_ISO	ITEM_ISO	CRITERIOS PRUEBA	CAL	OBSERVACIÓN OFICINA CONTROL INTERNO
SEGURIDAD DE LAS OPERACIONES		A.11.2.7	Disposición segura o reutilización de equipos	Se debe verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reusó.	0	No se evidencian medidas de borrado seguro cuando se dan equipos de baja y/o devolución de arrendamiento.
		A.11.2.8	Equipos de usuario desatendidos	Los usuarios deben asegurarse de que a los equipos desatendidos se les dé protección apropiada.	20	No existen medidas de seguridad documentadas para equipos desatendidos.
		A.11.2.9	Política de escritorio limpio y pantalla limpia	Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.	0	No se evidencian políticas ni medidas de seguridad para escritorio limpio
	PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES	A.12.1.1	Procedimientos de operación documentados	Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesiten.	20	Se evidencian documentos de procedimientos e instructivos se encuentran desactualizados y no dan cuenta de la realidad.
		A.12.1.2	Gestión de cambios	Se debe controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	0	No se cuenta con procedimientos de gestión de cambios para los desarrollos realizados al interior de la subred.
		A.12.1.3	Gestión de capacidad	Para asegurar el desempeño requerido del sistema se debe hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.	20	Se realizan procedimientos de gestión de capacidad en servidores. No obstante no se cuenta con documentación ni programación de actividades
		A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	Se debe separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	20	Aunque en la declaración de aplicabilidad de los controles, se afirma que en la Subred no se realizan desarrollos, se evidencian desarrollos realizados al interior de la subred (mesa de servicios, aplicativo de certidicaciones) sin contar con ambiente de puebas. De la misma manera no se evidencia entrono de puebas para las actualizaciones del sistema Servinte.
	PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS	A.12.2.1	Controles contra códigos maliciosos	Se debe implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	20	Los instructivos de uso de tecnología y las políticas no han sido socializadas. Adicionalmente se materializó el riesgo de pérdida de información por malware, dado el vencimiento del sistema antimalware.
	COPIAS DE RESPALDO	A.12.3.1	Respaldo de la información	Se debe hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.	20	A las copias de respaldo no se hacen pruebas y no se tiene definido un esquema de copias de seguridad.
	REGISTRO Y SEGUIMIENTO	A.12.4.1	Registro de eventos	Se debe elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	20	No se evidencia la revisión de logs de auditoría sobre los sistemas críticos.
		A.12.4.2	Protección de la información de registro	Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	20	No se cuenta con documentación ni controles
		A.12.4.3	Registros del administrador y del operador	Las actividades del administrador y del operador del sistema se debe registrar, y los registros se deben proteger y revisar con regularidad.	20	No se evidencian registros de las actividades de los administradores u operadores del sistema

GRUPO CONTROL	TEMA CONTROL	ID_ISO	ITEM_ISO	CRITERIOS PRUEBA	CAL	OBSERVACIÓN OFICINA CONTROL INTERNO
	CONTROL DE SOFTWARE OPERACIONAL	A.12.4.4	Sincronización de relojes	Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.	20	No se define la fuente de sincronización de servidores.
		A.12.5.1	Instalación de software en sistemas operativos	Se debe implementar procedimientos para controlar la instalación de software en sistemas operativos.	20	No se evidencian las pruebas sobre las actualizaciones.
		A.12.6.1	Gestión de las vulnerabilidades técnicas	Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	0	Sin evidencia sobre los parámetros de la prueba sobre: Gestión de las vulnerabilidades técnicas
		A.12.6.2	Restricciones sobre la instalación de software	Se debe establecer e implementar las reglas para la instalación de software por parte de los usuarios.	40	El instructivo e encuentra desactualizado y falta su socialización.
	AUDITORÍAS DE SISTEMAS DE INFORMACIÓN	A.12.7.1	Controles sobre auditorías de sistemas de información	Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se debe planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	40	La oficina de contro Interno
SEGURIDAD DE LAS COMUNICACIONES	GESTIÓN DE LA SEGURIDAD DE LAS REDES	A.13.1.1	Controles de redes	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	20	Se ejecutan procedimientos y tecnicas de seguridad de redes. No obstante, estos no se encuentran documentados.
		A.13.1.2	Seguridad de los servicios de red	Se debe identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.	20	Se evidencia ANS en los proveedores de servicios de comunicaciones. No se evidencia seguimiento por parte de la Subred.
		A.13.1.3	Separación en las redes	Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	20	No se evidencia segregación de las redes. La red de datos es totalmente plana.
	TRANSFERENCIA DE INFORMACIÓN	A.13.2.1	Políticas y procedimientos de transferencia de información	Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación.	20	El manual de politicas de seguridad, no ha sido socializado y no se mide el cumplimiento de las políticas ni procedimientos y controles de transferencia de información
		A.13.2.2	Acuerdos sobre transferencia de información	Los acuerdos deben tener en cuenta la transferencia segura de información del negocio entre la organización y las partes externas.	0	El manual de politicas de seguridad de la informaión no da cuenta de las trasnferencias seguras de información.
		A.13.2.3	Mensajería electrónica	Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	40	La mensajería de correo electrónico se hace a travez de Outlook, la mensajería instantanea se realiza a travez de whatsapp usando cuentas personales no corporativas.
		A.13.2.4	Acuerdos de confidencialidad o de no divulgación	Se debe identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.	40	Se cuenta con acuerdos de confidencialidad para el personal contratado por OPS con cumplimiento parcial del ciclo de confidencialidad. El personal de planta no tiene determinados acuerdos de confidencialidad.

GRUPO CONTROL	TEMA CONTROL	ID_ISO	ITEM_ISO	CRITERIOS PRUEBA	CAL	OBSERVACIÓN OFICINA CONTROL INTERNO
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN	A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Los requisitos relacionados con seguridad de la información se debe incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	0	Para la adquisición de herramientas de software no se tienen definidos los requisitos de seguridad de la información.
		A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	0	No se cuenta con las directrices para la seguridad de servicios de las aplicaciones en redes públicas.
		A.14.1.3	Protección de transacciones de los servicios de las aplicaciones	La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.	0	No se evidencian directrices protección de transacciones de los servicios de las aplicaciones
	SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE	A.14.2.1	Política de desarrollo seguro	Se debe establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización.	0	No se evidencian las directrices en los desarrollos hechos por la entidad (orfeo, aplicativo de certificación de contratistas, pagina web)
		A.14.2.2	Procedimientos de control de cambios en sistemas	Los cambios a los sistemas dentro del ciclo de vida de desarrollo se debe controlar mediante el uso de procedimientos formales de control de cambios.	0	No se lleva un registro de control de cambios
		A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y ponerlas a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.	0	La entidad no dispone de un procedimiento de despegue de aplicaciones, tampoco dispone de un ambiente de pruebas
		A.14.2.4	Restricciones en los cambios a los paquetes de software	Se deben desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	20	El proceso de actualización de los aplicativos no se documenta y no se miden los riesgos de las actualizaciones fallidas
		A.14.2.5	Principios de construcción de sistemas seguros	Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	0	Sin evidencia sobre los parámetros de la prueba sobre: Principios de construcción de sistemas seguros
		A.14.2.6	Ambiente de desarrollo seguro	Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	0	Los desarrollos realizados al interior de la subred, no están asegurados bajo un ambiente seguro
		A.14.2.7	Desarrollo contratado externamente	La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	0	No se aplican medidas de seguridad sobre desarrollos contratados
		A.14.2.8	Pruebas de seguridad de sistemas	Durante el desarrollo se debe llevar a cabo pruebas de funcionalidad de la seguridad.	0	Sin evidencia sobre los parámetros de la prueba sobre: Pruebas de seguridad de sistemas
		A.14.2.9	Prueba de aceptación de sistemas	Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se debe establecer programas de prueba para aceptación y criterios de aceptación relacionados.	0	Sin evidencia sobre los parámetros de la prueba sobre: Prueba de aceptación de sistemas
	DATOS DE PRUEBA	A.14.3.1	Protección de datos de prueba	Los datos de ensayo se deben seleccionar, proteger y controlar cuidadosamente.	0	Sin evidencia sobre los parámetros de la prueba sobre: Protección de datos de prueba

GRUPO CONTROL	TEMA CONTROL	ID_ISO	ITEM_ISO	CRITERIOS PRUEBA	CAL	OBSERVACIÓN OFICINA CONTROL INTERNO
GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	GESTIÓN DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN	A.16.1.1	Responsabilidades y procedimientos	Se debe establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	0	Sin evidencia sobre los parámetros de la prueba sobre: Responsabilidades y procedimientos
		A.16.1.2	Reporte de eventos de seguridad de la información	Los eventos de seguridad de la información se debe informar a través de los canales de gestión apropiados, tan pronto como sea posible.	20	La entidad desconoce acerca de eventos de seguridad
		A.16.1.3	Reporte de debilidades de seguridad de la información	Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	0	Sin evidencia sobre los parámetros de la prueba sobre: Reporte de debilidades de seguridad de la información
		A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Los eventos de seguridad de la información se debe evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.	0	Sin evidencia sobre los parámetros de la prueba sobre: Evaluación de eventos de seguridad de la información y decisiones sobre ellos
		A.16.1.5	Respuesta a incidentes de seguridad de la información	Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	0	Sin evidencia sobre los parámetros de la prueba sobre: Respuesta a incidentes de seguridad de la información
		A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.	0	Sin evidencia sobre los parámetros de la prueba sobre: Aprendizaje obtenido de los incidentes de seguridad de la información
		A.16.1.7	Recolección de evidencia	La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	0	Sin evidencia sobre los parámetros de la prueba sobre: Recolección de evidencia

ANEXO No. 3 VISITA DE CAMPO A LOS PUNTOS Y EVALUACIÓN DE LOS CONTROLES

Durante la visita a los puntos de servicio se aplicaron 5 Pruebas de recorrido con una lista de chequeo para verificar las condiciones, características y controles de la Red LAN Y WIFI a continuación se muestran las respuestas obtenidas junto con la evidencia fotográfica de cada punto visitado.

CAPS CHAPINERO.

CHECKLIST AUDITORÍA RED LAN Y WIFI			
Nombre:	Checklist Red LAN y WIFI		
Versión	1.0		
INFORMACIÓN DE LA ENTIDAD			
Nombre de la entidad	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E. -- CAPS CHAPINERO		
Nombre de quien diligencia	LUIS ANTONIO TRISTANCHO ROBLES		
Cargo	AUDITOR CONTROL INTERNO	Dependencia	OFICINA DE CONTROL INTERNO
Fecha de diligenciamiento	14/09/2022		
ITEM	SI	NO	OBSERVACIONES OCI
¿Todos los nodos se encuentran bajo un mismo estándar de modo que no se reduzca la velocidad de transmisión?	X		CATEGORIA 6
¿La longitud de los tramos de cableado horizontal no excede de los 90 metros?	X		
¿El armado del patch panel cumple con los requerimientos básicos del estándar 568-A y 568-B?	X		
¿El etiquetado implementado en la organización cuenta con un código de colores para facilitar su identificación?		X	
¿Cuenta con un mapa arquitectónico para la verificación del sembrado de nodos?		X	
¿Cuenta con mapas arquitectónicos de rutas de red para la implementación de un nuevo nodo?		X	
¿Se tiene implementado el protocolo CSMA/CD para un mejor funcionamiento del sistema Ethernet?		X	
¿El cableado estructurado del interior del edificio viaja dentro de canaleta o ducto?		X	
¿Cuenta con dispositivo firewall físico para protección y aseguramiento de la red?	X		FISICO
¿Las direcciones IP'S de los equipos de cómputo son implementadas de forma fija?		X	DHCP, DOMINIO
¿Cuentan con conmutadores en red para la expansión de redes locales?		X	
¿Cuenta con una memoria técnica de direccionamiento ip?		X	
¿El rack donde se colocan los dispositivos cuenta con espacio libre para agregar más dispositivos?		X	SUPERIOR AL 90%
¿Se tiene conexión a tierra física para protección de equipos ante posibles descargas eléctricas que puedan afectar?	X		
¿Cuenta con dispositivos para la regulación del voltaje?	X		UPS 180 KWA X CADA + DACLAMER 20 KWA
¿La topología establecida se puede actualizar de tal manera que no ocurra ninguna anomalía dentro de la red?		X	
¿Se tiene implementado un sistema de control de acceso para los dispositivos?	X		CON CONTRL DE ACCESO A DATACENTER
¿Los equipos se encuentran instalados en áreas con temperaturas adecuadas para su funcionamiento?		X	NO TODOS
¿La empresa posee como mínimo 2 enlaces de Internet y un número igual de direcciones IP Publicas ?	X		
¿Los cables de los equipos se encuentran en buen estado?	X		
¿Esta implementado un modelo de QoS en la red?		X	
¿La red cuenta con los equipos y aplicaciones (IDS,IPS,NIDS)?	X		
¿Existen planes de contingencia y continuidad que garanticen el buen funcionamiento de la red?		X	
¿Se utiliza cable tipo STP en los tramos donde se agrupa con el cableado eléctrico?	X		
¿Las terminaciones del cable de red están correctamente configuradas en base al código de colores de los pares trenzados?	X		
¿Se tienen suficientes nodos en la red para conectar todos los equipos que lo requieren?		X	OCUPACION SUPERIOR AL 90%
¿El cableado pasa por un techo falso o tubería subterránea para mayor protección?		X	
¿Se monitoriza la red para la revisión de errores o situaciones anómalas?	X		
¿Cuenta con un análisis de vulnerabilidades en la implementación y configuración de los dispositivos de red?		X	
¿Los mensajes de transmisión dentro de la red cuentan con el origen, fecha, hora y receptor?		X	
¿Los datos que viajan por internet se encuentran cifrados?		X	
¿La instalación de tierra física esta retirada al menos 5 metros del edificio?			NO SE TUVO RESPUESTA DE INGENIERIA
¿El cableado se encuentra blindado?		X	CATEGORIA 6
¿La entidad genera sus propios ataques para probar la solidez de la red y encontrar posibles fallas?		X	
¿Cuentan con VLAN's para administración en cada una de las oficinas que se dedican a diferente rubro?		X	LA RED ES TOTALMENTE PLANA

CHECKLIST AUDITORÍA RED LAN Y WIFI	
Nombre:	Checklist Red LAN y WIFI
Versión	1.0

INFORMACIÓN DE LA ENTIDAD			
Nombre de la entidad	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E. -- CAPS CHAPINERO		
Nombre de quien diligencia	LUIS ANTONIO TRISTANCHO ROBLES		
Cargo	AUDITOR CONTROL INTERNO	Dependencia	OFICINA DE CONTROL INTERNO
Fecha de diligenciamiento	14/09/2022		

ITEM	SI	NO	OBSERVACIONES OCI
¿Los enlaces de la red se testean frecuentemente?		X	
¿Los Access point cuentan con encriptación?	X		8 ACCES POINT
¿La señal Wifi cubre a las áreas debidas?		X	
¿El ancho de banda de la red inalámbrica es suficiente para soportar el tráfico de datos?		X	
¿Cuenta con un registro de los usuarios que acceden a la red?	X		POLITICAS EN LA CONTROLADORA
¿El acceso a la red WLAN está protegido por WPA2 con AES?	X		AUTENTICACION SE REALIZA POR MAC
¿Los dispositivos Access Point se encuentran en lugares estratégicos considerando la distancia de propagación de señal como lo marca el estándar IEEE 802.11?		X	8AP
¿Se trabajan en diferentes frecuencias de transmisión, como lo marca el estándar IEEE 802.11g?	X		
¿La cantidad de dispositivos Access Point es la adecuada en función del número de usuarios que se conectan, como lo establece el estándar 802.11?		X	8AP
¿La red inalámbrica proporciona velocidades de transmisión de 54Mbps en distancias cortas?	X		
Hay una política para uso aceptable de Wifi		X	
Hay una política para instalación de fuentes de Wifi autorizadas		X	
Hay una política para hardware permitido		X	
Hay un WIDS o un WIPS en la red Wifi	X		SE REALIZA CON EL FIREWALL
La red Wifi esta separada de la red LAN por segmentación		X	
Los Access Point se auditan frecuentemente para verificar la configuración realizada por el administrador		X	
Los usuarios finales están debidamente capacitados en el uso de todas las funciones de seguridad de la WLAN		X	
Las estaciones de trabajo que son clientes de la WLAN, están debidamente protegidas	X		
Los passwords de los Access Point son seguros		X	NO EXISTE POLÍTICA
La configuración predeterminada de los Access Point, ha sido cambiada		X	
Deshabilitar todas las interfaces de administración no utilizadas	X		TODAS ESTAN EN USO
La administración de los Access Point se hace desde una VLAN diferente		X	
No se usa el nombre de la entidad, la dirección, el número de teléfono en el SSID.			PREGUNTAR INGENIERO ALFARO
El SSID no se difunde	X		
La WLAN esta monitoreada y loggeada	X		AUTENTICACION SE REALIZA POR MAC
Hay un tiempo de espera de sesión razonable		X	
Se realizan pruebas de seguridad regularmente a la WLAN		X	

Chapinero - LAN WIFI



En la visita a este punto se encontró que las condiciones del Data Center y su seguridad es buena, se tiene control de ingreso biométrico y las condiciones de ambientes son aceptables.

Para el ingreso al datacenter se cuenta con dispositivo para acceso con huella y código de seguridad, además se tiene el registro de las planillas de ingreso de las personas. Se observa equipo de aire acondicionado de precisión y los Racks de cableado con problemas de ordenamiento.

En esta unidad se encontraron algunas debilidades en cuanto seguridad de accesos a los centros de cableado y de la organización de los Racks, en el área de contratación se encuentra un Rack al cual se tiene acceso sin ninguna restricción por lo que se configura un riesgo de seguridad.

Adicionalmente se observan techos con falta de paneles, cables sueltos y desordenados, debilidades de ventilación y en general las condiciones no son buenas.

UMHES ENGATIVA CALLE 80

CHECKLIST AUDITORÍA RED LAN Y WIFI			
Nombre:	Checklist Red LAN y WIFI		
Versión	1.0		
INFORMACIÓN DE LA ENTIDAD			
Nombre de la entidad	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E. -- UMHES ENGATIVA CALLE 80		
Nombre de quien diligencia	LUIS ANTONIO TRISTANCHO ROBLES		
Cargo	AUDITOR CONTROL INTERNO	Dependencia	OFICINA DE CONTROL INTERNO
Fecha de diligenciamiento	14/09/2022		
ITEM			
¿Cuenta con un mapa arquitectónico para la verificación del sembrado de nodos?	SI	NO	OBSERVACIONES DE OCI
¿Cuenta con mapas arquitectónicos de rutas de red para la implementación de un nuevo nodo?		X	SIN CERTIFICACION DEL CABLEADO
¿Se tiene implementado el protocolo CSMA/CD para un mejor funcionamiento del sistema Ethernet?		X	
¿El cableado estructurado del interior del edificio viaja dentro de canaleta o ducto?	X		
¿Cuenta con dispositivo firewall físico para protección y aseguramiento de la red?	X		
¿Las direcciones IP'S de los equipos de cómputo son implementadas de forma fija?		X	DHCP
¿Cuentan con conmutadores en red para la expansión de redes locales?	X		SE CUENTAN CON 6 CUARTOS DE CABLEADO
¿Cuenta con una memoria técnica de direccionamiento ip?		X	SIN INVENTARIO
¿El rack donde se colocan los dispositivos cuenta con espacio libre para agregar más dispositivos?	X		
¿Se tiene conexión a tierra física para protección de equipos ante posibles descargas eléctricas que puedan afectar?			NO SE TUVO RESPUESTA DE INGENIERIA
¿Cuenta con dispositivos para la regulación del voltaje?	X		UPS 25, 10, 10
¿La topología establecida se puede actualizar de tal manera que no ocurra ninguna anomalía dentro de la red?		X	
¿Se tiene implementado un sistema de control de acceso para los dispositivos?	X		CON CLAVE PERO NO SE REALIZAN CAMBIOS DE ESTA
¿Los equipos se encuentran instalados en áreas con temperaturas adecuadas para su funcionamiento?		X	
¿La empresa posee como mínimo 2 enlaces de Internet y un número igual de direcciones IP Publicas ?	X		3 ENLACES - 2 DE CANAL DEDICADO Y 1 ADSL 190 M
¿Los cables de los equipos se encuentran en buen estado?	X		
¿Esta implementado un modelo de QoS en la red?		X	
¿La red cuenta con los equipos y aplicaciones (IDS,IPS,NIDS)?	X		IMPLEMENTADOS EN FIREWALL FISICO Y SOFTWARE
¿Existen planes de contingencia y continuidad que garanticen el buen funcionamiento de la red?		X	
¿Se utiliza cable tipo STP en los tramos donde se agrupa con el cableado eléctrico?	X		
¿Las terminaciones del cable de red están correctamente configuradas en base al código de colores de los pares trenzados?	X		
¿Se tienen suficientes nodos en la red para conectar todos los equipos que lo requieren?	X		OCUPACION DEL 80%
¿El cableado pasa por un techo falso o tubería subterránea para mayor protección?	X		
¿Se monitoriza la red, para la revisión de errores o situaciones anómalas?	X		
¿Cuenta con un análisis de vulnerabilidades en la implementación y configuración de los dispositivos de red?		X	
¿Los datos que viajan por internet se encuentran cifrados?		X	
¿La instalación de tierra física esta retirada al menos 5 metros del edificio?			NO SE TUVO RESPUESTA DE INGENIERIA
¿El cableado se encuentra blindado?	X		
¿La entidad genera sus propios ataques para probar la solidez de la red y encontrar posibles fallas?		X	
¿Cuentan con VLAN's para administración en cada una de las oficinas que se dedican a diferente rubro?		X	LA RED ES TOTALMENTE PLANA

Engativá calle 80 - LAN WIRED



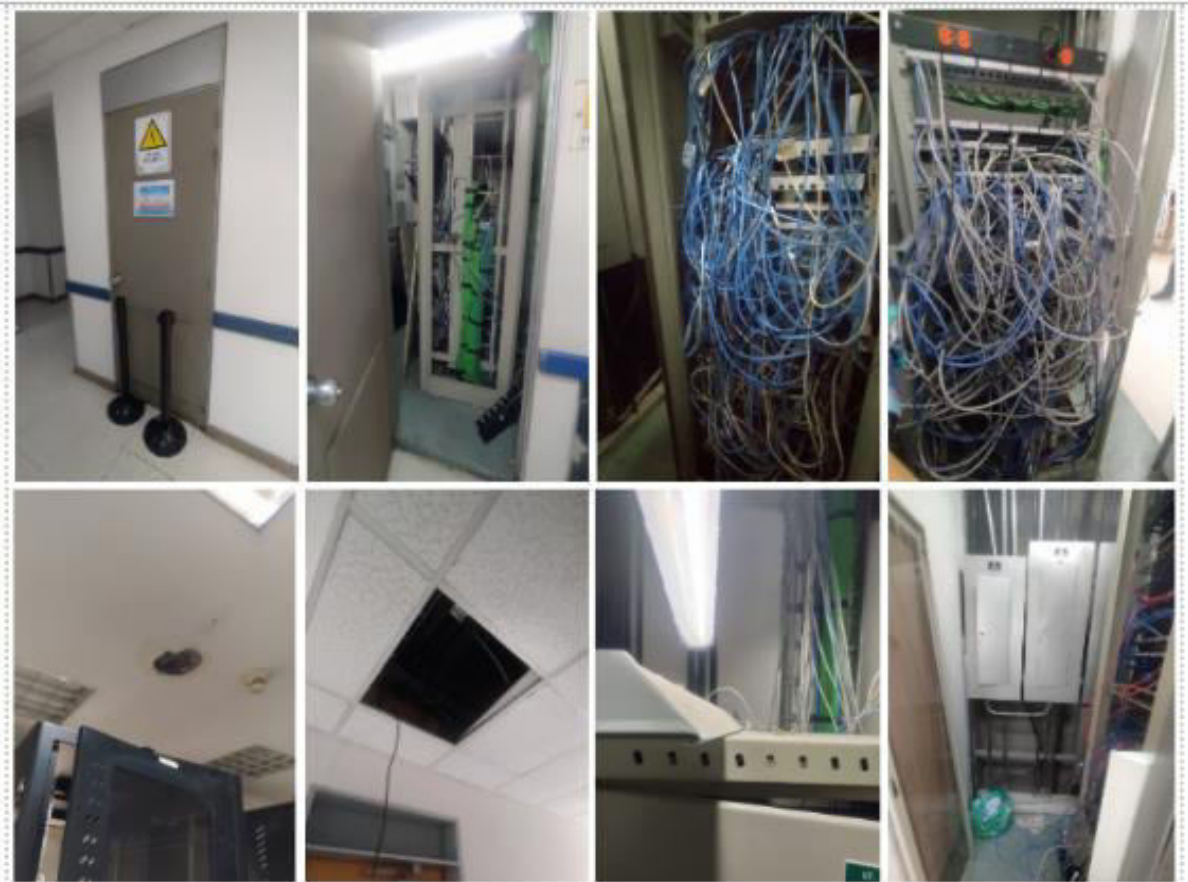
En la verificación de este punto se pudo evidenciar una buena organización del cableado, los cuartos tienen demarcación e identificación visible, sin embargo, se recomienda que se utilicen mensajes de advertencia o de restricción del acceso sin informar a que corresponde o que contiene el cuarto demarcado para evitar el riesgo de intromisiones no deseadas. En algunos de los cuartos se encontraron elementos que no corresponden al centro de cableado, y algunas instalaciones eléctricas a la vista o sin tapas. Se tiene demarcación de los cuartos de cableado con armarios y racks organizados.

UMHES CSE SUBA

CHECKLIST AUDITORÍA RED LAN Y WIFI			
Nombre:	Checklist Red LAN y WIFI		
Versión	1.0		
INFORMACIÓN DE LA ENTIDAD			
Nombre de la entidad	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E. -- UMHES CSE SUBA		
Nombre de quien diligencia	LUIS ANTONIO TRISTANCHO ROBLES		
Cargo	AUDITOR CONTROL INTERNO	Dependencia	OFICINA DE CONTROL INTERNO
Fecha de diligenciamiento	16/09/2022		
ITEM			
		SI	NO
OBSERVACIONES OCI			
¿Todos los nodos se encuentran bajo un mismo estándar de modo que no se reduzca la velocidad de transmisión?			
		X	CAT 6 y 6A, PROBLEMAS CON INFRAESTRUCT
¿La longitud de los tramos de cableado horizontal no excede de los 90 metros?			
		X	
¿El armado del patch panel cumple con los requerimientos básicos del estándar 568-A y 568-B?			
		X	
¿El etiquetado implementado en la organización cuenta con un código de colores para facilitar su identificación?			
		X	
¿Cuenta con un mapa arquitectónico para la verificación del sembrado de nodos?			
		X	
¿Cuenta con mapas arquitectónicos de rutas de red para la implementación de un nuevo nodo?			
		X	
¿Se tiene implementado el protocolo CSMA/CD para un mejor funcionamiento del sistema Ethernet?			
		X	
¿El cableado estructurado del interior del edificio viaja dentro de canaleta o ducto?			
		X	
¿Cuenta con dispositivo firewall físico para protección y aseguramiento de la red?			
		X	
¿Las direcciones IP'S de los equipos de cómputo son implementadas de forma fija?			
		X	
¿Cuentan con conmutadores en red para la expansión de redes locales?			
		X	
¿Cuenta con una memoria técnica de direccionamiento ip?			
		X	
¿El rack donde se colocan los dispositivos cuenta con espacio libre para agregar más dispositivos?			
		X	MAYOR AL 90%
¿Se tiene conexión a tierra física para protección de equipos ante posibles descargas eléctricas que puedan afectar?			
		X	
¿Cuenta con dispositivos para la regulación del voltaje?			
		X	UPS
¿La topología establecida se puede actualizar de tal manera que no ocurra ninguna anomalía dentro de la red?			
		X	
¿Se tiene implementado un sistema de control de acceso para los dispositivos?			
		X	
¿Los equipos se encuentran instalados en áreas con temperaturas adecuadas para su funcionamiento?			
		X	
¿La empresa posee como mínimo 2 enlaces de Internet y un número igual de direcciones IP Publicas ?			
		X	ENLACES REDUNDANTES CON DIFERENTE PROVEEDOR
¿Los cables de los equipos se encuentran en buen estado?			
		X	
¿Esta implementado un modelo de QoS en la red?			
		X	
¿La red cuenta con los equipos y aplicaciones (IDS,IPS,NIDS)?			
		X	
¿Existen planes de contingencia y continuidad que garanticen el buen funcionamiento de la red?			
		X	
¿Se utiliza cable tipo STP en los tramos donde se agrupa con el cableado eléctrico?			
		X	
¿Las terminaciones del cable de red están correctamente configuradas en base al código de colores de los pares trenzados?			
		X	
¿Se tienen suficientes nodos en la red para conectar todos los equipos que lo requieren?			
		X	
¿El cableado pasa por un techo falso o tubería subterránea para mayor protección?			
		X	
¿Se monitoriza la red, para la revisión de errores o situaciones anómalas?			
		X	
¿Cuenta con un análisis de vulnerabilidades en la implementación y configuración de los dispositivos de red?			
		X	
¿Los mensajes de transmisión dentro de la red cuentan con el origen, fecha, hora y receptor?			
		X	
¿Los datos que viajan por internet se encuentran cifrados?			
		X	
¿El cableado se encuentra blindado?			
		X	EXISTEN TRAMOS EN CATEGORIA 6
¿La entidad genera sus propios ataques para probar la solidez de la red y encontrar posibles fallas?			
		X	
¿Cuentan con VLAN's para administración en cada una de las oficinas que se dedican a diferente rubro?			
		X	LA RED ES TOTALMENTE PLANA

CSE SUBA - LAN WIRED

Durante la visita a este punto se pudo observar que se presentan problemas evidentes de seguridad de los cuartos de cableado, debido a la falta de chapas, llaves y/o cierres en las entradas, presentándose el riesgo de que personal ajeno al área pueda ingresar y causar daño a la red. Adicionalmente, se evidencia desorganización del cableado, deterioro en la infraestructura de los cuartos y la presencia de elementos tales como residuos de construcción; los sistemas de aire acondicionado no cumplen la función efectivamente.



Se ven cuartos sin llave y se han colocado bastones como medida restrictiva para evitar el paso lo cual no es seguro, los cables están desordenados y no es claro a que switch y/o servicio corresponden. En algunos cuartos se observa humedad y techos en mal estado, hay elementos dentro del cuarto que no deberían estar, como luminarias, dañadas, residuos de construcción bolsas de basura.

UMHES SIMON BOLIVAR

CHECKLIST AUDITORÍA RED LAN Y WIFI			
Nombre:	Checklist Red LAN y WIFI		
Versión	1.0		
INFORMACIÓN DE LA ENTIDAD			
Nombre de la entidad	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E. -- UMHES SIMON BOLIVAR		
Nombre de quien diligencia	OSCAR IVAN VERTGARA MEDINA		
Cargo	AUDITOR CONTROL INTERNO	Dependencia	OFICINA DE CONTROL INTERNO
Fecha de diligenciamiento	20/09/2022		
ITEM		SI	NO
¿Todos los nodos se encuentran bajo un mismo estándar de modo que no se reduzca la velocidad de transmisión?			X
¿La longitud de los tramos de cableado horizontal no excede de los 90 metros?		X	
¿El armado del patch panel cumple con los requerimientos básicos del estándar 568-A y 568-B?			X
¿El etiquetado implementado en la organización cuenta con un código de colores para facilitar su identificación?			X
¿Cuenta con un mapa arquitectónico para la verificación del sembrado de nodos?			X
¿Cuenta con mapas arquitectónicos de rutas de red para la implementación de un nuevo nodo?			X
¿Se tiene implementado el protocolo CSMA/CD para un mejor funcionamiento del sistema Ethernet?			
¿El cableado estructurado del interior del edificio viaja dentro de canaleta o ducto?		X	
¿Cuenta con dispositivo firewall físico para protección y aseguramiento de la red?		X	
¿Las direcciones IP'S de los equipos de cómputo son implementadas de forma fija?			X
¿Cuentan con conmutadores en red para la expansión de redes locales?			X
¿Cuenta con una memoria técnica de direccionamiento ip?			X
¿El rack donde se colocan los dispositivos cuenta con espacio libre para agregar más dispositivos?		X	
¿Se tiene conexión a tierra física para protección de equipos ante posibles descargas eléctricas que puedan afectar?		X	
¿Cuenta con dispositivos para la regulación del voltaje?		X	
¿La topología establecida se puede actualizar de tal manera que no ocurra ninguna anomalía dentro de la red?			X
¿Se tiene implementado un sistema de control de acceso para los dispositivos?		X	
¿Los equipos se encuentran instalados en áreas con temperaturas adecuadas para su funcionamiento?		X	
¿La empresa posee como mínimo 2 enlaces de Internet y un número igual de direcciones IP Públicas ?		X	
¿Los cables de los equipos se encuentran en buen estado?			X
¿Esta implementado un modelo de QoS en la red?			X
¿La red cuenta con los equipos y aplicaciones (IDS,IPS,NIDS)?		X	
¿Existen planes de contingencia y continuidad que garanticen el buen funcionamiento de la red?			X
¿Se utiliza cable tipo STP en los tramos donde se agrupa con el cableado eléctrico?			X
¿Las terminaciones del cable de red están correctamente configuradas en base al código de colores de los pares trenzados?			X
¿Se tienen suficientes nodos en la red para conectar todos los equipos que lo requieren?		X	
¿El cableado pasa por un techo falso o tubería subterránea para mayor protección?			X
¿Se monitoriza la red, para la revisión de errores o situaciones anómalas?		X	
¿Cuenta con un análisis de vulnerabilidades en la implementación y configuración de los dispositivos de red?			X
¿Los mensajes de transmisión dentro de la red cuentan con el origen, fecha, hora y receptor?			X
¿Los datos que viajan por internet se encuentran cifrados?		X	
¿La instalación de tierra física esta retirada al menos 5 metros del edificio?		X	
¿El cableado se encuentra blindado?			X
¿La entidad genera sus propios ataques para probar la solidez de la red y encontrar posibles fallas?			X
¿Cuentan con VLAN's para administración en cada una de las oficinas que se dedican a diferente rubro?		X	

SIMON BOLIVAR - LAN WIRED

En este punto de servicio se evidencio que todos los puntos de cableado se encuentran bien demarcados, bajo llave y con restricciones de acceso adecuado, sin embargo, la organización de los cables, los Rack y en general el estado físico de los cuartos podrían ser mejores, se evidencio que el centro de cableado que soporta el área de laboratorio clínico al ser de los más actualizados presenta una organización y buenas condiciones físicas.



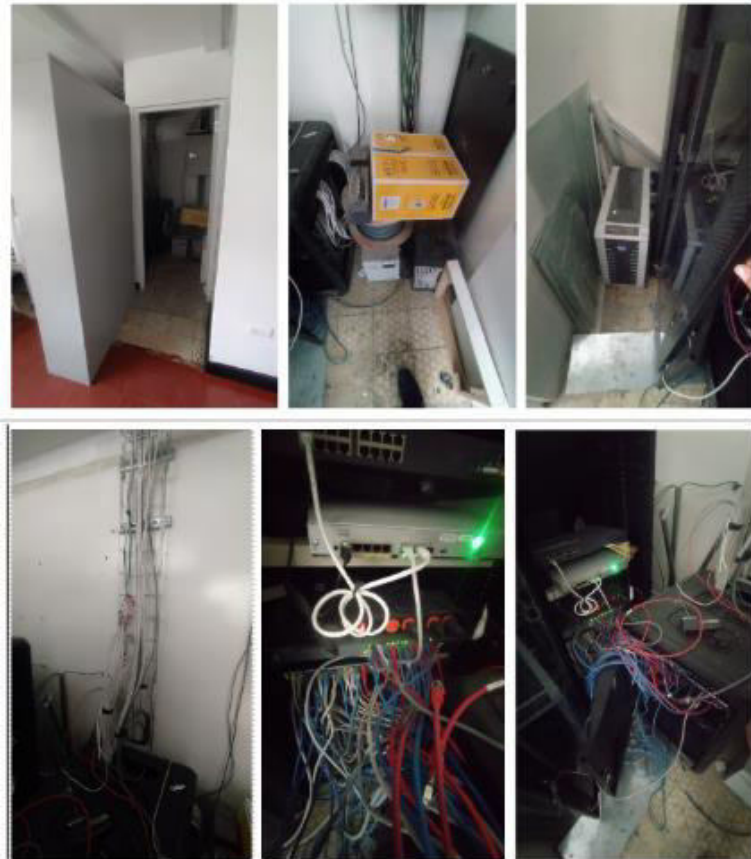
Se observan cuartos con llave, techos abiertos con falta de paneles e instalaciones eléctricas a la vista, los cables de red están desordenados y no es claro a que switch y/o servicio corresponden, dificultando la detección de fallas.



En el área de laboratorio se observa buena organización del cableado, condiciones físicas y de refrigeración son buenas esto se debe a que son instalaciones nuevas. sin embargo, en algunos cuartos aún existen cables e infraestructura sin mantenimiento.

CAPS SAN CRISTOBAL

En la verificación de este punto se encontraron grandes deficiencias en la seguridad física. Libre acceso al rack de cableado, sin demarcación del área, desorganización y conexión del cableado, no hay refrigeración.

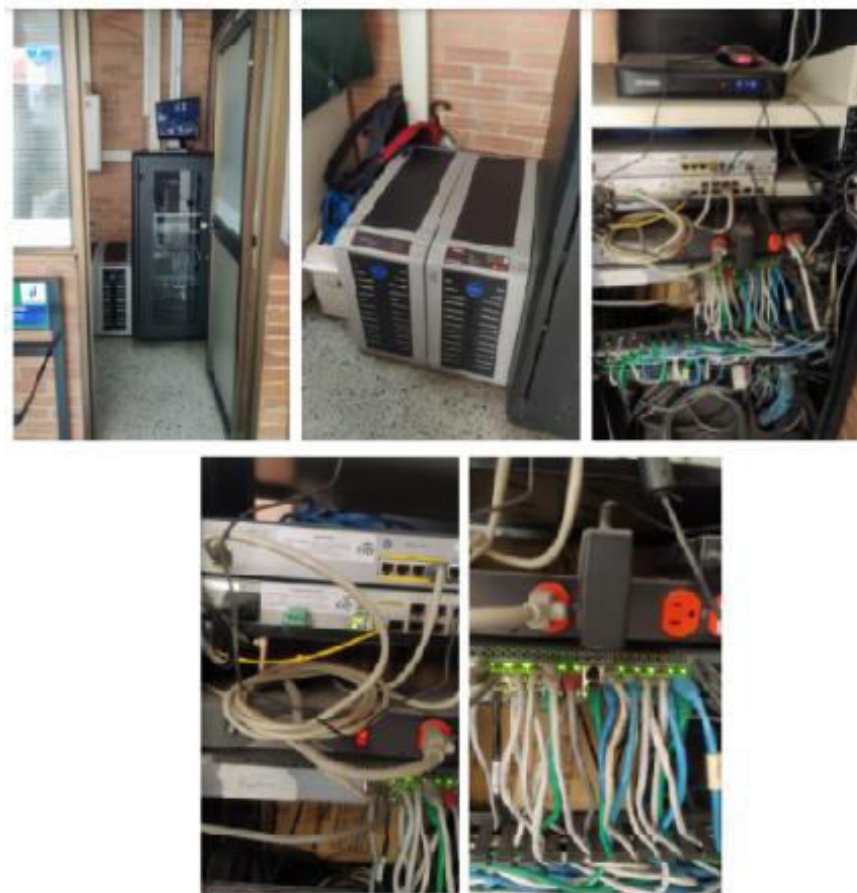


La puerta del cuarto de cableado del punto es un stand de lockers por lo que no existe restricción para el ingreso, por lo tanto se presentan elementos que no corresponden al centro de cableado.

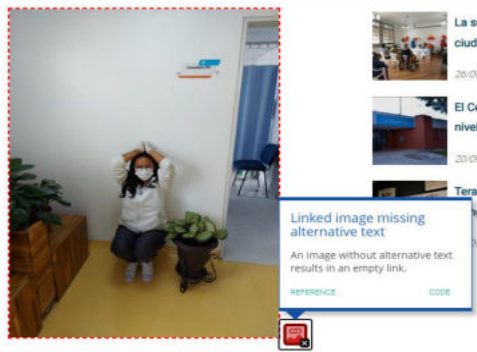
La conexión de los cables no es la adecuada, se observa la presencia de cables que pasan de un rack a otro, mostrando un desorden evidente.

USS ORQUIDEAS

Durante la verificación de este punto se encontró que el centro de cableado es compartido con el personal de seguridad y vigilancia, por lo que permanece cerrado y tiene el acceso restringido, pero al ser compartido, presenta un riesgo de acceso no autorizado.



Se observa que el centro permanece con llave y comparte el espacio con el cuarto de cámaras de seguridad. No se evidencian elementos de ventilación ni refrigeración, los cables tienen una organización aceptable para un centro de servicio pequeño.

cod_preg	Pregunta	Respuesta líder de política	Observaciones OCI	Cmp Líder	Cmp OCI
GDI01	Señale los criterios de accesibilidad web, del anexo 1 de la Resolución MinTIC 1519 de 2020 que cumple la entidad en todas las secciones de su portal Web oficial:	Alternativa texto para elementos no textuales, Complemento para videos o elementos multimedia, Guión para solo video y solo audio. (regla CC1, CC2, y CC3)	De acuerdo con la auditoría realizada en la vigencia 2021 por la OCI a la implementación de la resolución 1519 de 2020 y su plan de mejora, todos los hallazgos formulados quedarían subsanados al terminar la actual vigencia. Sin embargo, al hacer una prueba sobre la página principal de la subred, se encuentra que "falta texto alternativo en la imagen vinculada" como muestra la siguiente imagen.  Dicha situación nos lleva a concluir que a la fecha de esta auditoría no se ha completado el plan de mejor y por lo tanto la actual página web no da cumplimiento total con la norma 1519.	CT	CP
		Textos e imágenes ampliables y en tamaños adecuados, Contraste de color suficiente en textos e imágenes, Imágenes alternas al texto cuando sea posible, Identificación coherente, Todo documento y página organizado en secciones y tablas / listas usados correctamente. (regla CC4, CC5, CC6, CC7, y CC8)			
		Orden adecuado de los contenidos si es significativo. (Regla CC14)			
		No utilizar audio automático. Permitir control de eventos temporizados. Permitir control de contenidos con movimiento y parpadeo. No generar actualización automática de páginas. (regla CC18, CC19, CC20, y CC21)			
		Utilice instrucciones expresas y claras (incluido el color). (regla CC23)			
		Manejable por teclado. (regla CC32)			
		Permitir control de eventos temporizados. (regla CC19)			
		Permitir control de contenidos con movimiento y parpadeo. (regla CC20)			
		Permitir saltar bloques que se repiten. (regla CC10)			
		Utilice textos adecuados en títulos, páginas y secciones. (regla CC23)			
		Orden adecuado de los elementos al navegar con tabulación. (regla CC16)			
		Enlaces adecuados. (regla CC26)			
		Idioma. (regla CC27)			
		No generar cambios automáticos al recibir el foco o entradas. (regla CC22)			
		Manejo del error. (regla CC25)			
		Utilice instrucciones expresas y claras. (regla CC11)			
		Lenguaje de marcado bien utilizado. (regla CC11)			
		Desde una letra hasta un elemento complejo utilizable. (regla CC31)			
		Ninguna de las anteriores			
		No tiene conocimiento de los criterios de accesibilidad que debe cumplir la entidad en sus sedes electrónicas			
		Foco visible al navegar con tabulación. (regla CC17)			
		Imágenes de texto. (regla CC29)			
		Objetos programados. (regla CC30)			
GDI02	Señale los criterios de usabilidad web que cumple la entidad en todas las secciones de su portal Web oficial:	El sitio web permite conocer la ruta recorrida por el usuario en la navegación del sitio (Ruta de migas)	De acuerdo con la auditoría realizada en la vigencia 2021 por la OCI a la implementación de la resolución 1519 de 2020 y su plan de mejora, todos los hallazgos formulados quedarían subsanados al terminar la actual vigencia. En la página "Participa" se evidencian 9 errores de "falta texto alternativo en la imagen vinculada", dicha situación origina que "una imagen sin texto alternativo da como resultado un enlace vacío."	CT	CP
		Las URL generadas en los diferentes niveles de navegación no tienen variables o caracteres especiales y son fáciles de leer (URL limpios)			
		El diseño gráfico del sitio web se conserva en todos los sitios de navegación (Navegación global consistente)			
		El logo de la entidad ubicado en el encabezado, direcciona al inicio del sitio web (Vínculo a página de inicio)			
		El sitio web de la entidad permite el ingreso a través de diferentes navegadores como Google Chrome, Internet Explorer, Mozilla, entre otros (Independencia de navegador)			
		Los enlaces del sitio web indican claramente el contenido al cual conducen. No tienen textos como "ver más", "clic aquí", entre otros. (Enlaces bien formulados).			
		El sitio no cuenta con ventanas emergentes en ningún nivel de navegación			
		El sitio web hace un uso adecuado de títulos y encabezados con sus correspondientes etiquetas HTML, por ejemplo <h1>, <h2> ...			
		El sitio web no tiene vínculos rotos			
		Todos los contenidos del sitio web están alineados a la izquierda (Justificación del texto)			
		El cuerpo de texto no supera los 100 caracteres por línea (Ancho del cuerpo de texto)			
		En ningún contenido del sitio web existen textos subrayados para destacar, excepto si son enlaces a otros contenidos (Texto subrayado)			

cod_preg	Pregunta	Respuesta líder de política	Observaciones OCI	Cmp Líder	Cmp OCI
		El sitio web no permite desplazamiento de izquierda a derecha para consultar contenidos El sitio web cuenta con diferentes hojas de estilo para su correcta navegación (pantalla, móvil, impresión). En caso de que el sitio web sea responsivo sólo requiere formato de impresión El sitio web le indica al usuario cuando ha visitado contenidos de la página (Vínculos visitados) Los formularios del sitio web tienen correctamente señalizados los campos obligatorios Es clara la correspondencia entre el título del campo en los formularios y el espacio dispuesto para el ingreso de la información Ejemplos en los campos de formulario Ninguno de los anteriores No tiene conocimiento sobre las directrices de usabilidad que debe cumplir la entidad en su sitio Web			
GDI03	Con respecto al Plan Estratégico de Tecnologías de la Información (PETI) para esta vigencia, la entidad:	Lo formuló, está aprobado y se ha integrado al plan de acción anual Lo formuló, está aprobado, pero no se ha integrado al plan de acción anual Lo formuló, pero no ha sido aprobado por el comité de gestión y desempeño institucional Se encuentra en proceso de construcción y cuenta con una hoja de ruta definida No ha formulado el PETI o se encuentra desactualizado	Esta oficina evidenció que el PETI está formulado pero no ha sido aprobado por el comité de gestión y desempeño institucional.	CT	CP+
GDI04	El Plan Estratégico de Tecnologías de la Información (PETI) incluye:	El portafolio o mapa de ruta de los proyectos La proyección del presupuesto El entendimiento estratégico El análisis de la situación actual El plan de comunicaciones del PETI Tablero de indicadores para el seguimiento y control Definición de la situación objetivo y modelo de gestión de TI Ninguna de las anteriores	El PETI presenta deficiencias en los temas de presupuesto, portafolio de proyectos e indicadores, por lo tanto no cumple con las calificación dada en FURAG.	CT	CP+
GDI05	Con respecto a los proyectos de TI definidos en el PETI para la vigencia 2021:	¿Cuántos tiene definidos? [9] ¿Cuántos están en ejecución? ¿Cuántos han finalizado? ¿Cuál es el valor en pesos del presupuesto planeado dentro del PETI para la vigencia 2021? [6045000000] ¿Cuál es el valor en pesos del presupuesto ejecutado para proyectos de TI establecidos en el PETI para la vigencia 2021? ¿Cuál es el valor en pesos del presupuesto ejecutado de la operación de TI (mantenimiento, licencias, soporte, entre otros) para la vigencia 2021? [1298760504]	El indicador de avance de los proyectos es de 0% Numero de proyectos ejecutados / Numero de proyectos formulados	CT	CT
GDI06	Para la gestión de tecnologías de la información (TI), la entidad cuenta con:	Un esquema de soporte con niveles de atención (primer, segundo y tercer nivel) a través de un punto único de contacto y soportado por una herramienta tecnológica, tipo mesa de servicio que incluya al menos la gestión de problemas, incidentes, requerimientos, cambios, disponibilidad y conocimiento Un proceso para atender los incidentes y requerimientos de soporte de los servicios de TI, tipo mesa de ayuda Catálogo de servicios de TI actualizado Acuerdos de Nivel de Servicios (SLA por sus siglas en inglés) con terceros y Acuerdos de Niveles de Operación (OLA por sus siglas en inglés) Ninguna de las anteriores	Se evidencia el cumplimiento de los documentos par la gestión de tecnologías de información.	CT	CT
GDI07	Señale los aspectos incorporados en el esquema de gobierno de tecnologías de la información (TI) de la entidad:	Políticas de TI definidas Macroproceso o proceso (procedimientos, actividades y flujos) de gestión de TI definido, documentado y actualizado Instancias o grupos de decisión de TI definidas Estructura organizacional del área de TI Indicadores para medir el desempeño de la gestión de TI Ninguna de las anteriores	No se evidencian: Manual de políticas de TI definidas, el proceso y procedimientos se encuentran desactualizados, al igual que los indicadores.	CT	CP-

cod_preg	Pregunta	Respuesta líder de política	Observaciones OCI	Cmp Líder	Cmp OCI
GDI08	Para la optimización de las compras de tecnologías de información (TI), la entidad:	Utilizó Acuerdos Marco de Precios para bienes y servicios de TI	Se evidencia que en las compras de TI se utilizan mecanismos o contratos de agregación	CT	CT
		Utilizó mecanismos o contratos de agregación de demanda para bienes y servicios de TI			
		Aplicó otras metodologías, casos de negocio o criterios documentados para la adquisición y/o evaluación de soluciones de TI			
		Ninguna de las anteriores			
GDI09	Respecto a la gestión de proyectos de tecnologías de la información (TI), la entidad:	Aplicó una metodología para la gestión de proyectos de TI que incluye seguimiento y control a las fichas de proyecto a través de indicadores	Se evidencia el cumplimiento parcial de las actividades y opciones de la respuesta en la gestión de proyectos de TI	CP	CP
		Garantizó que todas las iniciativas, proyectos o planes de la entidad que incorporen componentes de TI, son liderados en conjunto entre las áreas misionales y el área de TI de la entidad			
		Utilizó el principio de incorporar desde la planeación la visión de los usuarios y la atención de las necesidades de los grupos de valor			
		Realizó la documentación y transferencia de conocimiento a proveedores, contratistas y/o responsables de TI, sobre los entregables o resultados de los proyectos ejecutados en la vigencia evaluada			
		Contó con herramientas tecnológicas para la gestión de proyectos de TI			
GDI10	Con relación a la planeación y gestión de los componentes de información, la entidad:	Ninguna de las anteriores	No se evidencia el cumplimiento de procesos de calidad de datos y no existe un MSPi en la entidad.	CT	CP-
		Cuenta con el catálogo de componentes de información actualizado			
		Cuenta con vistas de información actualizadas de la arquitectura de información para todas las fuentes de información			
		Implementa procesos o procedimientos de calidad de los datos			
GDI11	Con relación a la planeación y gestión de los sistemas de información, la entidad:	Implementa procesos o procedimientos que aseguren la integridad, disponibilidad y confidencialidad de los datos	Esta auditoría no evidencia el cumplimiento de funcionalidades de trazabilidad, log de auditoría en los sistemas de información implementados.	CP+	CP-
		Ninguna de las anteriores			
		Cuenta con un catálogo actualizado de todos los sistemas de información			
		Cuenta con una arquitectura de referencia y una arquitectura de solución debidamente documentadas o actualizadas para todas sus soluciones tecnológicas			
		Incluyó características en sus sistemas de información que permitan la apertura de sus datos de forma automática y segura			
		Incorporó dentro de los contratos de desarrollo de sus sistemas de información, cláusulas que obliguen a realizar transferencia de derechos de autor a su favor			
		Implementó para sus sistemas de información funcionalidades de trazabilidad, auditoría de transacciones o acciones para el registro de eventos de creación, actualización, modificación o borrado de información			
		Cuenta con la documentación técnica y funcional debidamente actualizada, para cada uno de los sistemas de información			
		Cuenta con manuales de usuario y manuales técnicos y de operación debidamente actualizados, para cada uno de los sistemas de información			
		Realiza desarrollos de software y cuenta con todos los documentos de arquitectura de software actualizados			
		Definió e implementó una metodología de referencia para el desarrollo de software o sistemas de información, indique cuál:			
GDI12	Con relación al esquema de soporte y mantenimiento de los sistemas de información, la entidad:	Ninguna de las anteriores	Se cuenta con un esquema de soporte, pero no se evidencia la aprobación ni la mejora continua	CT	CP-
		Lo definió, lo documentó, está aprobado e implementado, y se actualiza mediante un proceso de mejora continua			
		Lo definió, lo documentó, está aprobado e implementado			
		Lo definió, lo documentó y está aprobado por el comité de gestión y desempeño institucional, pero no está implementado			
		Lo definió y lo documentó, pero no está aprobado			
GDI13	Con respecto al ciclo de vida de los sistemas de información, la entidad:	No lo tiene o se encuentra desactualizado	No se evidencia el cumplimiento de implementación de un plan de aseguramiento de la calidad. Solo se evidencia el uso de la guía de estilo en la página WEB.	CP+	CP-
		Definió un proceso de construcción de software que incluya planeación, diseño, desarrollo, pruebas, puesta en producción y mantenimiento			
		Implementó un plan de aseguramiento de la calidad durante el ciclo de vida de los sistemas de información que incluya criterios funcionales y no funcionales			
		Definió y aplicó una guía de estilo en el desarrollo de sus sistemas de información e incorpora especificaciones y lineamientos de usabilidad definidos por el MinTIC			
		Tienen las funcionalidades de accesibilidad que indica la Política de gobierno Digital, en los sistemas de información de acuerdo con la caracterización de usuarios			
		Ninguna de las anteriores			
GDI13	Con respecto al ciclo de vida de los sistemas de información, la entidad:	No tiene conocimiento sobre los ciclos de vida de los sistemas de información			

cod_preg	Pregunta	Respuesta líder de política	Observaciones OCI	Cmp Líder	Cmp OCI
GDI14	Con relación al soporte y operación de la infraestructura de TI (o servicios tecnológicos), la entidad:	Implementó un plan de mantenimiento preventivo y evolutivo (de mejoramiento) sobre la infraestructura de TI	Solo se cuenta con plan de mantenimiento de equipos de computo, no se evidencia planes de mantenimiento a servidores, redes y equipos activos de comunicación. No se evidencia el uso de computación en la nube, el plan de continuidad de los servicios tecnológicos se encuentra en elaboración. El monitoreo se realiza sobre la disponibilidad de canales y actividad de servidores.	CT	CP
		Implementó un programa de correcta disposición final de los residuos tecnológicos de acuerdo con la normatividad del gobierno nacional			
		Cuenta con un directorio actualizado de todos los elementos de infraestructura de TI			
		Cuenta con vistas actualizadas de despliegue, conectividad y almacenamiento de la arquitectura de infraestructura de TI			
		Hace uso de servicios de computación en la nube para mejorar los servicios que presta la entidad			
		Documentó e implementó un plan de continuidad de los servicios tecnológicos mediante pruebas y verificaciones acordes a las necesidades de la entidad			
		Implementó mecanismos de disponibilidad de la infraestructura de TI de tal forma que se asegure el cumplimiento de los ANS establecidos			
		Realiza monitoreo del consumo de recursos asociados a la infraestructura de TI			
		Ninguna de las anteriores			
GDI15	¿En qué fase de la adopción de IPv6 se encuentra actualmente la entidad?	Fase de planeación	Se evidencia plan de transición de IPV4 a IPV6	CP-	CP-
		Fase de implementación			
		Fase de pruebas de funcionalidad			
		Ha adoptado en su totalidad IPv6 en la entidad			
		No ha iniciado ninguna fase			
		No tiene conocimiento sobre qué es IPV6			
GDI16	Con respecto a la adopción de IPv6, la entidad cuenta con:	Plan de Diagnóstico (Fase planeación)	No se evidencia diagnostico, plan detallado, plan de direccionamiento ni plan de contingencia.	CP	CP-
		Plan detallado del proceso de transición (Fase planeación)			
		Plan de direccionamiento IPv6 (Fase planeación)			
		Plan de contingencias para IPv6 (Fase planeación)			
		Documento de diseño detallado de la implementación de IPv6 (Fase implementación)			
		Informe de pruebas piloto realizadas (Fase implementación)			
		Informe de activación de políticas de seguridad en IPv6 (Fase implementación)			
		Documento de pruebas de funcionalidad en IPv6 (Pruebas de funcionalidad)			
		Acta de cumplimiento a satisfacción de la entidad sobre el funcionamiento de los elementos intervenidos en la fase de implementación. (Pruebas de funcionalidad)			
GDI17	Frente a la estrategia para el uso y apropiación de tecnologías de la información (TI), la entidad:	Ninguna de las anteriores	No se evidencia estrategia implementada de uso y apropiación de tecnología con formación y/o capacitación de servidores.	CP+	NC
		Implementó una estrategia de uso y apropiación para todos los proyectos de TI, teniendo en cuenta estrategias de gestión del cambio			
		Implementó una estrategia de divulgación y comunicación de los proyectos de TI			
		Realizó la caracterización de los grupos de interés internos y externos			
		Ejecutó un plan de formación o capacitación dirigido a servidores públicos para el desarrollo de competencias requeridas en TI			
		Realizó seguimiento a través de indicadores sobre el uso y apropiación de TI en la entidad			
		Ejecutó acciones de mejora a partir de los resultados obtenidos a través de los indicadores de uso y apropiación			
		Ninguna de las anteriores			

cod_preg	Pregunta	Respuesta líder de política	Observaciones OCI	Cmp Líder	Cmp OCI
GDI18	¿La entidad cuenta con un diagnóstico de seguridad y privacidad de la información para la vigencia, construido a través de la herramienta de autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI)?	Si, y cuenta con las evidencias:	Se evidencia el diagnostico de la seguridad y privacidad de la información	CT	CT
		Si, y cuenta con las evidencias-Evidencia			
		Está elaborado, pero no aprobado			
		No			
GDI19	La política de seguridad y privacidad de la información de la entidad:	Está formulada, aprobada, implementada y se actualiza mediante un proceso de mejora continua	El manual de políticas de seguridad de la información no ha sido implementado, ni aprobado por la alta gerencia, ni se gestiona con mejora continua.	CT	CP-
		Está formulada, aprobada e implementada			
		Está formulada y aprobada por el comité de gestión y desempeño institucional, pero aún no ha sido implementada			
		Está formulada pero no ha sido aprobada por el comité de gestión y desempeño institucional			
		La entidad no cuenta con una política de seguridad y privacidad de la información			
GDI20	¿La entidad cuenta con procedimientos de seguridad y privacidad de la información?	Los procedimientos están definidos, aprobados e implementados, y se actualizan mediante un proceso de mejora continua	Solo se evidencia el procedimiento de gestión de incidentes en una versión preliminar	CP+	CP-
		Los procedimientos están definidos, aprobados e implementados			
		Cuenta con procedimientos definidos y aprobados por el comité de gestión y desempeño institucional, pero no han sido implementados			
		Cuenta con procedimientos definidos y documentados, pero no han sido aprobados por el comité de gestión y desempeño institucional			
		No cuenta con procedimientos de seguridad y privacidad de la información o están en proceso de construcción			
GDI21	Con respecto al inventario de activos de seguridad y privacidad de la información de la entidad:	El inventario está aprobado, clasificado y se actualiza mediante un proceso de mejora continua	Se evidencia una versión preliminar de inventario de activos de información. Pero no se encuentra clasificado, ni se actualiza mediante mejora continua	CT	NC
		El inventario está aprobado y se clasifica de acuerdo con los criterios de disponibilidad, integridad y confidencialidad			
		Cuenta con el inventario y está aprobado por el comité de gestión y desempeño institucional			
		Cuenta con el inventario, pero no ha sido aprobado			
		No cuenta con el inventario de activos de seguridad y privacidad de la información o está en proceso de construcción			
GDI22	Con respecto a los riesgos de seguridad y privacidad de la información de la entidad:	Los identifica, están aprobados, se implementa un proceso para valorarlos y se actualizan mediante un proceso de mejora continua	No se evidencia caracterización de riesgos de seguridad y privacidad de la información	CP	NC
		Los identifica, están aprobados y se implementa un proceso para valorarlos			
		Los identifica y están aprobados por el comité de gestión y desempeño institucional, pero aún no se implementa un proceso para valorarlos			
		Los identifica, pero no han sido aprobados por el comité de gestión y desempeño institucional			
		No identifica los riesgos de seguridad y privacidad de la información			
GDI23	¿La entidad implementó el plan de tratamiento de riesgos de seguridad de la información?	Sí, ya lo implementó y cuenta con las evidencias	No se evidencia plan de tratamiento de riesgos de seguridad de la información	CP-	NC
		Sí, ya lo implementó y cuenta con las evidencias-Evidencia			
		Está en proceso de implementarlo			
		No			
GDI24	Con respecto al plan operacional de seguridad y privacidad de la información, la entidad:	El plan está aprobado, implementado y se actualiza mediante un proceso de mejora continua	La entidad cuenta con un plan de seguridad de la información que no ha sido aprobado	CT	CP-
		El plan está aprobado y se implementa			
		Cuenta con un plan y ha sido aprobado por el comité de gestión y desempeño institucional			
		Cuenta con un plan pero no ha sido aprobado			
		No cuenta con un plan operacional de seguridad y privacidad de la información			
GDI25	Con respecto a los indicadores de implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) en la entidad:	Los indicadores están definidos, aprobados e implementados, y se actualizan mediante un proceso de mejora continua	No se evidencian indicadores definidos, aprobados e implementados	CP+	NC
		Los indicadores están definidos, aprobados e implementados			
		Los indicadores están definidos y aprobados por el comité de gestión y desempeño institucional, pero no están implementados			
		Los indicadores están definidos, pero no han sido aprobados por el comité de gestión y desempeño institucional			
		No ha definido indicadores para medir la eficiencia y eficacia de la implementación del MSPI en la entidad			

cod_preg	Pregunta	Respuesta líder de política	Observaciones OCI	Cmp Líder	Cmp OCI
GDI27	Con respecto a los procesos, trámites o servicios de la entidad que requieren interoperabilidad:	Ha hecho un proceso completo de identificación y su documentación está actualizada	Se evidencia un proceso parcial de identificación	CT	CP-
		Ha hecho un proceso completo de identificación y está parcialmente documentado			
		Ha hecho un proceso completo de identificación, pero no lo ha documentado			
		Ha hecho un proceso parcial de identificación			
		No los ha identificado			
GDI28	Con respecto al Marco de Interoperabilidad para realizar intercambio de información con otras entidades:	Lo utiliza y su documentación está actualizada	Existe evidencia parcial del uso del marco de interoperabilidad.	CT	CP
		Lo utiliza y su implementación está parcialmente documentada			
		Lo utiliza pero no tiene documentada su implementación			
		Lo utiliza parcialmente			
		La entidad no utiliza el Marco de Interoperabilidad			
GDI29	Con respecto a los servicios de intercambio de información de la entidad:	¿Cuántos servicios de la entidad son susceptibles de intercambio de información con otras entidades? [6]	Se evidencian servicios de interoperabilidad de la historia clínica	CP	CP
		¿Cuántos servicios utilizan la plataforma de interoperabilidad (PDI)? [6]			
		¿Cuántos servicios de la entidad utilizan el estándar de lenguaje común de intercambio de información? [6]			
		De los servicios que utilizan el estándar de lenguaje común de intercambio de información, ¿Cuántos están certificados? [6]			
		¿Cuántos servicios certificados (en el uso del estándar) utilizan la plataforma de interoperabilidad (PDI)?			
		En la vigencia 2021, ¿Cuántos servicios de la entidad se certificaron en el uso del estándar de lenguaje común de intercambio de información? [6]			
GDI30	Con respecto a los datos abiertos indique:	¿Cuántos conjuntos de datos abiertos estratégicos (por ej. aquellos que contribuyen al logro de la misión institucional, de alto impacto social, más demandados) fueron identificados? [21]	Se evidencian conjuntos de datos abiertos publicados, sin evidencia proceso de identificación de datos abiertos estratégicos.	CP+	CP-
		¿Cuántos de los conjuntos de datos abiertos estratégicos identificados fueron publicados en el catálogo de datos del Estado colombiano www.datos.gov.co? [21]			
		¿Cuántos de los conjuntos de datos abiertos fueron publicados, están actualizados y fueron difundidos? [21]			
		¿Cuántos de los conjuntos de datos abiertos de la entidad fueron desarrollados en procesos de cocreación o consulta pública?			
GDI31	Para el tema de datos abiertos de la entidad, especifique:	Número total de usuarios de los datos abiertos de la entidad contactados durante 2021:	No se evidencia el contacto con usuarios de datos abiertos	CP	NC
		Número total de usuarios contactados y satisfechos con el uso de los datos abiertos de la entidad durante 2021:			
		La entidad no mide la satisfacción de los usuarios con el uso de los datos abiertos			
GDI32	Con respecto al plan de apertura, mejora y uso de datos abiertos para esta vigencia, la entidad:	Lo formuló, está aprobado y se ha integrado al plan de acción anual	Se evidencia un instructivo para la apertura, mejora y uso de datos abiertos; pero este no soporta la respuesta de que fue aprobado y que se integra al plan de acción anual.	CT	CP
		Lo formuló, está aprobado pero no se ha integrado al plan de acción anual			
		Lo formuló, pero no ha sido aprobado por el comité de gestión y desempeño institucional			
		Se encuentra en proceso de construcción y cuenta con una hoja de ruta definida			
		No lo ha formulado o se encuentra desactualizado			
GDI33	Con respecto a la ejecución del plan de apertura, mejora y uso de datos abiertos para esta vigencia, indique:	Número total de actividades o acciones establecidas en el plan: [8]	En el documento: instructivo para la apertura, mejora y uso de datos abiertos, no se evidencia un plan de apertura de datos con actividades programadas	CT	NC
		Número de actividades o acciones completadas a la fecha: [8]			
GDI34	Con respecto a los procesos de la entidad, indique:	¿Cuántos procesos tiene la entidad? [17]	No se evidencian ejercicios de arquitectura empresarial de TI	NC	NC
		¿Cuántos procesos se han automatizado teniendo en cuenta las definiciones (lineamientos, guías, herramientas y mejores prácticas) del marco de referencia de arquitectura empresarial?			
		¿Cuántos procesos se han mejorado incorporando esquemas de manejo seguro de la información conforme a lo establecido en el Modelo de Seguridad y Privacidad de la Información?			
		¿Cuántos procesos se han digitalizado teniendo en cuenta las definiciones (lineamientos, guías, herramientas y mejores prácticas) del marco de referencia de arquitectura empresarial?			

cod_preg	Pregunta	Respuesta líder de política	Observaciones OCI	Cmp Líder	Cmp OCI
GDI35	La automatización o mejora de los procesos le ha permitido a la entidad:	Mejorar los tiempos de respuesta	No se evidencian ejercicios de arquitectura empresarial de TI	NC	NC
		Reducir costos operacionales			
		Mejorar la disponibilidad de sus servicios			
		Mejorar la satisfacción de los ciudadanos			
		Mejorar la satisfacción de los usuarios internos			
		Otro. ¿Cuál?			
		Ninguna de las anteriores			
GDI36	¿La entidad ha implementado iniciativas de ciudades y territorios inteligentes?	Si, y cuenta con las evidencias:	Se evidencia la participación activa de la subred en la construcción de la plataforma Bogotá Salud Digital	CT	CT
		Si, y cuenta con las evidencias:-Evidencia			
		No			
GDI37	En cuáles instrumentos de planeación de la entidad se contemplaron las iniciativas o proyectos de ciudad o territorio inteligente:	Plan de desarrollo territorial o plan estratégico institucional	Se evidencia la participación activa de la subred en la construcción de la plataforma Bogotá Salud Digital	CT	CT
		Plan de desarrollo territorial o plan estratégico institucional y planes de acción anual			
		Planes de acción anual			
		Otro. ¿Cuál?			
		Ninguna de las anteriores			
GDI38	Para el despliegue y operación de servicios relacionados con iniciativas de ciudad o territorio inteligente, la entidad utiliza algunos de los siguientes servicios de computación en la nube:	Infraestructura como servicio (IaaS) como: procesamiento, almacenamiento, servidores, backups, entre otros	Se evidencia el uso de SAS en el correo electrónico.	NC	CP-
		Plataforma como servicio (PaaS) como: servicios de administradores de bases de datos, sistemas operativos, herramientas de desarrollo, entre otros			
		Software como servicios (SaaS) como correo electrónico, servicios de analítica de datos, entre otros			
		Ninguna de las anteriores			
GDI39	Con respecto al uso de internet de las cosas (IoT), la entidad ha realizado:	Identificación y priorización de la infraestructura y servicios de IoT que requiere o se necesita para adelantar iniciativas de ciudad o territorio inteligente	Sobre IoT, la entidad no ha realizado ejercicios	NC	NC
		Estructuración de la arquitectura de la infraestructura de IoT a desplegar en la ciudad o territorio			
		Instalación y despliegue de sensores y redes de IoT			
		Analítica y explotación de datos capturados por medio de dispositivos IoT			
		Ninguna de las anteriores			
GDI40	¿La entidad hace uso de los instrumentos de agregación de demanda y priorización de los servicios de nube (como Acuerdos Marco de precios) para la gestión de recursos públicos en proyectos de Tecnologías de la Información?	Si, y cuenta con las evidencias	La entidad solo cuenta con servicio de correo como SaaS	NC	CP-
		Si, y cuenta con las evidencias-Evidencia			
		No			
GDI41	¿La entidad hace uso de tecnologías basadas en software libre o código abierto?	Si, y cuenta con las evidencias	Se evidencia el uso de plataformas de software libre	CT	CT
		Si, y cuenta con las evidencias-Evidencia			
		No			
GDI42	Cuáles de las siguientes tecnologías emergentes de la Cuarta Revolución Industrial que facilitan la prestación de servicios del Estado utiliza la entidad:	Tecnologías de desintermediación, DLT (Distributed Ledger Technology) como cadena de bloques (Blockchain) o contratos inteligentes, entre otros	No se evidencia el uso de inteligencia artificial en los procesos de prestación de servicios	CP	CP-
		Análisis masivo de datos (Big data)			
		Inteligencia Artificial (AI)			
		Internet de las Cosas (IoT)			
		Robótica y similares			
		Ninguna de las anteriores			
		Automatización robótica de procesos			
GDI43	¿La entidad aplica programas de uso de tecnología para participación ciudadana y Gobierno abierto en sus procesos misionales?	Si, y cuenta con las evidencias	En los procesos misionales no se evidencia el uso de tecnología para la participación ciudadana y gobierno abierto. Adicionalmente la evidencia enviada no es accesible	CT	NC
		Si, y cuenta con las evidencias-Evidencia			
		No			

cod_preg	Pregunta	Respuesta líder de política	Observaciones OCI	Cmp Líder	Cmp OCI
GDI44	¿La entidad hace uso de estrategias público-privadas que propendan por el uso de medios de pago electrónico?	Si, y cuenta con las evidencias	Se evidencia el uso de estrategias para el fomento de pago electrónico	CT	CT
		Si, y cuenta con las evidencias-Evidencia			
		No			
		No aplica			
GDI45	¿La entidad cuenta con programas de capacitación que permitan a sus servidores públicos apropiarse de capacidades para conocer tecnologías de la cuarta revolución industrial?	Si, y cuenta con las evidencias	No se evidencia el fomento de conocimiento de tecnologías de la 4ta revolución industrial	NC	NC
		Si, y cuenta con las evidencias-Evidencia			
		No			
GDI46	¿La entidad hace uso de contratos de Asociaciones Público Privadas (APP) relacionados con Tecnologías de la Información y las Comunicaciones?	Si, y cuenta con las evidencias	La entidad no hace uso de asociaciones publico privadas relacionadas con TI	NC	NC
		Si, y cuenta con las evidencias-Evidencia			
		No			
GDI47	La entidad hace uso del machine learning para:	Experimentación, producción y decisiones estratégicas	La subred no hace uso de Machine Learning	NC	NC
		Experimentación y producción			
		Experimentación			
		Procesos de planeación en la materia de machine learning			
		Ninguna de las anteriores			
GDI48	¿En cuál de los siguientes niveles la entidad hace uso de la Inteligencia Artificial –IA?	Inteligencia asistida: En esta primera etapa, la entidad obtiene ventajas de programas de datos a gran escala, del potencial de la nube y de enfoques científicos para tomar decisiones basadas en datos	En concordancia con la pregunta No. 42. La entidad no hace uso de inteligencia artificial	NC	NC
		Inteligencia aumentada: las capacidades de aprendizaje automático superan a las de los sistemas de gestión de la información, lo que maximiza las competencias analíticas humanas			
		Inteligencia autónoma: los procesos se encuentran digitalizados y automatizados hasta el grado en que máquinas, robots y sistemas puedan actuar directamente sobre la inteligencia derivada de ellos mismos			
		Ninguno de los anteriores			
GDI49	Con respecto al Plan de Transformación Digital (entendido en los términos del artículo 147 del PND y bajo los lineamientos del Marco de Transformación Digital) para la vigencia 2021, la entidad:	Lo formuló, está aprobado, y se ha actualizado el PETI conforme a las iniciativas, procesos y áreas priorizadas para la transformación digital	De acuerdo con la pregunta 03. Esta oficina evidenció que el PETI está formulado pero no ha sido aprobado por el comité de gestión y desempeño institucional.	CT	CP+
		Lo formuló, está aprobado, pero no se ha actualizado el PETI conforme a las iniciativas, procesos y áreas priorizadas para la transformación digital			
		Lo formuló, pero no ha sido aprobado por el comité de gestión y desempeño institucional			
		Se encuentra en proceso de construcción			
		No ha formulado el Plan de Transformación Digital			
GDI50	Con respecto al uso de tecnologías DTL (Distribute Ledger Technologies) como Blockchain, la entidad:	Ha terminado una implementación de aplicaciones basadas en DLT y se encuentra en uso	La entidad no ha desarrollado proyectos o aplicaciones de DLT	NC	NC
		Ha terminado una implementación de aplicaciones basadas en DLT, pero no superó la etapa piloto			
		Está piloteando una aplicación de DLT			
		Está en proceso de diseño de una aplicación de DLT			
		No ha desarrollado proyectos o aplicaciones de DLT			
GDI51	¿Existe en la entidad un equipo dedicado exclusivamente a la explotación de datos mediante la aplicación de técnicas y métodos de analítica de datos y Big Data?	Existe un equipo dedicado exclusivamente a la explotación de datos que, brinda apoyo a otras dependencias, satisface las necesidades de información definidas por la alta dirección para la toma de decisiones, y desarrolla actividades interinstitucionales para el aprovechamiento de datos, consolidando así el conocimiento y experiencia de la entidad en explotación de datos	se evidencia que la entidad cuenta con un equipo de estadística, no con un equipo de explotación de datos.	CT	NC
		Existe un equipo dedicado exclusivamente a la explotación de datos que, brinda apoyo a otras dependencias, satisface las necesidades de información definidas por la alta dirección para la toma de decisiones, y está orientado a consolidar el conocimiento y experiencia de la entidad en explotación de datos			
		Existe un equipo dedicado exclusivamente a la explotación de datos que brinda apoyo a otras dependencias y está orientado a consolidar el conocimiento y experiencia de la entidad en explotación de datos			
		La entidad cuenta con un equipo que realiza estudios piloto o pruebas de concepto para la explotación de datos			
		La entidad no cuenta con un equipo encargado de la explotación de datos			

cod_preg	Pregunta	Respuesta líder de política	Observaciones OCI	Cmp Líder	Cmp OCI
GDI52	Con respecto a la capacitación que brinda la entidad en analítica de datos y Big Data:	La entidad ofrece de manera periódica capacitaciones de profundización estandarizadas y participa en ejercicio de intercambio de conocimientos en Big Data con otras entidades y actores de la academia y el sector privado	La entidad no usa técnicas de explotación de datos. Adicionalmente esta respuesta controvierte la respuesta de la pregunta 51	NC	NC
		La entidad ofrece de manera periódica capacitaciones de profundización estandarizadas, el cual apoya la formación continua en Big Data para cada uno de los perfiles y es apoyado por la alta gerencia			
		La entidad realiza capacitaciones de profundización que están en curso de ser estandarizadas en un programa institucional e identifica profesionales en las dependencias que por sus perfiles puedan ser parte del equipo capacitado			
		La entidad realiza capacitaciones de forma aislada y con poca profundidad que son asumidas en costo por cada profesional			
		La entidad no brinda capacitaciones sobre estos temas			
GDI53	¿Durante los últimos cinco años la entidad ha destinado un presupuesto específico a la explotación de datos?	Durante los últimos cinco años consecutivos la entidad ha incluido en el presupuesto un rubro para atender las necesidades asociadas a explotación de datos dentro de la entidad	La entidad no usa técnicas de explotación de datos. Adicionalmente esta respuesta controvierte la respuesta de la pregunta 51	NC	NC
		Durante los últimos tres años consecutivos la entidad ha incluido en el presupuesto un rubro para atender las necesidades asociadas a explotación de datos dentro de la entidad			
		En el último año la entidad ha incluido en el presupuesto un rubro para atender las necesidades asociadas a explotación de datos dentro de la entidad			
		La entidad ha destinado eventualmente un presupuesto específico a proyectos aislados de explotación de datos			
		La entidad no ha destinado un presupuesto específico para explotación de datos durante los últimos cinco años			
GDI54	A la hora de priorizar inversiones y distribuir el presupuesto de la entidad:	En la etapa de diseño y planeación de la entidad en cada vigencia, se destina presupuesto para explotación de datos y Big Data orientado a: mejorar las capacidades tecnológicas y humanas y responder a las necesidades de la alta gerencia; mejorar y generar productos, procesos y servicios; desarrollar proyectos conjuntos con otras entidades o actores como academia y sector privado	La entidad no usa técnicas de explotación de datos.	NC	NC
		En la etapa de diseño y planeación de la entidad en cada vigencia, se destina presupuesto para explotación de datos y Big Data orientado a: mejorar las capacidades tecnológicas y humanas y responder a las necesidades de la alta gerencia con proyectos específicos.			
		Se reconoce la importancia de explotación de datos y Big data en la entidad. Por tanto se han iniciado ejercicio de planeación organizacional, para incluir rubros relacionados con el fortalecimiento de capacidades tecnológicas y de recurso humano, y la realización de proyectos de explotación de datos			
		Se destina presupuesto para iniciativas, pruebas de concepto y proyectos relacionados con explotación de datos, pero la destinación del presupuesto no responde a un ejercicio de planeación organizacional.			
		La inversión en explotación de datos y Big Data no se prioriza ya que no se reconoce como algo importante para el desempeño misional de la entidad			
GDI55	¿La entidad ha implementado alguna iniciativa, proyecto o prueba de concepto de explotación de datos y Big Data?	Si, y cuenta con las evidencias:	Se evidencia la participación de la subred en la construcción de la plataforma Bogotá Salud Digital. No se evidencia iniciativa, proyecto de explotación de datos.	CT	CP
		Si, y cuenta con las evidencias:-Evidencia			
		No			
GDI56	Con respecto a la calidad de los conjuntos de datos de la entidad:	Los procesos de validación, limpieza, aseguramiento y control de calidad están documentados, implementados y automatizados, y permiten garantizar la disponibilidad, usabilidad, confiabilidad, relevancia y presentación de los conjuntos de datos de la entidad. Esto permite su aprovechamiento por parte de actores interesados (otras entidades públicas, academia, sector privado) de forma directa y oportuna	Se evidencia un instructivo para la apertura, mejora y uso de datos abiertos. Sin embargo su procesamiento se realiza manual y con el uso de herramientas ofimáticas	CP	CP-
		Los procesos de validación, limpieza, aseguramiento y control de calidad están documentados, implementados y automatizados, y permiten garantizar la disponibilidad, usabilidad, confiabilidad, relevancia y presentación de los conjuntos de datos de la entidad			
		Los procesos de validación, limpieza, aseguramiento y control de calidad están documentados, implementados pero no automatizados, y permiten garantizar la disponibilidad, usabilidad, confiabilidad, relevancia y presentación de algunos conjuntos de datos de la entidad			
		Los procesos de validación, limpieza, aseguramiento y control de calidad se hacen de manera manual con el apoyo de herramientas informáticas			
		El proceso de calidad de datos se realiza de manera manual como respuesta a solicitudes específicas			

cod_preg	Pregunta	Respuesta líder de política	Observaciones OCI	Cmp Líder	Cmp OCI
GDI57	En el contexto de la explotación de datos y Big Data, ¿La entidad ha aplicado alguna técnica de anonimización que preserve la privacidad de los datos?	La entidad aplica técnicas que garantizan la privacidad de todos sus conjuntos de datos personales de manera automatizada y controlada, a lo largo de todo el ciclo de vida de datos La entidad aplica técnicas que garantizan la privacidad de algunos de sus conjuntos de datos personales de manera automatizada y controlada, a lo largo de todo el ciclo de vida de datos La entidad aplica técnicas de manera manual y estandarizada que garantizan la privacidad de algunos de sus conjuntos de datos personales Existe conocimiento de técnicas de anonimización y se aplican para algunos de los conjuntos de datos personales de la entidad, como respuesta a solicitudes específicas La entidad no ha aplicado técnicas de anonimización de los datos	No se evidencian técnicas ni herramientas de anonimización de datos.	NC	NC
GDI58	¿La entidad define métricas para medir la calidad de los datos?	Las métricas de la calidad de los datos se monitorean periódicamente desde la alta gerencia, como garantía para el aprovechamiento conjunto con actores interesados (otras entidades públicas, academia, sector privado y ciudadanos) Las métricas de la calidad de los datos se monitorean periódicamente pero solamente para los conjuntos priorizados por parte de la alta gerencia Se han definido métricas de la calidad de los datos pero no se monitorean periódicamente No se han definido métricas de calidad, pero es posible generarlas como respuesta a proyectos o solicitudes específicas La entidad no mide la calidad de los datos	No se evidencian métricas de (DQA) Data Quality Assessment	CT	NC
GDI59	¿La entidad cuenta con un protocolo estandarizado para la anonimización y protección de datos personales (seguridad y privacidad)?	Existe un protocolo de anonimización y protección de datos personales que se implementa y tiene el respaldo de la alta dirección. Esto facilita el trabajo colaborativo para la explotación de datos con otras entidades públicas, privadas y academia Existe un protocolo de anonimización y protección de datos personales, que se implementa en la alta dirección Se ha definido un protocolo básico de anonimización de los datos generados por la entidad para su acceso y consulta. Se esta trabajando en la implementación de este protocolo No existe un protocolo estandarizado para la anonimización y protección de datos. Para la elaboración de proyectos o iniciativas, se solicita a la fuente de datos que gestione la anonimización de los conjuntos de datos que se requiera, de acuerdo con la necesidad La entidad no cuenta con un protocolo estandarizado para la anomimización y protección de datos personales	No se evidencia protocolo estandarizado para la anonimización y protección de datos. Adicionalmente esta respuesta controvierte la respuesta de la pregunta 51	CT	NC
GDI60	¿La entidad tiene definida una política de gobernanza de datos?	La política de gobernanza de datos de la entidad está implementada, y cumple con los requerimientos de privacidad, estándares de calidad, archivo, preservación y reutilización de los datos. Adicionalmente, se monitorea periódicamente para identificar avances y oportunidades de mejora La política de gobernanza de datos de la entidad está implementada, y cumple con los requerimientos de privacidad, estándares de calidad, archivo, preservación y reutilización de los datos. Sin embargo, no se monitorea periódicamente La política de gobernanza de datos de la entidad está formulada, y cumple con los requerimientos de privacidad, estándares de calidad, archivo, preservación y reutilización de los datos. Sin embargo, su implementación es dispersa Se ha identificado la necesidad de una política de gobernanza de datos y está en proceso de formulación No existe un política de gobernanza de datos en la entidad	No se evidencia el proceso de construcción de una política de gobernanza de datos en la entidad	CP-	NC
GDI61	¿La entidad ha desarrollado iniciativas o proyectos basados en el uso de tecnologías emergentes (Inteligencia artificial, Internet de las cosas, Blockchain, Big Data, Robótica, entre otros)?	Sí, y cuenta con las evidencias: Sí, y cuenta con las evidencias: -Evidencia No	No se evidencia el desarrollo de iniciativas o proyectos basados en uso de tecnologías emergentes. Adicionalmente la evidencia enviada no es accesible	CT	NC
GDI62	Con respecto a los servicios de la entidad:	¿Cuántos servicios de la entidad utilizan X-ROAD? ¿Cuántos servicios de la entidad utilizan el servicio de autenticación digital? ¿Cuántos servicios de la entidad disponen sus resultados a los usuarios por medio de la carpeta ciudadana digital?	Esta auditoría no pudo confirmar el dato aquí consignado	CT	ND
GDI63	Con respecto a los trámites de la entidad:	¿Cuántos trámites de la entidad utilizan X-ROAD? ¿Cuántos trámites de la entidad utilizan el servicio de autenticación digital? [1] ¿Cuántos de trámites de la entidad disponen sus resultados a los usuarios por medio de la carpeta ciudadana digital? [1] No aplica porque la entidad no tiene trámites	Esta auditoría no pudo confirmar el dato aquí consignado	CT	ND