Fecha de la Auditoría:

Diciembre 13 del 2021

Objetivo:

Evaluar el cumplimiento de los requisitos de la Norma ISO/IEC 27001:2013, verificando el cumplimiento de las disposiciones planificadas y comprobando que se mantienen de manera eficaz los controles, en el Modelo de Seguridad y Privacidad de la información implementado en el SANATORIO DE CONTRATACION.

Alcance:

La Auditoría Interna aplica al proceso de las TIC de Sanatorio dentro del marco operativo del Modelo de Seguridad y Privacidad de la información implementado.
Las políticas de Seguridad de la Información son aplicables a todos los servidores públicos, pasantes, y contratistas del Sanatorio de Contratación que procesan y/o manejan información de la entidad, incluidas las operaciones de recopilación, análisis, procesamiento, disponibilidad, custodia, conservación y recuperación.

Criterios:

- Documento Conpes 3854: Política Nacional de Seguridad Digital
- Circular externa conjunta No. 04 del 5 de septiembre de 2019: Tratamiento de datos personales en sistemas de información interoperables.
- Norma Técnica Colombiana NTC-ISO/IEC Colombiana 27001:2013 Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.

Metodología:

Entrevista, revisión documental y observación.

Equipo Auditor:

- Gloria Esperanza Berdugo (Encargada Of. Control Interno)

DESCRIPCION DEL TRABAJO REALIZADO, OPCIONES DE MEJORA Y CONCLUSIONES

Evaluar el estado actual del Modelo de Seguridad de la Información del Sanatorio de Contratación, con respecto a la ISO/IEC 27001:2013

Se aplicó la encuesta (Objetivos de control y controles de referencia) a la Gestión de Tecnología de la Información, la cual, fue realizada con los funcionarios líderes del área de Sistemas, sobre el cumplimiento relacionado con los dominios y controles de seguridad que establece la Norma ISO/IEC 27001:2013.

Las respuestas posibles están dadas por: NC, CP, CS, NA. De acuerdo a la información que se presenta en la siguiente tabla:

SIGLA	ESTADO DE EVALUACION	DESCRIPCION
NC	NO CUMPLE	No existe y/o no se está haciendo
CP	CUMPLE PARCIALMENTE	Lo que la norma requiere (ISO/IEC 27001 versión 2013) se está haciendo de manera parcial, se está haciendo diferente, no está documentado, se definió y aprobó, pero no se gestiona
CS	CUMPLE SATISFACTORIAMENTE	Existe, es gestionado, se está cumpliendo con lo que la norma ISO/IEC 27001 versión 2013 solicita, está documentado, es conocido y aplicado por todos los involucrados en el SGSI cumple 100%
NA	NO APLICA	No se aplica en la Entidad

"Diagnóstico inicial encuesta aplicada"

OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA		CS	CP	NC	NA
1	**Política de la seguridad de la información**				
1.1.	Política para la seguridad de la información	x			
2	**Organización Interna**				
2.1.	Roles y responsabilidades para la seguridad de la información: Identificación de los responsables.	x			
3.	**Plan de sensibilización, capacitación y comunicación**				
3.1.	Programa que explique de manera apropiada las reglas de comportamiento adecuadas para el uso de los sistemas y la información: Busca asegurar que los usuarios desde el más principiante hasta el más experimentado tengan los conocimientos suficientes para desempeñar sus roles.		x		
4.	**Seguridad del Recurso Humano**				
4.1.	Procedimiento de capacitación y sensibilización del personal en temas de seguridad de la información	X			
4.2.	Procedimiento de ingreso y desvinculación del personal: acuerdos de confidencialidad, paz y salvos.		X		

	OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA	CS	CP	NC	NA
5.	**Gestión de activos**				
5.1.	Inventario de activos de información	x			
5.2.	Propiedad de los activos: los activos de información del inventario deben tener un propietario.	x			
5.3.	Clasificación de la información	x			
6.	**Gestión de riesgos**				
6.1.	Identificación de riesgos	x			
6.2.	Identificación y análisis de riesgos en la nube				x
7.	**Control de acceso**				
7.1.	Procedimiento para ingreso seguro a los sistemas de información		x		
7.2.	Procedimiento de acceso a usuarios		x		
7.3.	Procedimiento asignación de contraseñas		x		
8.	**Seguridad física y del entorno**				
8.1.	Control de acceso físico: registros de fecha y hora de ingreso		x		
8.2.	Procedimiento protección de activos: controles que se aplican para minimizar riesgos de desastres naturales, agua, descargas eléctricas, etc.			x	
8.3.	Protección contra amenazas externas y ambientales.			x	
8.4.	Procedimiento retiro de activos: debe contemplar como los activos son retirados de la entidad con previa autorización. Qué controles deberá tener el equipo cuando esté fuera de la entidad-			x	
8.5.	Procedimiento mantenimiento de equipos	x			
8.6.	Seguridad del cableado			x	
9.	**Seguridad de las operaciones**				
9.1.	Procedimiento de protección contra códigos maliciosos: qué controles utiliza (hardware o software)		x		
10.	**Seguridad de las comunicaciones**				
10.1.	Controles de redes: Cómo la Entidad protege la información en las redes. Uso de registro (logs) que permitan realizar seguimiento a acciones sospechosas.		x		
10.2.	Políticas y procedimientos de transferencia de información: como se transfiere la información de manera segura dentro de la Entidad o con entidades externas donde se apliquen métodos para proteger la información de interceptación, copiado, modificación y/o destrucción.		x		
10.3.	Acuerdos de confidencialidad y no divulgación.			x	
11.	**Aspectos de seguridad de la información de la gestión de continuidad del negocio**				

	OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA	CS	CP	NC	NA
11.1.	Procedimiento de gestión de la continuidad de negocio: Se debe indicar la manera en que la Entidad garantiza la continuidad para todos sus procesos (de ser posible o por lo menos los misionales) identificando los procesos críticos que tendrán mayor prioridad en las fases de recuperación ante algún desastre o incidente crítico.			x	
12.	**Transicion IPV4 - IPV6**				
12.1.	Qué proyección se tiene para el cambio de IPV y con cuantos recursos presupuestales se cuenta ?		X		
13.	**Gestión de incidentes**				
13.1.	Politica de comunicación: Definir qué incidente puede ser comunicado a los medios y cual no.		x		
13.2.	Tener un listado de los puertos conocidos y de los puertos utilizados para realizar un ataque.	x			
13.3.	Clasificación de incidentes de seguridad de la información-			x	

RESULTADOS DE LA ENCUESTA

Como resultado de la encuesta anterior y de la información entregada por los líderes del proceso de las TIC del Sanatorio se concluye:

- Se evaluaron y revisaron veintiocho (28) criterios obteniendo un puntaje de:

Estado de evaluación	No. Criterios	% de cumplimiento
CS	10	36%
CP	10	36%
NC	8	28%

Fortalezas

- Se adoptó la Política de seguridad para la información mediante Resolución 0371 de abril del 2020. En la cual está contemplado los roles y responsabilidades para la seguridad de la información.
- Los activos de información se encuentran publicados en la pag web institucional, donde cada activo tiene un responsable y la información se encuentra debidamente clasificada.
- En el 2021 se elaboró el "Mapa de riesgos de seguridad de la información"

- La Institución cuenta con lectores biométricos de asistencia de personal.
- El Sanatorio de Contratación cuenta con el procedimiento "Mantenimiento de equipos", el cual, se está dando cumplimiento y así mismo en la presente vigencia se ha podido adquirir nuevos equipos de cómputo para remplazar algunos que se han tenido que dar de baja por su obsolescencia.
- Se cuenta con antivirus actualizado.
- En el 2021 se trabajó en el diagnostico de la estructura de la red actual para el cambio de IPV, para lo cual, la oficina de presupuesto se ha comprometido con destinar recursos de alrededor de cincuenta (50) millones para la implementación de IPV4 a IPV6 en la vigencia 2022
- La Institución cuenta con alrededor de 50 puertos habilitados.

No Conformidades

No	Hallazgos
1	En los contratos laborales no hay acuerdo de confidencialidad.
2	A la fecha el Sanatorio de Contratación no ha comprado el espacio para publicación de información en la nube.
3	Se requiere actualizar el procedimiento "Ingreso seguro a los sistemas de información"
4	Se requiere actualizar el "Procedimiento acceso a usuarios"
5	Se requiere actualizar el "Procedimiento asignación de contraseñas"
6	No hay seguridad suficiente para el ingreso a la oficina de Sistemas. No hay cuarto exclusivo para servidores
7	No se cuenta con el procedimiento protección de activos. No hay alarma de seguridad . No hay sifón si llegara el caso de una inundación.
8	No hay procedimiento "retiro de activos" (equipos de cómputo y activos de información)
9	El cableado no tiene seguridad porque no está blindado.

No	Hallazgos
10	El Hospital Sanatorio de Contratación, tiene su red intranet obsoleta.
11	No está documentado el procedimiento contra códigos maliciosos.
12	No se cuenta con Logs que permita realizar seguimiento a acciones sospechosas.
13	Se debe actualizar la Política de protección de la Información.
14	No hay acuerdos de confidencialidad y su divulgación
15	No se cuenta con el "Procedimiento de gestión de la continuidad de negocio"
16	El Manual de Comunicaciones tiene pendiente incluir "Plan de Comunicaciones" donde se determine el responsable y contenido.
17	No se encuentra la clasificación de incidentes de seguridad de la información.

Conclusiones y Recomendaciones

- Presentar resultados del grado de avance en la implementación del Sistema integrado de gestión de Seguridad de la información SIGSI, al Comité de Gestión y Desempeño Institucional, con el fin de contar con información sobre la gestión adelantada, de modo que la Alta Dirección pueda tomar acciones sobre la mejora continua.

- Fortalecer las campañas de sensibilización para asegurar que los empleados y contratistas tomen conciencia y den cumplimiento a sus responsabilidades en materia de seguridad de la información.

- Fortalecer los procedimientos de operación documentándolos y poniéndolos a disposición de todos los usuarios que los necesitan, con el fin de que todos los colaboradores tengan acceso a la documentación del SGSI y se fomente la cultura de la mejora continua en lo que respecta al SGSI, tal como lo define la NTC-ISOIEC 27001:2013.

- Fortalecer la política para el reporte y tratamiento de incidentes de seguridad mediante controles que permitan asegurar una respuesta rápida eficaz y ordenada a los incidentes de Seguridad de la Información.

- Definir acuerdos con los proveedores y estos incluyen requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.

- El Sanatorio de Contratación cuenta con el Software G.D. desde hace aproximadamente seis (6) años, el cual, cuenta con los módulos del área asistencial, financiera y presupuestal. Sin embargo los módulos del área asistencial presentan varias inconformidades por parte de los usuarios ya que no está parametrizado de acuerdo a la normatividad vigente, por lo anterior, recomiendo a los líderes del área informática de la Institución apropiarse de gestionar ante el proveedor del Software el contrato para mantenimiento, actualización y parametrización de dicho Software que es la columna vertebral en la generación de información para toda la Entidad.

Plan de mejoramiento

Como mecanismo de control y con base en las opciones de mejora encontrados, la Oficina de Tecnología de la Información, deberá elaborar un plan de mejoramiento interno, tendiente a corregir y subsanar los puntos susceptibles de mejora, el cual, será dado a conocer a la Oficina de Control Interno, cinco (5) días hábiles después de la entrega final del informe.

Elaboró:
Gloria E. Berdugo
Nombre: Gloria E. Berdugo
Cargo: Encargada de Control Interno