Fecha de la Auditoría:

25 de Septiembre del 2023

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 de la seguridad de la Información**				
2.1.	Roles y responsabilidades para la seguridad de la información: Identificación de los responsables.	x			
2.2.	Políticas para dispositivos móviles			x	
3.	**Seguridad del recurso humano**				
3.1.	Capacitación y sensibilización del personal en temas de seguridad de la información			x	
3.2.	El tema de seguridad de la información está incluido en el programa de inducción y reinducción para los funcionarios	x			
3.3.	Acuerdos de confidencialidad o de no divulgación para empleados y contratistas			x	

OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA		CS	CP	NC	NA
3.4.	Proceso disciplinario formal: contra empleados que hayan cometido violación a la seguridad de la información			x	
3.5.	Terminación o cambio de responsabilidades de empleo			x	
4.	**Gestión de activos**				
4.1.	Inventario de activos de información	x			
4.2.	Propiedad de los activos: los activos de información del inventario deben tener un propietario.	x			
4.3.	Clasificación de la información	x			
4.4.	Devolución de activos: "Incluir en el compromiso de confidencialidad y no divulgación de la información"			x	
4.5.	Etiquetado de la información	x			
4.6.	Disposición de los medios: Se cuenta con el proveedor de servicios: nube privada ?			x	
5.	**Control de acceso**				
5.1.	Política control de acceso		x		
6.	**Criptografía**				
6.1.	Política uso de controles criptográficos				x
6.2.	Guía para el uso y protección de firmas electrónicas			x	
7.	**Seguridad física y del entorno**				
7.1.	Control de acceso físico: Las áreas que contengan información sensible o crítica deberían protegerse mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.		x		
7.2.	Seguridad de oficinas, recintos e instalaciones		x		
7.3.	Protección de activos contra amenazas externas y ambientales (protección contra desastres naturales, ataques maliciosos o accidentes)		x		
	Seguridad de equipos				
7.4.	Seguridad de equipos y activos fuera de las instalaciones	x			
7.5	Servicios de suministro: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.		x		
7.6.	Seguridad del cableado			x	
7.7.	Mantenimiento equipos de cómputo	x			
7.8.	Disposición segura o reutilización de equipos	x			
7.9.	Equipos de usuarios desatendidos: implementar el bloqueo automático de pantallas de todos los computadores, después de 5 minutos de inactividad y se realiza divulgación y sensibilización de métodos rápidos de bloqueo.		x		
7.10	Política de escritorio limpio y pantalla limpia			x	

OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA		CS	CP	NC	NA
8.	**Seguridad de las operaciones**				
8.1.	Protección contra códigos maliciosos			x	
8.2.	Protección contra la pérdida de datos: copias de respaldo	x			
8.3	Registrar eventos y generar evidencia: elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.		x		
	Control de Software operacional				
8.4	Restricciones sobre la instalación de software	x			
9.	**Seguridad de las comunicaciones**				
9.1.	Controles de redes: Cómo la Entidad protege la información en las redes. Uso de registro (logs) que permitan realizar seguimiento a acciones sospechosas.		x		
9.2.	Políticas y procedimientos de transferencia de información: como se transfiere la información de manera segura dentro de la Entidad y/o con entidades externas donde se apliquen métodos para proteger la información de interceptación, copiado, modificación y/o destrucción.		x		
10.	**Aspectos de seguridad de la información de la gestión de continuidad del negocio**				
10.1.	Implementación de la continuidad de la seguridad de la información: 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	
11.	**Cumplimiento**				
11.1.	Identificación de la legislación aplicable y de los requisitos contractuales.		x		
11.2.	Protección de registros: Los registros se deben proteger contra perdida, destrucción, falsificación, acceso no autorizado; de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio		x		
12.	**Gestión de incidentes: eventos que atentan contra la confidencialidad**				
12.1.	Estableces responsabilidades y procedimientos			x	
12.2.	Reportes de debilidades 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 treinta y ocho (38) criterios obteniendo un puntaje de:

Estado de evaluación	No. Criterios	% de cumplimiento
CS	12	32%
CP	11	29%
NC	14	37%
NA	1	2%
Total	**38**	**100%**

Fortalezas

- La ESE Sanatorio de Contratación cuenta la Unidad funcional de Gestión de Información y Tecnología y el líder del proceso es un profesional asignado a la planta de la Institución y a su vez se cuenta con un contratista Ingeniero de Sistemas quien apoya y hace seguimiento contribuyendo con el desarrollo e implementación del Sistema de gestión de seguridad en la entidad.

- 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.

- El inventario de activos de información se actualiza cada año con corte al 30 de Junio y se publica 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"

- Se observa que la entidad hace uso de contraseñas como medida para restringir el acceso a sus sistemas .

- 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.

No Conformidades

No	Hallazgos
1	En los acuerdos contractuales con empleados y contratistas no está incluido el acuerdo de confidencialidad y no divulgación de la información durante y después de terminado el contrato laboral y así mismo se debe incluir la devolución de activos al terminar su empleo, contrato o acuerdo.
2	No hay una política definida para el uso de dispositivos móviles que tengan información institucional.
3	Ausencia de capacitación y sensibilización a los empleados y contratistas de la entidad en temas de seguridad de la información.
4	No se cuenta con un proceso disciplinario formal, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.
5	No está documentada la política control de acceso (Ingreso seguro a los sistemas de información.
6	El cableado no tiene seguridad porque no está blindado
7	La página web institucional se encuentra fuera de servicio debido a que no hay contrato vigente con proveedor del Hosting (quien aloja los contenidos de la web para que puedan ser visitados en todo momento desde cualquier dispositivo conectado a internet)
8	Licencia de antivirus vencida
9	A la fecha el Sanatorio de Contratación no ha comprado el espacio para publicación de información en la nube.
10	No hay seguridad suficiente para el ingreso a la oficina de Sistemas. No hay cuarto exclusivo para servidores
11	No se cuenta con el procedimiento protección de activos. No hay alarma de seguridad . No hay sifón si llegara el caso de una inundación.

12	No se cuenta con políticas y procedimientos de transferencia de información.
13	No está definida ni implementada la política de escritorio limpio y pantalla limpia.
14	El Hospital Sanatorio de Contratación, tiene su red intranet obsoleta.
15	No está documentado el procedimiento contra códigos maliciosos.
16	No se cuenta con Logs que permita realizar seguimiento a acciones sospechosas.
17	No está documentado los procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.
18	No se tiene documentado los procedimientos y responsabilidades frente a incidentes de seguridad de la información.
19	Se debe actualizar la Política de protección de la Información.
20	El Manual de Comunicaciones tiene pendiente incluir "Plan de Comunicaciones" donde se determine el responsable y contenido.
21	No se encuentra la clasificación de incidentes de seguridad de la información.

Conclusiones y Recomendaciones

- 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.

- El documento "Compromiso de confidencialidad y no divulgación de la Información", se encuentra en proceso de revisión por parte de la Oficina Asesora Jurídica".

- Se sugiere que tan pronto se adopte el "Compromiso de confidencialidad y no divulgación de la información" sea socializado con todo el personal tanto de planta como

contratistas y así mismo incluir esta cláusula de compromiso en los acuerdos contractuales con empleados y contratistas, lo cual, debe seguir vigente incluso después de la terminación laboral o contractual.

- Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación de contrato o cambio de responsabilidades de empleo se deberían definir, comunicar al empleado o contratista y se deberían hacer cumplir.

- 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

- Se debería contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra empleados que cometan violación a la seguridad de la información.

- Se debería adoptar una política y medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles que manejen información del Sanatorio.

- El acceso a la información y a los módulos del Software G.D. se debería restringir de acuerdo con la política de control de acceso y/o controlar mediante un proceso de ingreso seguro.

- 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-ISO/IEC 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.

- Se deberían definir y usar perímetros de seguridad física y usarlos para proteger áreas que contengan información sensible o critica e instalaciones de manejo de información; dichas áreas se deberían proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.

- Se debería diseñar y aplicar seguridad física a oficinas, recintos e instalaciones del Sanatorio, teniendo en cuenta que en su gran mayoría las puertas y chapas no están en buen estado.

- En este momento los equipos no tienen antivirus porque la licencia se venció y la Gerencia se encuentra gestionando el proceso de contratación.

- Así mismo se venció el contrato con el proveedor del hosting, actualmente la Gerente de la entidad se encuentra en proceso de contratación con un nuevo proveedor, por lo anterior, la pag www.sanatoriocontratacion.gov.co se encuentra fuera de servicio.

- El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debería estar protegido contra interceptación, interferencia o daño.

- Se recomienda dar cumplimiento estricto al plan de mantenimiento programado para los equipos de cómputo y actualizar la hoja de vida de los mismos.

- Se sugiere implementar el bloqueo automático de pantallas para todos los computadores, después de ciertos minutos de inactividad y los usuarios deben asegurarse que los equipos desatendidos se les dé protección apropiada.

- Se debería 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

- Se deberían implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos

- El Sanatorio de Contratación cuenta con el Software G.D. desde hace aproximadamente siete (7) años, el cual, cuenta con los módulos del área asistencial, financiera y presupuestal.

- Se recomienda a Gerencia gestionar con el proveedor del Software G.D. contratar los servicios de mantenimiento, actualización y parametrización de los diferentes módulos de acuerdo a la normatividad vigente en materia de salud, tal es el caso del área asistencial donde hay varios informes que no se pueden generar directamente del Software sino que se elaboran con información manual (digitalizada)

- Se sugiere a los profesionales que se encuentran responsables de la unidad funcional de Gestión de información y tecnología, 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.

Plan de mejoramiento

Como mecanismo de control y con base en las opciones de mejora encontrados, la Unidad funcional de Gestión de información y Tecnología, deberá elaborar un plan de mejora 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:
Nombre: Gloria E. Berdugo
Cargo: Encargada de Control Interno