Proceso: **Gestión de Servicios TIC**

Política __, Plan__, Programa __, Proyecto __, Procedimiento __ y/o Actividad __

Auditoría Interna bajo la norma ISO IEC 27001:2013

Número de Auditoria: 2023-MR-03

Fecha Reunión de Apertura: 20/11/2023

Fecha Reunión de Cierre: 27/11/2023

LÍDER DE PROCESO / JEFE(S) DEPENDENCIA(S)
LIGIA DEL CARMEN GALVIS AMAYA

EQUIPO AUDITOR
ALEXANDRA BIBIANA CALA MORENO

OBJETIVO DE AUDITORÍA: Validación del cumplimiento del SGSI con base a lo establecido en la norma ISO IEC 27001:2013

ALCANCE DE AUDITORÍA: Validación del cumplimiento del SGSI con base a lo establecido en la norma ISO IEC 27001:2013 - Gestión de Servicios TIC

CRITERIOS DE AUDITORÍA: Norma ISO IEC 27001:2013, Normatividad Legal, Documentación del Ministerio de Educación

RESUMEN GENERAL

I. FORTALEZAS

- Disposición y apertura por parte de los funcionarios para la atención de la Auditoría
- Conocimiento del personal de TI con respecto a las actividades realizadas al interior del proceso
- Conocimiento por parte del Líder y de sus segundos al mando sobre la norma ISO IEC 27001:2013

II. RIESGOS Y EVALUACIÓN DE CONTROLES

No se tiene un manejo adecuado de los riesgos, lo cual se soporta en que:

1. No se tiene identificado el dueño del riesgo
2. No se tiene relación del Anexo A de la norma con los controles que se tienen en el MEN para cada riesgo
3. No se identificación si el riesgo afecta la confidencialidad, integridad o disponibilidad

4. No se tiene seguimiento a los riesgos
5. No se tiene acta de aceptación de riesgo residual y de plan de tratamiento de los riesgos

Lo anterior incumpliendo con lo establecido en la norma ISO IEC 27001:2013 en los numerales 6.1.2 (c) y 6.1.3 (a, c, f).

III. PLANES, PROGRAMAS, PROYECTOS E INDICADORES

- % Avance e la implementación del Plan de Seguridad y Privacidad de la información. Meta: 90%. Resultado: Semestre 1: 50%
- % de ejecución del Plan de Comunicaciones del SGSI Meta: 80% Resultado: Semestre 1: 50%
- % de Procesos con riesgos de seguridad de la información gestión, Meta: 80%. Resultado: Semestre 1: 75%
- % de Implementación de Acciones de Mejora. Meta: 80% Resultado: Semestre 1: 100%

IV. MECANISMOS DE SEGUIMIENTO Y AUTOEVALUACIÓN

N.A.

V. PARTICIPACION CIUDADANA

N.A

VI. ESTADO DE LAS PETICIONES, QUEJAS, RECLAMOS, SUGERENCIAS Y DENUNCIAS

N.A

VII. CONCLUSIONES Y RECOMENDACIONES

- Se lograron los objetivos de la Auditoría
- La actividad fue realizada 100% presencial
- Se hace necesario programar la auditoría sobre el Proceso de Talento Humano para validar la implementación del numeral 7.2 y el dominio A.7
- Elaborar Planes de Acción para las No Conformidades y las Observaciones emitidas en el informe

INFORME DETALLADO (N.A)			
Resultado		Descripción	Recomendación
HZ	OM		
		N.A	

INFORME DETALLADO (N.A)			
Resultado		**Descripción**	**Recomendación**
HZ	**OM**		
		N.A	

AUDITORIA SISTEMAS DE GESTIÓN DE CALIDAD / AMBIENTAL Y OTROS MODELOS REFERENCIALES				
Resultado			**Requisito o Numeral**	**Descripción**
C	**NC**	**OM**		
	X		A.8.2.2	No se evidencia que la organización aplique el etiquetado de la información, de acuerdo a la clasificación establecida por el MEN, lo cual se soporta que durante toda la auditoría, ningún documento se encontraba etiquetado, lo anterior incumpliendo con lo establecido en la norma ISO IEC 27001:2013 en el control A.8.2.2.
	X		7.5.3 (a)	No se evidencia que se diligencien los registros de manera adecuada, lo cual se soporta que se tiene formato PM-FT-07 Versión 3, para diligenciar el análisis de contexto; sin embargo, el mismo no se encuentra diligenciado y el análisis del contexto fue realizado en un documento no controlado, lo anterior incumpliendo con lo establecido en la norma ISO IEC 27001:2013 en el numeral 7.5.3 (a)
		X	4.1	Garantizar la actualización del contexto externo e interno teniendo en cuenta los cambios del entorno presentados en el MEN,
		X	4.1	Reforzar el DOFA, teniendo en cuenta el Proveedor del DataCenter (Tigo)
		X	4.2	Evidenciar claramente las necesidades y expectativas de las partes interesadas.
		X	4.2	Garantizar que existe relación entre las Partes Interesadas y los grados: Poder, interés, Impacto, Influencia, Necesidad de información,
		X	4.3	Completar el Alcance del SGSI con la identificación de la Declaración de Aplicabilidad (SOA)
		X	6.1.3 (d)	Validar las No Aplicabilidades del SGSI de acuerdo a las actividades realizadas por el MEN

AUDITORIA SISTEMAS DE GESTIÓN DE CALIDAD / AMBIENTAL Y OTROS MODELOS REFERENCIALES				
Resultado			Requisito o Numeral	Descripción
C	NC	OM		
		X	6.1.3 (d)	Incluir dentro de la Declaración de Aplicabilidad (SOA), la forma como se aplica cada control dentro del MEN y la correspondiente justificación de aplicación de cada control
	X		5.1.(b) 4.4	No se tienen identificados claramente los numerales y controles de la noma por cada proceso, lo anterior incumpliendo lo establecido en la norma ISO IEC 27001:2013 en los numerales 4.4 y 5.1 (b)
	X		5.2 (f y g)	No se tiene evidencia de la divulgación de la política del SGSI al interior del MEN; y la política publicada en la página WEB del MEN para que esté disponible para las partes interesadas se encuentra desactualizada; lo anterior incumpliendo con lo establecido en la norma ISO IEC 27001:2013 en el numera 5.2 (f y g)
		X	6.2 (f, g, h, i)	Garantizar que se tiene documentado para los objetivos del sistema lo que se va a hacer; que recursos se requerirán; quién será responsable y cuándo se finalizarán.
		X	5.2	Garantizar que en todas partes donde se referencie la política, siempre se relacione la última versión de la misma.
		X	7.1	Garantizar que se tenga claramente identificado el presupuesto y recursos necesarios para la implementación, mantenimiento y Operación del SGSI
		X	7.2 A.7	Garantizar la auditoría al Proceso de Talento Humano
	X		6.1.2 (c) 6.1.3 (a, c, f)	No se tiene un manejo adecuado de los riesgos, lo cual se soporta en que: • No se tiene identificado el dueño del riesgo • No se tiene relación del Anexo A de la norma con los controles que se tienen en el MEN para cada riesgo • No se tiene identificación si el riesgo afecta la confidencialidad, integridad o disponibilidad • No se tiene acta de aceptación de riesgo residual y de plan de

AUDITORIA SISTEMAS DE GESTIÓN DE CALIDAD / AMBIENTAL Y OTROS MODELOS REFERENCIALES				
Resultado			Requisito o Numeral	Descripción
C	NC	OM		
				tratamiento de los riesgos por parte de los dueños de los riesgos Lo anterior incumpliendo con lo establecido en la norma ISO IEC 27001:2013 en los numerales 6.1.2 (c) y 6.1.3 (a, c, f)
	X		A.6.1.5	No se tienen identificados los riesgos de seguridad de la información al realizar el cambio de Sede del CNA de la 93 al Centro, lo anterior, incumpliendo con lo establecido en la norma ISO IEC 27001:2013 en el control A.6.1.5
	X		8.1	No se evidencia que se realicen las actividades de manera controlada, lo cual se soporta en que al revisar los tickets: 1. SOL807292 de fecha 23 de octubre de 2023.ubicar 5 puntos de red para la sede de CNA en la calle 19 # 6 - 68 oficinas 404 y 405. No se tiene evidencia de la gestión realizada sobre el ticket. se escalo a Medardo Castro 2. SOL 806321 de fecha: 19 de octubre de 2023,. Restauración de Clave para Colegio Nueva Andalucía, Aplicativo EVI DANE:325754001549. Se genera nuevo caso SOL806785. Resuelto 20 de octubre de 2023. Se tiene envio en texto plano del usuario y clave. 3. SOL814531 de fecha 15 de noviembre de 2023. Corrección del participante Ana Cristina González con respecto a la fecha de nacimiento. Se solucionó el mismo día, no se indica porque se presentaba el error, 4. SOl814420 de fecha 15 de noviembre, se indica que se presentó incidente pero el incidente presentado corresponde al: 814296. No está toda la información de la atención. y gestión de lecciones aprendidas Lo anterior incumpliendo con lo establecido en la norma ISO IEC 27001:2013 en el numeral 8.1

AUDITORIA SISTEMAS DE GESTIÓN DE CALIDAD / AMBIENTAL Y OTROS MODELOS REFERENCIALES				
Resultado			Requisito o Numeral	Descripción
C	NC	OM		
		X	A.6.1.2	Garantizar la segregación de deberes entre el oficial y el área de TI
		X	A.6.1.1	Diligenciar completamente la Matriz de roles y responsabilidades de seguridad de la información el documento en la matriz no tiene la información de experiencia, educación y habilitades, en todos dice N.A.
		X	A.8.1.1	Completar el inventario de activos de información, dado que se deben identificar tanto el contenedor como el contenido, falta entre otros: Código fuente, SharePoint, OneDrive, Backups, Licencia de Office, Documentación de los procesos.
	X		A.11.1.1	No se evidencia que se tenga una protección adecuada contra accesos no autorizados al DataCenter, lo cual se soporta en que la puerta del DataCenter se encuentra daña, lo anterior incumple con lo establecido en la norma ISO IEC 27001:2013 en el control A.11.1.1
	X		A.11.1.4	No se tiene un control adecuado contra amenazas externas y ambientales, lo cual se soporta en que: 1. Los extintores del DataCenter se encuentran vencidos desde el 2020 2. Se tienen cajas y elementos inflamables dentro del DataCenter 3. Dentro de los centros de Cableado se encuentra un Servidor para las Cámaras sobre ICOPOR 4. En el centro de Cableado del ala Oriental se tiene aire acondicionado que indica temperatura de 18ºC; sin embargo, no se evidencia que se sople viento Lo anterior incumpliendo con lo establecido en el control A.11.1.4 de la norma ISO IEC 27001:2013
		X	A.11.1.4	Validar si los extintores de los centros de cableado, dan la capacidad para lo allí alojado.
		X	A.11.2.3	Garantizar que el diagrama de elementos ubicados en el DataCenter y el Diagrama de

AUDITORIA SISTEMAS DE GESTIÓN DE CALIDAD / AMBIENTAL Y OTROS MODELOS REFERENCIALES				
Resultado			Requisito o Numeral	Descripción
C	NC	OM		
				Topología se encuentre con el mismo etiquetado que se encuentra en el etiquetado del cableado.
		X	A.13.1.1	Validar porque se puede realizar la navegación en TIKTOK si se tiene la parametrización para el bloqueo de ingreso a estas páginas.
		X	A.14.1.1	Garantizar que se tengan claramente identificados los aspectos de seguridad de la información que se deben tener en los desarrollos nuevos o para mejoras de los sistemas existentes
	X		A.9.4.5	No se tiene un control adecuado del código fuente, lo cual se soporta en que: 1. No se tiene evidencia de la versión del código fuente del proyecto SISMA Fase 2 2. Se tiene acceso de personal que ya no está en la organización o que no es del área de TI Lo anterior incumpliendo con lo establecido en la norma ISO IEC 27001:2013 en el control A.9.4.5
		X	A.14.2.2	Garantizar que en la documentación del Rollback se encuentren documentados todos los aspectos a realizar.
	X		A.9.3.1	No se evidencia un control adecuado de las claves, lo cual se soporta en que se tiene un block de notas con las contraseñas para el ingreso a aplicativos del Ministerio por parte de un Profesional de la Oficina, lo anterior incumpliendo con lo establecido en la norma ISO IEC 27001:2013 en el control A.9.3.1
		X	A.9.2.6	Garantizar que todo cambio de rol y de usuarios queda debidamente soportado
	X		A.10.1.1 A.10.1.2	No se evidencia que se lleve un manejo adecuado de la criptografía lo cual se soporta en que en la política ST-GU-10 Guía Política de uso de controles criptográficos, se indica: se cifran los discos duros, información digital reservada y clasificada y el correo electrónico; sin embargo al revisar, no se tiene etiquetado de la información clasificada

AUDITORIA SISTEMAS DE GESTIÓN DE CALIDAD / AMBIENTAL Y OTROS MODELOS REFERENCIALES				
Resultado			Requisito o Numeral	Descripción
C	NC	OM		
				y reservada por tal razón no se está aplicando, a los correos tampoco se ha dado la instrucción para esto y el responsable indica que no se hace. Lo anterior incumpliendo con lo establecido en la norma ISO IEC 27001:2013 en los controles A.10.1.1 y A.10.1.2
	X		A.12.1.3	No se evidencia una correcta gestión de capacidades, lo cual se soporta en que: "Se tiene infartado el monitoreo de canales de Fusagasuga, Uribia y Sincelejo lo anterior segun lo informado porque está en proceso de traslado, no se tiene seguimiento de esta gestión, lo anterior incumpliendo con lo establecido en la Norma ISO IEC 27001:2013 en el Control A.12.1.3
		X	A.12.3.1	Garantizar que se utiliza el ultimo Formato ST-FT-16 Listado Full de Políticas para la programación de Backups
	X		A.15.1.3	No se evidencia que se realice la divulgación de las políticas de seguridad de la información a la cadena de suministros; esto soportado en que la empresa que realiza la custodia de los Backups es Alpopular que fue contratado por Grow Data quien trabaja para Infotic y no se tiene evidencia de la divulgación de las políticas. Lo anterior incumpliendo con lo establecido en la norma ISO IEC 27001:2013 en el control A.15.1.3
		X	A.16.1.3	Garantizar que las amenazas reportadas por los dispositivos perimetrales y antivirus son gestionados de manera adecuada.
	X		A.12.6.1	No se evidencia que las vulnerabilidades que no tienen plan de remediación sean tratadas como riesgos, lo anterior incumpliendo con lo establecido en la Norma ISO IEC 27001:2013 en el control A.12.6.1
	X		A.12.4.3	No se tiene log de auditoría de los sistemas de información, lo anterior incumpliendo con lo establecido en la norma ISO IEC 27001:2013 en el control A.12.4.3
	X		A.17.1. A.17.2.	No se tiene un plan de continuidad, ni pruebas de continuidad y contingencia, lo

AUDITORIA SISTEMAS DE GESTIÓN DE CALIDAD / AMBIENTAL Y OTROS MODELOS REFERENCIALES				
Resultado			Requisito o Numeral	Descripción
C	NC	OM		
				anterior incumpliendo con lo establecido en la norma ISO IEC 27001:2013 en los objetos de control A.17.1 y A.17.2
	X		A.18.1.2	No se evidencia un control sobre derechos de autor, lo cual se soporta en que en el equipo de un Profesional de la Oficina, se tiene guardada música, lo anterior incumpliendo con la norma ISO IEC 27001:2013 en el control A.18.1.2

LÍDER DEL EQUIPO AUDITOR: Alexandra Bibiana Cala

JEFE OFICINA DE CONTROL INTERNO: Luis Alfredo Contreras