INFORME DE AUDITORIA SEGURIDAD DE LA INFORMACIÓN

Información General de la Auditoría	
Área	**Área de Tecnologías y Sistemas de la Información**
Responsable	Sonia Cardozo
Fecha de Inicio	01-Dic-2021
Alcance	el Área de Tecnología y Sistemas de la Información en un periodo de siete (7) días y de manera virtual, en el cual se validará el cumplimiento de lo siguiente: ▪ Evaluación del cumplimiento de los requisitos 4 al 10 de la norma ISO/IEC 27001:2013 ▪ Evaluación del cumplimiento de los controles del anexo A de la norma ISO/IEC 27001:2013
Objetivo	Evaluar el Sistema de Gestión de Seguridad de la Información – SGSI alineado a las prácticas lideres ISO 27000
Criterio de Auditoría	Integralidad en la norma ISO 27001:2013.
Equipo Auditor	Edinson Murillo Albornoz – Auditor Líder Maria Alejandra Suarez Rojas – Auditora (contratista)

Generalidades desarrollo y metodológico de la auditoría.

Para el desarrollo de la auditoría se llevaron a cabo las siguientes actividades:

- Reunión de apertura con la presentación del plan de auditoría, equipo auditor, personal a entrevistar y cronograma de reuniones.
- Entrevistas virtuales con el personal responsable de los respectivos procesos involucrados en el SGSI.
- Revisión de evidencias y documentación suministrada.
- Reunión de cierre y presentación de resultados.

1. Evidencias solicitadas.

- Socialización de políticas de seguridad de la información.
- Procedimientos relacionados con seguridad de la información
- Resolución interna G-Suite
- Sesiones realizadas con MinTic
- Capacitaciones institucionales
- Matriz activos de información
- Matriz de riesgos de seguridad de la información
- Informe de vulnerabilidades
- Actas de comité.

2. Revisión de evidencias

Las evidencias solicitadas fueron validadas durante y en el transcurso de los días que fue desarrollada la auditoria.

Aquellas validadas durante, se evidenciaron a través de pantalla compartida durante la sesión y las solicitadas fueron cargadas en plataforma Drive licenciada por la Entidad en la cual fue otorgado el acceso para la visualización y validación.

3. Conclusión:

1. OBSERVACIONES.
4 CONTEXTO DE LA ORGANIZACIÓN • No se determina partes interesadas externas del SGSI, a la fecha se encuentra en construcción. • El proceso no se encuentra caracterizado, sin embargo, el área cuenta con un documento borrador en donde se están definiendo los elementos esenciales de su funcionamiento. • No se presenta evidencia de Resolución interna 316 del 2019, en donde se identifique la creación del área y sus funciones. **5 LIDERAZGO** • Si bien se informan actividades puntuales en los Comités Institucional de Gestión y Desempeño, no se comunica sobre el desempeño del sistema de gestión de seguridad de la información. • La política y manual de seguridad y privacidad de la información adoptada por la Entidad, carece de los siguientes aspectos: compromiso de mejora continua, roles y

responsabilidades de los colaboradores institucionales sobre el cumplimiento de los aspectos relacionado con seguridad de la información.

6 PLANIFICACIÓN

La matriz de riesgos de seguridad de la información carece de un control de versión

7 SOPORTE

- Carencia de soporte documental requerido por la norma y los controles del anexo A para la gestión de seguridad de la información

A.15 RELACIONES CON LOS PROVEEDORES

- No se evidencia lineamientos de seguridad para la cadena de suministros y proveedores
- No se evidencia lineamientos para el monitoreo o seguimiento en la gestión de cambio de los proveedores

A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

- No se evidencia el cumplimiento del procedimiento en cuanto a notificación y uso de los canales formales establecidos
- No se evidencia gestión de conocimiento y costeo de incidentes de seguridad de la información
- Debilidad en la gestión de evaluación y aprendizaje de los eventos de seguridad

A.18 CUMPLIMIENTO

La Revisión del cumplimiento técnico de políticas a los sistemas de información se realiza, sin embargo no se encuentra documentada

2. NO **CONFORMIDADES**

4 CONTEXTO DE LA ORGANIZACIÓN

- No se evidencia la composición y adopción formal del sistema de seguridad de la información dentro de la Entidad.

5 LIDERAZGO

- No se identifica la formalización del rol como líder de seguridad de la información
- No se cuenta con documentación formal respecto a roles y responsabilidades de seguridad de la información.

6 PLANIFICACIÓN

No se evidencia lineamientos documentados para

- Acciones destinadas a la gestión de riesgos y oportunidades
- Evaluación de la eficacia y eficiencia de controles
- Tratamiento de riesgos y oportunidades

No se evidencia documentación de gestión y seguimiento de los riesgos asociados a seguridad de la información.

No se identifica la aprobación del plan de tratamiento de riesgos de la seguridad de la información, y la aceptación de los riesgos residuales de la seguridad de la información por parte de los dueños de los activos de información.

7 SOPORTE

- No se evidencia el proceso o procedimiento para determinar la competencia necesaria de las personas que efectúan las gestiones de seguridad de la información
- No se evidencia un programa de toma de conciencia o apropiación por parte de los colaboradores en seguridad de la información
- No se evidencia una gestión de comunicación a los colaboradores o partes interesadas en los referente a seguridad de la información
- Carencia de soporte documental requerido por la norma y los controles del anexo A para la gestión de seguridad de la información

8 OPERACIÓN

- No se evidencia una planificación para la implementación y control de los procesos necesarios para cumplir con los requisitos de seguridad de la información
- No se evidencia una valoración a intervalos planificados de los riesgos de seguridad de la información con criterios establecidos
- No se evidencia un plan de tratamiento de los riesgos de seguridad de la información

10 MEJORA CONTINUA

- No se evidencia seguimiento y monitoreo a la gestión de los lineamientos definidos en la política de seguridad de la información
- No se está verificando la efectividad del SGSI, sin embargo, en el comte de gestión y desempeño se plantean actividades para desarrollar correspondientes a seguridad de la información.
- No se evidencia mecanismos, lineamientos o procedimientos para la mejora continua del SGSI

A.5 POLÍTICAS DE LA SEGURIDAD DE LA INFORMACION

- No se evidencia seguimiento y monitoreo a la gestión de los lineamientos definidos en la política de seguridad de la información.

A.7 SEGURIDAD DE LOS RECURSOS HUMANOS

- No se evidencia cláusulas contractuales de seguridad de la información en la gestión de contratos de la entidad
- No se evidencia comunicaciones de actualizaciones o novedades en la documentación del SGSI
- No se evidencia lineamientos o procedimientos al respecto de procedimientos disciplinarios por incumplimiento o violación a las políticas del SGSI

A.8 GESTIÓN DE ACTIVOS

No se evidencia lineamientos formales para la gestión de activos de la información respecto a

- Teletrabajo o trabajo remoto (solicitudes de acceso a VPN)
- Tiempos de retención
- Retiro de activos de las instalaciones
- Destrucción de activos de información

No se evidencian lineamientos para la clasificación y etiquetado de la información

No se evidencian lineamientos para la disposición final de los activos

A.12 SEGURIDAD DE LAS OPERACIONES

- No se evidencio documentación y administración de los procedimientos de Backup
- No se evidencia respaldo de los logs de auditoría de servicios o infraestructuras criticas
- No se evidencia registro y seguimiento a la instalación de firmware, parches o actualizaciones de fabricantes

A.13 SEGURIDAD DE LAS COMUNICACIONES

- No se evidencia gestión de herramientas para prevenir la pérdida o fuga de datos en redes.
- No se establece evidencia sobre la segmentación de redes para los grupos de servicios de información, usuarios y sistemas de información.

A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

- No se evidencia un repositorio formal para el almacenamiento de código fuente
- No se evidencia lineamientos o procedimientos para el desarrollo seguro interno o de terceros y proveedores

A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO

- No se evidencian lineamientos para la seguridad de la información en contingencia

A.18 CUMPLIMIENTO

No se identifica un monitoreo y gestión del cumplimiento de requisitos normativos o legales.

No se evidencia seguimiento a la gestión legal y normativa referente a

- derechos de autor
- licenciamiento de software
- Privacidad de la información
- Derechos patrimoniales e intelectuales del software
- Decreto 612 de 2018

La Revisión del cumplimiento técnico de políticas a los sistemas de información se realiza, sin embargo no se encuentra documentada

3. HALLAZGOS

4. RECOMENDACIONES

Identificar y documentar:

- El contexto interno y externo de la entidad respecto a seguridad de la información.
- Necesidades y expectativas de las partes interesadas en seguridad de la información.
- Establecer de manera formal el Sistema de Gestión de Seguridad de la Información, en donde se defina su alcance, objetivos, cumplimiento, mantenimiento y mejora continua

Formalizar el responsable de la gestión de seguridad de la información

- Personal idóneo con independencia de la gestión de controles
- Conocimiento y experiencia en la gestión de seguridad de la información
- Experiencia en la gestión y liderazgo de sistemas de gestión
- Conocimiento y experiencia en gestión de riesgos e incidentes de seguridad de la información

Definir y documentar los roles y responsabilidades en seguridad de la información para todos los colaboradores de la entidad

- Gestores/lideres de procesos
- Colaboradores institucionales

Definir y documentar un proceso gestión de riesgos de seguridad de la información que contemple pero no se limite a:

- Contexto interno, externo y las partes interesadas
- Valoración del riesgo incluyendo probabilidad e impacto entre otros
- Tratamiento y control de los riesgos
- Monitoreo y seguimiento

Definir y documentar el seguimiento y eficacia de las acciones implementadas en los controles establecidos.

Establecer y documentar una declaración de aplicabilidad que contenga los controles necesarios y la justificación de las inclusiones, ya sea que se implementen o no, y la justificación para las exclusiones de los controles del Anexo A de la ISO 27001:2013.

Documentar y publicar los procesos o procedimientos para el cumplimiento de los requisitos de los colaboradores en seguridad de la información.

Diseñar y documentar un plan de toma de conciencia o apropiación en seguridad de la información para las partes interesadas.

Construir y publicar los documentos mínimos necesarios para la gestión de la seguridad de la información alineado a las practicas lideres entre estas ISO 27001:2013 y MSPI.

Determinar, documentar las necesidades internas y externas del SGSI mediante plan de comunicaciones.

Diseñar, documentar y hacer seguimiento a un plan para la implementación del modelo de seguridad de la información que permita monitorear y dar cumplimiento a los controles necesarios para mantener la Confidencialidad, Integridad y Disponibilidad de la información.

Realizar una gestión de riesgos de seguridad de la información donde se contemple la identificación, valoración, tratamiento, seguimiento a los riesgos de seguridad de la información bajo una metodología entre otras:

- ISO27005
- ISO31000

Realizar medición y seguimiento a la implementación de los controles mediante:

- Generación de indicadores
- Auditorías internas y externas

No conformidades y Acciones correctivas

- Gestión de NC-OM
- Evaluar la necesidad de tomar acciones para la mejora
- Revisar la eficacia de las AC o planes de mejora

Realizar medición y seguimiento periódico a la implementación de los controles mediante:

- Generación de indicadores
- Auditorías internas y externas
- GAP- Análisis de brechas - Autodiagnósticos
- Seguimiento de las políticas del SGSI aprobadas

Establecer y documentar cláusulas contractuales de seguridad de la información en los contratos de la Entidad con las partes interesadas (entre estas pero no limitándose a funcionarios, contratistas, proveedores)

- Acuerdo de confidencialidad para los contratos de acuerdo marco
- Cumplimiento a políticas y lineamientos
- Lineamientos de privacidad y no divulgación

Diseñar y documentar plan de comunicaciones referente a la gestión y novedades del SGSI

Definir y documentar lineamientos o procedimientos disciplinarios por incumplimiento a políticas o lineamientos de seguridad de la información por las partes interesadas.

Definir y documentar lineamientos para la gestión de activos de información incluyendo pero no limitándose a:

- Gestión de medios removibles
- Retiro y manipulación externa
- En trabajo remoto o fuera de la entidad
- Tiempos de retención (TRD)
- Clasificación y etiquetado de la información física, electrónica o digital
- Borrado seguro y destrucción física

Registrar de forma centralizad los Job y actividades de respaldo de información.

Centralizar y administrar los Log de auditoría de los servicios e infraestructuras críticas de forma que permita la correlación de eventos entre los dispositivos (SIEM - Sincronización de relojes)

Administrar, instalar, registrar y probar de forma periódica las actualizaciones emitidas por fabricantes de servicios, infraestructura o software de proveedores.

Construir y administrar mecanismos de protección para la pérdida o fuga de información entre estos pero limitándose a:

- Cifrado de información en tránsito con gestión de llaves
- Procedimientos para transferencia de información
- Acceso limitado a redes y servicios de red

Definir lineamientos y acuerdos documentados para la transferencia de información clasificada - Confidencial para

- Usuarios
- Proveedores
- Partes interesadas
- En redes publicas

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 servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.

Construir, administrar y documentar un repositorio de almacenamiento, control de código y versiona miento de los desarrollos internos.

Definir lineamientos y documentar mediante registro la validación de desarrollo seguro aliando a prácticas lideres (OWASP)

Definir lineamientos para la auditoria y pruebas de software interno o de proveedores

- Análisis de vulnerabilidades
- Pentest

Identificar, documentar y gestionar los riesgos asociados a la cadena de suministro de servicios o equipos de tecnología.

Diseñar y documentar procedimientos o mecanismo de validación para asegurar que los productos, equipos o servicios cumplen los requisitos de seguridad en la cadena de suministros.

Definir y documentar lineamientos o procedimientos de validación o ANS para la gestión de cambio en los terceros o proveedores.

Realizar y registrar la evidencia referenciada en el procedimiento de gestión de incidentes de seguridad de la información, aplicar como guía ISO 27035.

Generar un banco de lecciones aprendidas o gestión del conocimiento con base en la atención y control de incidentes de seguridad.

Incluir en el plan de cultura o apropiación el reporte y gestión de eventos e incidentes desde los usuarios finales.

Definir y documentar estrategias o planes de contingencia que incluyan pero no se limiten a:

- Estrategias de seguridad de la información en contingencia o crisis
- Sistemas de información críticos
- Servicios y procesos críticos
- Comunicación en contingencia
- Desastres tecnológicos
- Copias de seguridad y restauración

Identificar y documentar a través del normograma institucional los requisitos legales, normativos y regulatorios relevantes para la seguridad de la información y la operación de los procesos de la entidad, incluyendo pero no limitándose a:

- Privacidad – Habeas data
- Delitos informáticos
- Confidencialidad de la información
- Derechos de autor y licenciamiento de software – CMDB o inventario de software

Revisar y documentar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información

4. RESUMEN	
OBSERVACIONES	13
NO CONFORMIDADES	
HALLAZGOS	N/A
RECOMENDACIONES	37
Análisis de la Oficina de Control Interno:	

RESPONSABLES

Maria Alejandra Suarez
Nombre auditora
Oficina de Control Interno

EdinsonMurilloA
Edinson Murillo Albornoz
Jefe de la Oficina
Oficina de Control Interno.

Elaboró: Maria Alejandra Suarez
Revisó: Edinson Murillo Albornoz Jefe de Control Interno
Aprobó: Edinson Murillo Albornoz
Fecha de aprobación: 21 de diciembre de 2021