FECHA DE INFORME:	Mayo 07 de 2020
PROCESO Y/O DEPENDENCIA:	Gestión Tecnológica de la información y comunicaciones
LÍDER DEL PROCESO Y/O DEPENDENCIA:	Coronel (RA) Sonia Dolly Gutierrez Carrillo
TEMA DE SEGUIMIENTO:	Implementación de la normatividad vigente frente a Gobierno Digital

NORMATIVIDAD:

- Manual de Gobierno Digital
- Modelo de seguridad y Privacidad de la información en adelante (MSPI) MINTIC
- Plan de Seguridad y Privacidad de la Información 2019
- Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información Vigencia 2019
- Herramienta Suite Visión Empresarial ALFM / Gestión de TIC / vigencia 2019
- Centro Documental: Actas de Comité Institucional de Gestión y Desempeño de la Entidad.
- Carpeta compartida \\san-nas2\AUTODIAGNOSTICOS_MIPG
- Resolución 254 del 5 de marzo de 2019 fue derogada mediante Resolución No.446 de fecha 04-03-2020

JUSTIFICACIÓN DEL SEGUIMIENTO:

En cumplimiento de las instrucciones emitidas por la Dirección General mediante memorandos No.20202000175383 de fecha 02-04-2020 y 20201000188733 de fecha 14-04-2020 en cuanto recomendar una herramienta idónea para adoptar medidas que permitan evitar situaciones delictivas.

GESTIÓN / ACCIONES DEL SEGUIMIENTO:

Mediante memorando No.20201200198943 de fecha 20 de abril 2020 se realiza apertura de auditoria y se realiza solicitud de información correspondiente al soporte de la gestión y nivel de madurez de seguridad y privacidad de la información al interior de la ALFM, Identificación de vulnerabilidades técnicas y administrativas que sirvieron como insumos para la fase de planificación y que dieron lugar a la formulación de los Planes publicados en la SVE con sus respectivos soportes o estado de avance para cada una de las actividades relacionadas a continuación:

1. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2019

- Documento de definición del MSPI
- Documento con la política general actualizada.
- Documento inventario de activos dentro del alcance del MSPI.
- Entrega cuatrimestral del documento Identificar las amenazas a los nuevos activos.
- Análisis y evaluación de los riesgos asociados de acuerdo al impacto que pueden generar y a la probabilidad de ocurrencia para los nuevos activos identificados.
- Análisis y evaluación de los riesgos asociados de acuerdo al impacto que pueden generar y a la probabilidad de ocurrencia para los nuevos activos identificados.
- Obtener la aprobación de la Dirección sobre los nuevos riesgos residuales determinada.
- Elaborar la declaración de aplicabilidad (SoA).
- Actualizar el Plan de Tratamiento de Riesgos
- Plan y ejecución de sensibilización, capacitación y apropiación del MSPI, para toda la entidad.

2. PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN VIGENCIA 2019

- Plan y ejecución de capacitación y sensibilización a usuarios sobre temas de seguridad informática y riesgos informáticos.
- Estado de la adquisición del dispositivo, el cual protegerá los aplicativos webs de la ALFM.
- Estado de la migración de IPv4 a protocolo IPv6.

Además de allegar las actas de reunión llevadas a cabo en cumplimiento de las funciones del Comité de seguridad de la información ALFM Resolución No.254 de 2019.

Lo anterior con plazo de entrega miércoles 22-04-2020 a las 2 pm el cual a la fecha 29-04-2020 no se recibió respuesta por parte de la Oficina de Tecnologías de la información y comunicaciones. Incumplimiento enmarcado en la **Ley 734/2002 Artículo 35.** Prohibiciones. *A todo servidor público le está prohibido: (…)*
8. Omitir, retardar o no suministrar debida y oportuna respuesta a las peticiones respetuosas de los particulares o a solicitudes de las autoridades, así como retenerlas o enviarlas a destinatario diferente de aquel a quien corresponda su conocimiento.

Para el desarrollo del seguimiento se tuvieron en cuenta los siguientes insumos:

- Herramienta Suite Visión: reporte de Planes / Gestión de TIC / vigencia 2019
- Modelo de Seguridad y Privacidad de la información MINTIC
- Centro Documental: Actas de Comité Institucional de Gestión y Desempeño de la Entidad.
- Carpeta compartida \\san-nas2\AUTODIAGNOSTICOS_MIPG

OBSERVACIONES Y/O SUGERENCIAS:

Una vez analizada la información contenida en la normatividad del Ministerio de TIC, se precisa que la estrategia de Gobierno en Línea, tiene como objetivo, garantizar el máximo aprovechamiento de las

tecnologías de la información y las comunicaciones, con el fin de contribuir con la construcción de un Estado más participativo, más eficiente y más transparente. A través del decreto único reglamentario 1078 de 2015, del sector de Tecnologías de Información y las Comunicaciones, se define el componente de seguridad y privacidad de la información, como parte integral de la estrategia GEL.

Por lo anterior para el desarrollo de la presente verificación, se toma como punto referencia, las 5 fases de implementación del Modelo de Seguridad y Privacidad de la información: **Diagnostico, Planificación, Implementación, Evaluación de Desempeño y Mejora Continua**, adelantados por la ALFM, en cumplimiento de los lineamientos establecidos por MINTIC y lo establecido por la Oficina de TICS para la ALFM mediante documento Código GTI-MO-01 Versión 00 y 01 del (MSPI) y lo referente a la protección de la información y el tratamiento de los riesgos de seguridad de la información.

1. Dentro del documento Excel autodiagnóstico Gobierno Digital 02-07-2019 en las filas E69 A E92 se evalúa el componente de Seguridad y privacidad de la información con un 100% sin embargo no se evidencian soportes que respalden la evaluación.

   Dentro de las evidencias enmarcadas en las actividades del Plan de Seguridad y Privacidad de la Información, se encuentra el documento con Código: GTI-MO-01 firmado de fecha 31-12-2019 el cual contiene el Modelo de Seguridad y Privacidad de la información, sin embargo, no se encuentra publicado en la Herramienta Suite Visión Empresarial en el reporte Documentos del proceso Gestión TICs, además que las siglas MO no se encuentra enmarcadas dentro de la Guía para la Elaboración de Documentos del Sistema Integrado de Gestión Código GI-GU-03 sub numeral 4.2.2 Tipos de Documentos.

MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – MSPI

2. En la herramienta Suite Visión Empresarial, Menú Planes/Planificación/Planes, en el Plan de Seguridad y Privacidad de la información versión 1, se encuentra el inventario de **activos de la Información** numeral 3. IDENTIFICACIÓN Y VALORACIÓN DE LOS ACTIVOS TECNOLÓGICOS documento con Código: GTI-MO-01, donde se evidencio activos que no se tienen contemplados, entre otros, así:

- Actas de sub Comité de Control Interno Regionales
- Actas de Administrativas y de Directivos
- No se evidencia la información como propiedad de la Subdirección de Operaciones Logísticas
- Concertación de menús
- Informes de punto de equilibrio
- Auditorias de Gestión, Puntuales y/o de Reacción Inmediata
- Informes de Ley

El Comité de Seguridad de la Información tiene por Objeto la formulación, aprobación y seguimiento a las políticas, planes y proyectos que requiera la Entidad en materia de seguridad de la información, así la aprobación de modificaciones o cambios que afecten los sistemas de información y de la Integración del MSPI con el Sistema de Gestión documental que deben ser tenidos en cuenta para la vigencia 2020.

La Resolución 254 del 5 de marzo de 2019 fue derogada mediante Resolución No.446 de fecha 04-03-2020 y no se determinó donde se concentraran las funciones del mencionado Comité.

En las actas del Comité de Institucional de Gestión y Desempeño de la ALFM, se evidenció el seguimiento a los planes en contexto de Gobierno Digital.

3. En la **Política de Administración de Riesgos** numeral 4. PROBABILIDAD E IMPACTO DE LAS AMENAZAS Y ESTIMACIÓN DEL NIVEL DE RIESGO documento Código: GTI-MO-01 se evidencia que no se cuenta con fechas establecidas para la evaluación y/o actualización de acuerdo a lo establecido en la Resolución 254 del 5 de marzo de 2019 Artículo 4. numeral 9. Realizar revisiones periódicas del Modelo de Seguridad y Privacidad de la Información (por lo menos una vez al año) y según los resultados de esta revisión definir las acciones pertinentes.

Frente a la administración del Riesgo en la herramienta Suite Visión administra 3 Riesgos:
- Alteración o manipulación de sistemas y datos
- Pérdida, daño, manipulación o sustracción de información o de equipos tecnológicos
- Interrupción del servicio de la plataforma tecnológica

Sin embargo, en el documento MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – MSPI versión 01 Código: GTI-MO-01, el cual guarda relación con lo estipulado en la guía del MSPI emitida por MINTIC; se establecen riesgos que no son administrados por los responsables de los Procesos y liderados por Gestión TIC, los cuales se evidencia en la clasificación de acuerdo a la valoración en el mapa de calor, donde en los valores más altos se representan con un color rojo, que indica que son los riesgos prioritarios y a los que se debe dar tratamiento, así:

Cód. Grupo	**AMENAZAS**	**PROB.**	**IMPACTO**			**RIESGO**		
			[C]	**[I]**	**[D]**	**[C]**	**[I]**	**[D]**
[D] Datos								
Archivos	Errores de los usuarios	4	4	5	3	16	20	12
	Abuso de privilegios de acceso	3	4	5	3	12	15	9
Copias de respaldo	Errores de los usuarios	3	4	5	3	12	15	9
	Abuso de privilegios de acceso	3	4	5	3	12	15	9
Credenciales	Abuso de privilegios de acceso	3	4	5	3	12	15	9
Código fuente	Abuso de privilegios de acceso	3	4	5	3	12	15	9
[S] Servicios								
Al público en general	Errores de los usuarios	3	4	5	3	12	15	9
Interno	Errores de los usuarios	3	4	5	3	12	15	9
Externo	Errores de los usuarios	3	4	5	3	12	15	9
[SW] Software								
Servidor de presentación	Avería de origen físico o lógico	3			5			15
	Difusión de software dañino	4	4	4	4	16	16	16
Servidor de aplicaciones	Avería de origen físico o lógico	3			5			15
	Difusión de software dañino	4	4	4	4	16	16	16
Cliente de correo electrónico	Avería de origen físico o lógico	3			5			15
	Difusión de software dañino	4	4	4	4	16	16	16
Servidor correo electrónico	Avería de origen físico o lógico	3			5			15
	Difusión de software dañino	4	4	4	4	16	16	16
Gestor de base de datos	Avería de origen físico o lógico	3			5			15
	Difusión de software dañino	4	4	4	4	16	16	16

Cód. Grupo	AMENAZAS	PROB.	IMPACTO			RIESGO		
			[C]	[I]	[D]	[C]	[I]	[D]
Ofimática	Avería de origen físico o lógico	3			5			15
	Difusión de software dañino	4	4	4	4	16	16	16
Antivirus	Avería de origen físico o lógico	3			5			15
Sistema operativo	Avería de origen físico o lógico	3			5			15
	Difusión de software dañino	4	4	4	4	16	16	16
Sistema de backup	Avería de origen físico o lógico	3			5			15
	Difusión de software dañino	4	4	4	4	16	16	16
[HW] Hardware								
Grandes equipos	Pérdida de equipos-Robo	3	4		5	12		15
	Manipulación de los equipos	3	3	5		9	15	
Equipos medios	Pérdida de equipos-Robo	3	4		5	12		15
	Manipulación de los equipos	3	3	5		9	15	
Informática personal	Pérdida de equipos-Robo	3	4		5	12		
Informática móvil	Pérdida de equipos-Robo	3	4		5	12		15
Equipamiento de respaldo	Pérdida de equipos-Robo	3	4	5		12		15
	Manipulación de los equipos	3	3	5		9	15	
Medios de impresión	Pérdida de equipos-Robo	3	4		5	12		15
	Manipulación de los equipos	3	3	5		9	15	
Escáneres	Pérdida de equipos-Robo	3	4		5	12		15
	Manipulación de los equipos	3	3	5		9	15	
Dispositivos criptográficos	Pérdida de equipos-Robo	3	4		5	12		15
	Manipulación de los equipos	3	3	5		9	15	
Conmutadores	Pérdida de equipos-Robo	3	4		5	12		15
	Manipulación de los equipos	3	3	5		9	15	
Enrutadores	Pérdida de equipos-Robo	3	4		5	12		15
	Manipulación de los equipos	3	3	5		9	15	
Cortafuegos	Pérdida de equipos-Robo	3	4		5	12		15
	Manipulación de los equipos	3	3	5		9	15	
Centralita telefónica	Pérdida de equipos-Robo	3	4		5	12		15
	Manipulación de los equipos	3	3	5		9	15	
[Media] Soportes de información								
Discos	Avería de origen físico o lógico	3			5			15
	Errores de los usuarios	3	5	5	3	15	15	9
Almacenamiento en red	Avería de origen físico o lógico	3			5			15
Dvd	Avería de origen físico o lógico	3			5			15
	Errores de los usuarios	3	5	5	3	15	15	9
Cinta magnética	Avería de origen físico o lógico	3			5			15
Material impreso	Avería de origen físico o lógico	3			5			15
	Errores de los usuarios	3	5	5	3	15	15	9

Fuente: Documento MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – MSPI versión 01

4. **Controles**

Se evidencia en el documento Código: GTI-MO-01 numeral 5. APLICACIÓN DE CONTROLES, evaluación de controles establecidos en la entidad que no se encuentran al 100% de aplicación y no se cuenta con una programación para su tratamiento y/o actualización, a continuación, se relacionan dichos controles:

Control	Pregunta existencia control	Si	No	% cumplim.
6.1 Organización interna				
6.1.1 Asignación de responsabilidades para la seguridad de la información	¿Existen responsables para cada rol dentro del sistema de seguridad de la información?	X		90%
6.1.2 Segregación de tareas	¿Cada persona conoce sus funciones dentro del sistema?	X		90%
Contacto con grupos de interés especial	¿Se conocen las personas, datos de contacto y grupos de interés especial?	X		90%
6.2 Dispositivos para movilidad y teletrabajo				
para movilidad	¿Existe una política para el uso de dispositivos móviles? (tabletas, portátiles, celulares institucionales)		X	20%
6.2.2 Teletrabajo	¿Existen lineamientos que permitan el teletrabajo?		X	50%
7.3 Cese o cambio de puesto de trabajo				
7.3.1 Cese o cambio de puesto de trabajo	¿Existen los procedimientos a seguir en caso de cambio de puesto de trabajo o cese del mismo?	X		90%
8.2 Clasificación de la información				
8.2.2 Etiquetado y manipulado de la información	¿Se tienen implementado un procedimiento para el etiquetado de la información?			90%
8.3 Manejo de los soportes de almacenamiento				
8.3.2 Eliminación de soportes	¿Se cuenta con un procedimiento para la disposición final de los soportes extraíbles?		X	20%
8.3.3 Soportes físicos en tránsito	¿Se controla la tenencia de los soportes extraíbles?	X		50%
9. CONTROL DE ACCESOS				
9.1 Requisitos de negocio para el control de accesos				
9.1.1 Política de control de accesos	¿La empresa posee una política de control de accesos?	X		90%
9.1.2 Control de acceso a las redes y servicios asociados	¿Se tiene control sobre los accesos a las redes por parte personas internas y externas a la compañía?	X		90%
9.2 Gestión de acceso de usuario				
9.2.2 Gestión de los derechos de acceso asignados a usuarios	¿Se tiene un reporte de los procesos realizados por cada usuario en los Sistemas de información?	X		90%
9.2.3 Gestión de los derechos de acceso con privilegios especiales	¿La empresa realiza gestión de altas/bajas en el registro de usuarios?	X		90%
9.2.5 Revisión de los derechos de acceso de los usuarios	¿Se realiza una revisión periódica de los logs de acceso a las diferentes herramientas o sistemas de información?	X		70%
11. SEGURIDAD FÍSICA Y AMBIENTAL				
11.1 Áreas seguras				
11.1.6 Áreas de acceso público, carga y descarga	¿El lugar donde se realiza el despacho y carga de herramientas (computadores, teclados, entre otros), cuenta con medidas de seguridad?	X		90%
11.2 Seguridad de los equipos				
11.2.1 Emplazamiento y protección de equipos	¿La infraestructura eléctrica se encuentra bien instalada y sin riesgos?	X		90%

Control	Pregunta existencia control	Si	No	% cumplim.
11.2.2 Instalaciones de suministro	¿Los equipos informáticos y accesos de red, están seguros?	X		90%
11.2.3 Seguridad del cableado	¿Se tienen medidas de protección hacia el cableado eléctrico y de datos?	X		90%
11.2.6 Seguridad de los equipos y activos fuera de las instalaciones	¿Cuándo un activo es sacado de la empresa, este cuenta con las medidas de seguridad en caso de tener pérdida?	X		90%
11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento	¿Se realiza un backup y limpieza de los equipos de cómputo antes de entregarlo a otra persona?	X		90%
11.2.8 Equipo informático de usuario desatendido	¿Los equipos que no tienen personal asignado se les dan una protección adecuada?	X		90%
11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla	¿Se tiene una política de escritorio limpio para los papeles y medios de almacenamiento removibles?	X		90%
12. SEGURIDAD EN LA OPERATIVA				
12.1 Responsabilidades y procedimientos de operación				
12.1.2 Gestión de cambios	¿Existe un procedimiento de control de cambios?	X		90%
12.1.3 Gestión de capacidades	¿El personal es idóneo para el trabajo que se le encomienda?	X		90%
12.1.4 Separación de entornos de desarrollo, prueba y producción	¿Existen los entornos de desarrollo, prueba y producción?	X		90%
12.5 Control del software en explotación				
12.5.1 Instalación del software en sistemas en producción	¿Se tiene documentado el procedimiento de instalación de software en entornos de producción?	X		90%
12.6 Gestión de la vulnerabilidad técnica				
12.6.1 Gestión de las vulnerabilidades técnicas	¿Se tiene establecido un sistema de gestión de vulnerabilidades?	X		70%
12.7 Consideraciones de las auditorías de los sistemas de información				
12.7.1 Controles de auditoría de los sistemas de información	¿Se lleva a cabo la auditoría de los sistemas de información?	X		70%
13.2 Intercambio de información con partes externas				
13.2.1 Políticas y procedimientos de intercambio de información	¿Existen procedimientos para el intercambio de información?	X	70%	70%
13.2.2 Acuerdos de intercambio	¿Existen documentos de acuerdo para el intercambio de información?	X	70%	70%
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN				
14.1 Requisitos de seguridad de los sistemas de información				
14.1.1 Análisis y especificación de los requisitos de seguridad	¿Se han especificado los requisitos de seguridad de los sistemas?	X		90%
14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas	¿Se ha establecido el nivel de seguridad de las redes públicas?	X		90%
14.1.3 Protección de las transacciones por redes telemáticas	¿Se conoce el nivel de seguridad de las redes de datos?	X		90%
14.2 Seguridad en los procesos de desarrollo y soporte				
14.2.1 Política de desarrollo seguro de software	¿Se cuenta con un procedimiento para la solicitud de desarrollo de software?	X		90%

Control	Pregunta existencia control	Si	No	% cumplim.
14.2.2 Procedimientos de control de cambios en los sistemas	¿Existe un procedimiento de control de cambios en los sistemas?	X		70%
14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	¿Se revisa el funcionamiento del aplicativo después de actualizar el sistema operativo?	X		90%
14.2.5 Uso de principios de ingeniería en protección de sistemas	¿La protección de los sistemas está implementada?	X		90%
14.2.7 Externalización del desarrollo de software	¿El software es desarrollado por terceros?	X		90%
14.2.9 Pruebas de aceptación	¿Cuándo se realizan actualizaciones a los desarrollos de aplicaciones, se hacen pruebas de aceptación?	X		90%
15. RELACIONES CON SUMINISTRADORES				
15.1 Seguridad de la información en las relaciones con suministradores				
15.1.1 Política de seguridad de la información para suministradores	¿Existe la política de seguridad para con los proveedores?	X		70%
15.1.2 Tratamiento de riesgo dentro de acuerdos de suministradores	¿Existe el análisis del riesgo para los acuerdos con proveedores?	X		90%
15.1.3 Cadena de suministro en tecnologías de la información y las comunicaciones	¿Existe un proceso que determine la cadena de suministro en las TIC?	X		90%
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN				
16.1 Gestión de incidentes de seguridad de la información y mejoras				
16.1.1 Responsabilidades y procedimientos	¿Existen los responsables y los procedimientos en caso de presentarse un incidente de seguridad informático?	X		50%
16.1.2 Notificación de los eventos de seguridad de la información	¿Se notifican los eventos de seguridad a las personas involucradas?	X		50%
16.1.3 Notificación de puntos débiles de la seguridad	¿Se notifican las vulnerabilidades detectadas en el sistema de seguridad informática?	X		80%
16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones	¿Se hace la oportuna valoración de eventos y se toman decisiones con base en dicha valoración?	X		50%
16.1.5 Respuesta a los incidentes de seguridad	¿Se tiene una adecuada respuesta a los incidentes de seguridad ocurridos?	X		50%
16.1.6 Aprendizaje de los incidentes de seguridad de la información	¿Se tiene una base de datos de conocimientos sobre las incidencias presentadas y las soluciones dadas?	X		10%
16.1.7 Recopilación de evidencias	¿Existe una adecuada recopilación de evidencias de los incidentes?	X		10%
17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO				
17.1 Continuidad de la seguridad de la información				
17.1.1 Planificación de la continuidad de la seguridad de la información	¿Existe el plan de continuidad del negocio?	X		70%
17.1.2 Implantación de la continuidad de la seguridad de la información	¿Se ha implantado algún aspecto incluido en el plan?	X		70%
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	¿Se han hecho pruebas que permitan validar y evaluar el plan de continuidad del negocio?	X		70%

Control	Pregunta existencia control	Si	No	% cumplim.
18.2 Revisiones de la seguridad de la información				
18.2.1 Revisión independiente de la seguridad de la información	¿Se han hecho pruebas al sistema por parte de terceros?		X	10%
18.2.2 Cumplimiento de las políticas y normas de seguridad	¿Se cumplen las políticas de seguridad al interior de la empresa?	X		90%
18.2.3 Comprobación de cumplimiento	¿Se hace verificación periódica del cumplimiento de las políticas?	X		70%

Fuente: Documento MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – MSPI versión 01

Una vez se establezca el periodo de evaluación y actualización de los controles, se **recomienda** tener en cuenta controles preventivos y que sean virtuales, resultado de monitoreos y seguimientos periódicos en los sistemas de información, entre otros:

- Establecimiento y documentación de los roles que debe tener cada usuario en el aplicativo ERP- SAP (Coordinadores, Administradores, Tesoreros, Auxiliares)
- Monitoreos y reportes de uso de usuario y contraseñas en diferentes máquinas
- Monitoreos y reportes de aplicación de la Política de Seguridad.

PLAN DE TRATAMIENTO DE RIESGOS

La entidad cuenta con un plan de tratamiento de riesgos de seguridad y privacidad de la información vigencia 2019, cargado en la herramienta Suite Visión, el cual arroja un resultado de cumplimiento del 100%, sin embargo, al revisar las tareas concertadas, estas no enmarcan actividades con la finalidad de definir la aplicación de los controles de seguridad mencionadas anteriormente. No se evidencia que el plan de tratamiento de riesgos incluya el tratamiento que se dará a los riesgos, qué acciones se implementarán, quienes serán los responsables de esta implementación, plantear cada acción, etapa y procedimientos que se ejecutarán para poder ser monitoreado y lograr el seguimiento a la ejecución del mismo.

EVALUACIÓN OCI PLAN TRATAMIENTO DE RIESGOS

#	PLAN TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2019 SVE (Código: GTI-PL-02)	CUMPLE		OBSERVACIONES OCI
		SI	NO	
1	Plan de capacitación y sensibilización a usuarios sobre temas de seguridad informática y riesgos informáticos.			Plan sin firmas, Plan de sensibilizaciones Código: GTI-PL-03 el mismo de MSPSI Boletines - No evidencia de capacitaciones
2	Adquisición de un WAF (web application firewall) adquirir el dispositivo, el cual protegerá los aplicativos webs de la ALFM	**X**		Acta de recibo a satisfacción no se evidencia publicada Tarea: Puesta en marcha del WAF evidencia: Levantamiento de información configuración WAF

#	PLAN TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2019 SVE (Código: GTI-PL-02)	CUMPLE		OBSERVACIONES OCI
		SI	NO	
3	Migración de IPv4 a IPv6	X		Como finalización del proceso de migración de IPV6 se tiene el acta de entrega y el plan de implementación de IPV6, en cumplimiento al Contrato de consultoría N° 001-092-2019 cuyo objeto es "Servicio Profesional para la Planeación, Desarrollo e Implementación de la transición de IPv4 a IPv6. Su puesta en funcionamiento, operatividad, pruebas y estabilización de los servicios de la Red de Comunicaciones e Infraestructura Tecnológica de la Agencia Logística de las Fuerzas Militares en su Sede Principal y Sedes Regionales".
4	Realización periódica de backups	X		Se ejecuta solo a los sistemas de información ERP, PRODUCTIVO, SOLMAN, DESARROLLO y CALIDAD
5	Mantenimientos preventivos y correctivos	X		

Fuente: Soportes Herramienta Suite Visión Empresarial - Plan Tratamiento De Riesgos 2019

5. Una vez verificado el Plan de Seguridad y Privacidad de la Información 2019, se puede evidenciar que se encuentra administrado en la herramienta Suite Visión con 9 actividades, de las cuales la herramienta indica cumplimiento del 100%, sin embargo; al revisar los soportes cargados se encuentra cumplimiento a 4 actividades.

EVALUACIÓN OCI PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2019

#	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2019 SVE	CUMPLE		OBSERVACIONES
		SI	NO	
1	Ajustar el alcance y límites del MSPI en términos de las características del servicio que presta la Entidad, su estructura interna, su ubicación, sus activos de información, tecnología, e incluir los detalles y justificación de cualquier exclusión del alcance.		X	Documento MSPI, Código: GTI-MO-01 Versión No. 00 fecha 24-04-19 - Documento sin firmas, no se incluye a la Dirección General Las siglas MO no se encuentra enmarcadas dentro de la Guía para la Elaboración de Documentos del Sistema Integrado de Gestión Código GI-GU-03 sub numeral 4.2.2 Tipos de Documentos.
2	Documento con la política general actualizada.	X		Directiva Permanente No. 05 Política general Seguridad de la Información 12 03 19

#	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2019 SVE	CUMPLE		OBSERVACIONES
		SI	NO	
3	Actualizar el inventario de los activos dentro del alcance del MSPI y los propietarios de estos activos de información.	**X**		Versión 01. Fecha: 30-12-2019. En el numeral 3.1 Identificación de los activos tecnológicos, en las secciones correspondientes a Software y Hardware, se adicionó un activo. WAF (Web Application Firewall) - No se incluye el IPV6 - Pendiente análisis de activos de personal
4	Identificar las amenazas a los nuevos activos.		**X**	TICS: *no contienen modificaciones ya que el nuevo activo de información descrito en el numeral 3.1. se encuentra en fase productiva de aprendizaje, por lo que los reportes generados en esta etapa no fueron considerados;*
5	Análisis y evaluación de los riesgos asociados de acuerdo al impacto que pueden generar y a la probabilidad de ocurrencia para los nuevos activos identificados.		**X**	Documento MSPI, Código: GTI-MO-01 Versión No. 00 fecha 24-04-19 - Documento sin firmas, no se incluye a la Dirección General Las siglas MO no se encuentra enmarcadas dentro de la Guía para la Elaboración de Documentos del Sistema Integrado de Gestión Código GI-GU-03 sub numeral 4.2.2 Tipos de Documentos. No se evidencian actualización nuevos activos identificados.
6	Obtener la aprobación de la Dirección sobre los nuevos riesgos residuales determinad		**X**	Actividad cargada con fecha enero 2020, sin firma de la Dirección General No se evidencia en el control de cambios versión 01 aspectos de la actualización del riesgo residual
7	Elaborar la declaración de aplicabilidad (SoA).	**X**		Documento sin firmas, sin formato, Pendiente verificación frente a 3 riesgos en tratamiento SVE
8	Actualizar el Plan de Tratamiento de Riesgos	**X**		Formato sin firma de la Dirección General
9	Plan y ejecución de sensibilización, capacitación y apropiación del MSPI, para toda la entidad.		**X**	TICS: Evidencia: Plan de sensibilizaciones Código: GTI-PL-03 elaborado (primer cuatrimestre) y ejecutado (segundo cuatrimestre). - Cumplido Sensibilización de IPv6 - No se evidencia que se realizaran 8 sensibilizaciones y 3 capacitaciones que estaban programadas

Fuente: Soportes Herramienta Suite Visión Empresarial - Plan Tratamiento De Riesgos 2019

6. **ADOPCIÓN DEL PROTOCOLO IPv6** Se verifica expediente contractual

Proviene del proceso de concurso de méritos No. 002-069-2019
Contrato 001-092-2019 por un valor de $372.000.000
Plazo de ejecución 31-12-2019
Ordenador del Gasto Cr Riveros
Supervisión Cristian Cruz y Daniela Caro Quiroga
Proveedor IPV6 TECHNOLOGY SAS
Objeto: Puesta en funcionamiento, operatividad, pruebas y estabilización de los servicios en la red de comunicaciones e infraestructura.
Forma de Pago:
10% listado de asistencia, cumplimiento cronograma de transferencia de conocimientos
50% ejecución fases de planeación y de implementación
40% ejecución fase de pruebas de funcionalidad
En el anexo No. 2 del contrato se encuentra el inventario de activos de la ALFM por regional y Oficina Principal, la solución de conectividad, aplicaciones y software server físicos y/o virtualizados Vmware Vsphere Enterprise; que migraban a IPv6.

Mediante informe de supervisión No. 9 correspondiente al periodo del 11 al 19 de diciembre los supervisores del contrato reportan*: "Se da por finalizado el proceso de despliegue IPv6 en las sedes regionales. Continuará durante la fase de soporte y garantía (1 año de acuerdo a lo establecido en el contrato) con el proceso de seguimiento y estabilización de los servicios migrados, para ello en pro de garantizar éxito completo en esta fase de soporte y garantía se contará con apoyo de personal en sitio con el ánimo de atender los incidentes que puedan presentarse."*

En el repositorio que se encuentra en los equipos de cómputo de la Oficina TIC's se observa una carpeta compartida donde se encuentran los informes de supervisión, los informes presentados por el contratista y las actas de reunión sostenidas durante la ejecución del contrato.

Propuesta realizada por la Oficina de control

1) Teniendo en cuenta que la implementación del Modelo de Seguridad y Privacidad de la Información establecida por MINTIC es la herramienta idónea para adoptar medidas que permitan evitar situaciones delictivas.

   - ✓ Los Riesgos relacionados y clasificados en un orden de prioridad alto deben estar integrados en la política de administración del riesgo de la entidad y monitoreados en la SVE.
   - ✓ Aplicar las Guías No. 7 y 8 emitidas por el Ministerio TIC en cuanto los temas abordados de Riesgos y Controles.
   - ✓ Documentar y complementar la fase de implementación del MSPI establecido por MINTIC.
   - ✓ Desarrollar actividades correspondientes a la evaluación del desempeño del MSPI para la presente vigencia.

- ✓ Implementar en la entidad la Auditoria para la evaluación del MSPI y la implementación del Manual de Gobierno Digital. Las auditorias se deben realizar al menos con una vez en el año, aunque esta periodicidad depende de las necesidades de la ALFM.
- ✓ Documento de inventario final de la infraestructura de TI sobre el nuevo protocolo IPv6.

Una vez documentado y alineado el MSPI establecido por MINTIC con los elementos del modelo con que cuenta la entidad en las fases de Diagnostico, planeación e implementación, se deben implementar la Fase de Evaluación del desempeño y Mejora continua, de las que no se evidencia avance, así:

2) **Fase de Evaluación del Desempeño**

Una vez obtenidos los resultados anteriormente mencionados, es procedente evaluar y/o medir la efectividad de las acciones adelantadas por la entidad en cuanto la Seguridad de la información.

Que de acuerdo a lo establecido en el MSPI establecido por MINTIC Guía No.16, la entidad debe documentar los siguientes ítems:

- ✓ Documento con los resultados del Plan de seguimiento
- ✓ Documento con el Plan de auditoría interna y resultados revisado y aprobado por el Comité de Gestión Institucional o el que haga sus veces
- ✓ Comunicación de los indicadores al público a través de la rendición de cuentas, informe a la PGN y al Congreso de la República.

En cuanto al ejercicio de auditoria que tiene como finalidad verificar el estado de la implementación del Modelo de Seguridad y Privacidad de la Información a continuación se detalla lo correspondiente al desarrollo de dicha actividad:

- ➢ **La auditoría Informática** encaminada a recolectar, consolidar y evaluar evidencia para comprobar si la entidad ha avanzado en la implementación de controles, protección de los activos, mantenimiento de la integridad de los datos, si tiene claro los objetivos de seguridad de la entidad y si utiliza bien los recursos. De este modo la auditoría informática mantiene y confirma la consecución de los objetivos tradicionales de la auditoría, que son:

  - ✓ Protección de activos e integridad de datos.
  - ✓ Gestión de protección de activos, de manera eficaz y eficiente.

Esta puede ser externa como interna y debe ser una actividad ajena a influencias propias de la entidad. La función auditora puede actuar de oficio, por iniciativa o por solicitud de la dirección de la entidad.

- ➢ **La Auditoria de Sistemas** es aquella actividad donde se evalúa el manejo y la protección de la información residente en los sistemas de información, también califica la aptitud del recurso humano que gestiona estas plataformas y la eficiencia del recurso informático.

La función de la auditoria es preventiva, realiza revisiones utilizando recursos de hardware y software desarrollando procedimientos similares a los que emplea la entidad, con el fin de mejorar los procesos de la entidad.

El objetivo principal es la verificación del sistema de información, su confiabilidad y el uso del mismo por parte de la entidad.

Durante la planeación se lleva a cabo el ciclo (planear) determinando los recursos, los procesos y el tiempo para llevar a cabo las auditorias, teniendo en cuenta ***como insumos las revisiones o seguimientos a la implementación del modelo de seguridad y privacidad de la información, observaciones por parte de la alta dirección, el desempeño de los procesos, los cambios en el entorno, controles internos, estrategias, entre otros.***

Es importante que las auditorias se realicen con anterioridad a las auditorias de organismos de certificación y de control, con el fin de mejorar las deficiencias que pueda llegar a tener la implementación del modelo. También es necesario que los líderes de los procesos trabajen de forma alineada con el equipo de seguridad o la Oficina de Control Interno o la dependencia que haga sus veces, para determinar mesas de trabajo orientadas a revisar su proceso de manera que el trabajo se realice proactivamente y no reactivamente.

- Otra de las recomendaciones establecidas por MINTIC Guía No.15 se encuentra el uso de las **métricas**, estas permiten entender un proceso técnico que se está aplicando en la entidad, a través de ellas podemos medir dicho proceso y su producto para saber cómo mejorar su calidad.

  El utilizar métricas de seguridad en el Sistema de Gestión de Seguridad de la Información puede provocar que la norma 27001 perdure en el tiempo como un estándar potente y eficaz para gestionar las seguridad de la información de una forma óptima, debido a que las métricas de seguridad no están contempladas como un accesorio más a añadir al Sistema de Gestión de Seguridad de la Información según le interese a la entidad sino que lo absorbe y termina formando parte de él a lo largo de su ciclo de vida. Todo esto provoca que el sistema de medición junto a su Sistema de Gestión de Seguridad de la Información sea revisado y mejorado de una forma continua.

3) Fase de Mejora Continua

Una vez se tengan los resultados del componente de evaluación del desempeño se toman los resultados obtenidos y se preparan los correctivos necesarios que permitan a la misma crecer en el nivel de responsabilidad demostrada.

- ✓ Documento con los resultados del plan de seguimiento
- ✓ Documento con los resultados del plan de mejoramiento revisado y aprobado por el Comité de Gestión Institucional o el que haga sus veces.
- ✓ Documento con el consolidado de las auditorias.

4) Además de las recomendaciones plasmadas en el desarrollo de la actividad de Auditoria se sugiere tener en cuenta los resultados emitidos en informes de auditorías e informes de Ley emitidos por la Oficina de Control Interno.

INFORMES DE LEY EMITIDOS POR OCI				
No. documento	**Informe**	**Vigencia**	**Proceso y/o Dependencia**	**Observación**
No.20191200000383 ALOCI	Ley de transparencia	2018	Oficina principal	La web master debe verificar la migración de la información de manera total y de acuerdo con el contrato No. 001-037/2018 y la matriz de cumplimiento a la ley de transparencia. Actualizar la Directiva permanente No.05-ALDG-ALOP-140 política Editorial WEB.
No. 20181200007083-ALOCI-GSE	Ley de transparencia	2018	Oficina principal	El criterio de la ley 1712 "accesibilidad" no se evidenció en la página web el acceso a los medios de comunicación a personal con discapacidad, factor que se reportó en la vigencia 2016 como cumplido
20191200163163-ALOCI-GSE-120 de fecha 19-03-2019	Informe Avance licenciamiento software	2019	TIC	Observación: En las pruebas de recorrido realizadas, se evidencio Software no licenciado así: WinRar en 15 máquinas, Winzip en 2 máquinas; en cuanto al software Revit se desístala en una máquina, debido a que solo se cuenta con dos licencias autorizadas.
				sugerencias: Ejercer por parte de la Oficina TIC, control en la instalación del software por parte de los agentes de soporte en la Oficina Principal
No. 20201200145893 ALOCI –GSE-120	Informe Avance licenciamiento software	2020	TIC	De 329 equipos de la Oficina Principal se tomó como muestra 143 máquinas, que representa el 43% de las cuales 14 equipos de cómputo (9.79%), presentaron novedades en la versión de la ofimática instalada.
				De acuerdo a las novedades presentadas la Oficina de TIC's y Agentes de soporte, deben verificar el 100% de los equipos de la ALFM el sistema operativo v/s la ofimática y los contratos de adquisición. Implementar herramienta tecnológica que permita verificar en tiempo real el software debidamente licenciado en los equipos de la entidad a nivel nacional.
No. 20201200141283 ALOCI –GSE-120	licenciamiento software	2020	Regional Amazonía	Observación: en la Regional Amazonía se observó que el usuario Ydorado, está conectado en cinco (5) máquinas diferentes.

Fuente: Archivo de Gestión y Central OCI

REVISION AUDITORIAS VIGENCIA 2020					
No. Auditoria	**Donde se efectuó la auditoria**	**Proceso y/o Dependencia**	**Tipo**	**Descripción**	**Herramienta tecnológica**
1	Oficina Principal	Direccionamiento Estratégico	Observación	No se evidencia dentro de las actas Administrativas el seguimiento por cada Coordinación de la Oficina TIC´S (Coordinación Informática y Coordinación Informática Redes e Infraestructura Tecnológica) de acuerdo a la información presentada por el Proceso. Se identificaron instrucciones emitidas por la Dirección General para cumplimiento de la Oficina TICS de lo cual emitió respuesta sin diligenciar los campos de SI / NO, en el análisis de los soportes se establece que se da cumplimiento 7 de 9 tareas; las instrucciones que no se cumplieron son: Ø No se allegó el Plan anual de Capacitación en SAP para la vigencia 2019, para todas las dependencias de la Entidad; se adjuntó evidencia de capacitación de las Regionales Norte, Amazonia, y dependencias Almacenes y Créditos Ø La revisión de las licencias de SAP, se soportó con fecha 20-01-2020 (400 licencias: asignadas 383 y disponibles 17)	SECOP II SIIF Nación SVE
4	Oficina Principal Gestión de TICs	Gestión TICs – Controles y Riesgos Vigencia 2019	Recomendación	1. Implementar lo establecido en la Guía para la administración del riesgo y el diseño de controles en entidades públicas versión No 4 del Departamento Administrativo de la Función pública – riesgo de gestión, corrupción y seguridad Anexo No. 4 lineamientos para la gestión de riesgos de seguridad digital en entidades públicas. 2. Establecer de manera puntual las causas de los riesgos de corrupción y de los de gestión de acuerdo a las políticas y lineamientos de la Entidad. 3. Para el riesgo “Pérdida, daño, manipulación o sustracción de información o de equipos tecnológicos”, se recomienda establecer actividades de control en referencia a los equipos tecnológicos, ya que este concepto es genérico o delimitar	SVE

REVISION AUDITORIAS VIGENCIA 2020					
No. Auditoria	**Donde se efectuó la auditoria**	**Proceso y/o Dependencia**	**Tipo**	**Descripción**	**Herramienta tecnológica**
				su alcance conforme a la redacción del Riesgo. 4. Alinear la política de gestión de riesgo, donde se incluya el compromiso en la gestión de los riesgos de seguridad digital en todos los niveles de la entidad (Desarrollo organizacional y Gestión Integral).	
6	Regional Amazonia	Direccionamiento Estratégico Gestión Administrativa y del Talento Humano Gestión Financiera Operaciones Logísticas (Catering – CADS)	Hallazgo	Las unidades de negocio BASPC 12, BIMEJ, BITER 12 y BALOC 27 no diligencian los campos de texto de cabecera en las migos de entradas y salidas de mercancía	SVE SIIF Nación ERP SAP

Fuente: Archivo de Gestión y Central OCI

Se deja como anexo las recomendaciones y/o sugerencias realizadas por la Oficina de Control Interno durante las vigencias 2018 y 2019

5) Por último, es importante resaltar que de acuerdo al MSPI establecido por MINTIC. *Los plazos para la implementación de las actividades se establecieron para el Manual de Gobierno en Línea, y a través del Decreto 1078 de 2015, en el Artículo 10. "Plazos. Los sujetos obligados deberán implementar las actividades establecidas en el Manual de Gobierno en Línea dentro de los siguientes plazos:*

Sujetos Obligados del Orden Nacional

Componente/Año	2015	2016	2017	2018	2019	2020
TIC para ser servicios	90%	100%	Mantener 100%	Mantener 100%	Mantener 100%	Mantener 100%
TIC para Gobierno abierto	90%	100%	Mantener 100%	Mantener 100%	Mantener 100%	Mantener 100%
TIC para la Gestión	25%	50%	80%	100%	Mantener 100%	Mantener 100%
Seguridad y Privacidad de la Información	40%	60%	80%	100%	Mantener 100%	Mantener 100%

HALLAZGO:

Omitido

SOPORTES DE LA REVISIÓN:

1 CD

Elaboró:

NOMBRE	CARGO	FIRMA
Sandra Nerithza Cano Perez	Jefe Oficina de Control Interno	SANDRA NERITHZA CANO PEREZ — Firmado digitalmente por SANDRA NERITHZA CANO PEREZ Fecha: 2020.05.07 14:34:46 -05'00'
Yamile Andrea Munar Bautista	PD Control Interno	Yamile Andrea Munar Bautista — Firmado digitalmente por Yamile Andrea Munar Bautista Fecha: 2020.05.07 14:29:29 -05'00'
Leidy Andrea Aparicio	PD Control Interno	Leidy Andrea Aparicio Caicedo — Firmado digitalmente por Leidy Andrea Aparicio Caicedo Fecha: 2020.05.07 16:08:17 -05'00'
Johana González	PD Control Interno	Johana Patricia Gonzalez Molano — Firmado digitalmente por Johana Patricia Gonzalez Molano Fecha: 2020.05.07 15:41:42 -05'00'
Luisa Fernanda Vargas	PD Control Interno	Luisa Fernanda Vargas Figueredo — Firmado digitalmente por Luisa Fernanda Vargas Figueredo Fecha: 2020.05.07 16:16:46 -05'00'
Carmen Aurora Pulido	ASD Control Interno	Carmen Aurora Pulido Méndez — Firmado digitalmente por Carmen Aurora Pulido Méndez Fecha: 2020.05.07 14:50:27 -05'00'
Rosa García Chaux	PD Control Interno	ROSA GARCIA CHAUX — Firmado digitalmente por ROSA GARCIA CHAUX Fecha: 2020.05.07 14:44:05 -05'00'
Bryan Mosquera	PD Control Interno	Bryan Mosquera Sánchez — Firmado digitalmente por Bryan Mosquera Sánchez Fecha: 2020.05.07 16:04:29 -05'00'

Revisó:

NOMBRE	CARGO	FIRMA
Sandra Nerithza Cano Perez	Jefe Oficina de Control Interno	SANDRA NERITHZA CANO PEREZ — Firmado digitalmente por SANDRA NERITHZA CANO PEREZ Fecha: 2020.05.07 14:33:37 -05'00'