Al contestar por favor cite estos datos:
Radicado No.: 20171200222413

Pública [x] Privada [ ] Confidencial [ ]

Bogotá D.C, 02-11-2017

MEMORANDO

PARA: **MARIA JOHANA BELLAIZAN CASTILLO**
Profesional Junior área de Planeación y Gestión de Riesgos

ANGEL REINALDO NUNCIRA
Gerente Área de Tecnología de la Información

CON COPIA: **ALEJANDRA CORCHUELO MARMOLEJO**
Gerente General (E)

DE: **LUIS E. HERNANDEZ LEON**
Asesor de Control Interno

ASUNTO: Notificación informe final auditoria Gobierno en Línea- GEL Seguridad y Privacidad de la Información.

Respetados Doctores,

Adjunto para su conocimiento el informe final de la auditoria del asunto, realizada a las áreas de Planeación y Gestión de Riesgos y tecnología de la información.

De conformidad con lo establecido en el Procedimiento de Auditorías Internas de control Interno, se solicita:

- Proceder con la formulación de las acciones correctivas y preventivas que de acuerdo con su criterio sean necesarias para subsanar las debilidades descritas en las No conformidades y recomendaciones expuestas en el informe.

- Remitir dentro de los cinco (5) días hábiles siguientes a la fecha de la presente comunicación el respectivo plan de acción, el cual deberá indicar: descripción, actividades, causa raíz identificada, responsables, plazos y entregable/fuente de verificación, según cuadro anexo.

Cordialmente,

LUIS E. HERNANDEZ
Asesor de Control Interno

Elaboró: Celeny Gonzalez Parra (Auditora)

Revisó: Adriana Maria Ocampo Loaiza (Líder de Auditorias SGC – SCI)

INFORME FINAL

SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

1. OBJETIVO GENERAL

Evaluar el nivel de implementación de la estrategia de Gobierno en Línea, para el componente Seguridad y Privacidad de la Información, en concordancia con lo descrito en el decreto 1078 de 2015 y demás normatividad aplicable.

2. OBJETIVOS ESPECIFICOS

1. Verificar el grado de implementación del logro: Definición del marco de seguridad y privacidad de la información y de los sistemas de información.
2. Verificar el grado de ejecución del logro: Implementación del plan de seguridad y privacidad de la información y de los sistemas de información.
3. Verificar el grado de implementación del logro: Monitoreo y mejoramiento continuo.
4. Evaluar los riesgos, eventos y eficacia de los controles asociados.
5. Realizar seguimiento al avance y/o cumplimiento de las acciones formuladas frente a los resultados de las auditorías anteriores y planes de mejoramiento de la Contraloría General de la Republica y Revisoría fiscal, si aplica.
6. Emitir conclusiones, especificando las No conformidades, observaciones y/o recomendaciones que según el análisis realizado sean procedentes

3. ALCANCE

Agosto 2016 a agosto de 2017.

4. CRITERIOS

- Decreto único reglamentario del Sector de Tecnologías de la Información y las Comunicaciones- 1078 de 2015.
- Decreto 2573 de 2014.
- Modelo de Seguridad y Privacidad de la Información- MINTIC.
- Manual Estrategia de Gobierno en Línea- GEL.
- ISO/IEC 27001- 27002
- Otra normativa del orden nacional aplicable a la Entidad.

- Plan Institucional de Desarrollo Administrativo 2016- 2017.

- Disposiciones internas vigentes (Manuales, procedimientos, instructivos, guías, circulares)
  MAP804 Manual de Gestión de seguridad de la información v.5B
  PDI453 Gestión de registros de eventos para la plataforma tecnológica v.01
  MDI452 de Gestión de la Tecnología de la Información y las Comunicaciones v.4A

5. METODOLOGIA

La obtención y verificación de la información, se realizó mediante:

Entrevistas

Septiembre 08/2017

Dra. Mary Yazmin Vergel	Gerente área Planeación y Gestión de Riesgos
Ingeniera Diana Jaidy Piñeros	Líder GEL
Ingeniero Denis Fernando Montealegre	Oficial de Seguridad de la Información.
Dra. Sara Jennifer Salazar	Gerente área Desarrollo Administrativo

Sesiones de trabajo

Septiembre 01/2017 y septiembre 14/2017

Ingeniero Denis Fernando Montealegre Beltran	Oficial de Seguridad de la Información.

Revisión documental

Instrumento de evaluación MSPI 2016_feb17_ajustadomar17.xlsx
Actas de Comité de Desarrollo Administrativo.
Seg31Julio17_Cronograma de Trabajo_MSPI_2017_2018.xlsx
Perfil_SI_2016.pdf
MAP804 Manual de Gestión de Seguridad de la Información V05B_OYM_08082017.docx

Pruebas de funcionalidad

Claves de usuario-inicio de sesión

6. DESARROLLO

Introducción

En el año 2015, se expidió el Decreto No 1078 - Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, el cual compila la normatividad vigente relacionada con el sector de la Tecnologías de la Información y Comunicaciones. En la sección 2, presenta los componentes que facilitaran a las Entidades la implementación y mantenimiento de la estrategia Gobierno en Línea; los cuales se identifican como TIC para Servicios, TIC para el Gobierno Abierto, TIC para la Gestión, y Seguridad y Privacidad de la Información.

El componente TIC para servicios está orientado al uso de los medios electrónicos para facilitar los trámites y servicios requeridos por los grupos de interés; TIC para el Gobierno Abierto permitirá fortalecer el acercamiento de la ciudadanía al Estado, haciéndolo más transparente, participativo y colaborativo; TIC para la Gestión establece los lineamientos de una efectiva planeación y gestión de las tecnologías, y fortalecer la toma de decisiones y la administración de las entidades. El último componente de esta estrategia es Seguridad y Privacidad de la Información, mediante el cual se propende la protección de la información y los sistemas de información de la Entidad.

El Decreto No 1078 de 2015, en su Artículo 2.2.9.1.3.2., establece los siguientes plazos para que las Entidades del orden Nacional y Territorial implementen la estrategia de Gobierno en Línea:

Imagen No.1: Plazos implementación G.E.L

COMPONENTE / AÑO	2015	2016	2017	2018	2019	2020
TIC para Servicios	90%	100%	Mantener 100%	Mantener 100%	Mantener 100%	Mantener 100%
TIC para el 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%

Por lo anterior, en cumplimiento al Plan Anual de Auditoria 2017 de la Asesoría de Control Interno de FONADE, se realiza la presente auditoria al componente *Seguridad y privacidad*

de la información; tomando como referencias principales: Manual de Gobierno en Línea y el Modelo de Seguridad y Privacidad de la Información y sus anexos.

6.1 Verificar el grado de implementación del logro: Definición del marco de seguridad y privacidad de la información y de los sistemas de información.

Este logro busca definir el estado actual del nivel de seguridad y privacidad y define las acciones a implementar[1], a través de los siguientes criterios:

6.1.1 Diagnóstico de Seguridad y Privacidad

Se observa el archivo *Instrumento de evaluación MSPI 2016_feb17_ajustadomar17.xlsx*, cuyos resultados fueron presentados en Comité Institucional de Desarrollo Administrativo del 27/03/2017, en el punto *"6: Resultados del autodiagnóstico del modelo de Seguridad y Privacidad…"* que en resumen indica que FONADE tiene un avance del 68,4% en el ciclo PHVA y un cumplimiento del 48,3% en los dominios del Anexo A de la ISO 27001.
Es de anotar, que posterior al diligenciamiento de esta herramienta, el MINTIC, emitió el "*Instructivo para el diligenciamiento de la herramienta de diagnóstico de Seguridad y privacidad de la Información- v. 1.0 del 9/06/2017 Versión inicial del documento"*, por consiguiente, es necesario tomarlo como referencia, para la revisión y/o ajustes pertinentes, en aspectos como:

- ✓ Hojas levantamiento de información y áreas involucradas: completar información pendiente, como: análisis del contexto (documento que hace referencia a determinar los aspectos externos e internos que son necesarios para cumplir los resultados previstos), documento con el resultado de la estratificación de la entidad, metodología de gestión de proyectos, entre otros ítems de estas secciones.
- ✓ Hojas Administrativas, Técnicas y PHVA: complementar la evidencia de las verificaciones realizadas, indicando datos como: fechas del trabajo con las áreas, actividad realizada, anexos, versión del documento (manuales, procedimientos), numeral revisado, cuando aplique. Así mismo, describir la brecha identificada y recomendaciones según el caso. Se muestra un ejemplo a continuación:

Imagen No.2: ítem de autodiagnóstico.

ID	CARGO	ITEM	DESCRIPCIÓN	MSPI	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO PHVA
P.6	Responsable SI	Identificación y valoración de riesgos	Metodología de análisis y valoración de riesgos e informe de análisis de riesgos	componente planificación	MAP805,MAP804		60

- ✓ Llama la atención, que en la hoja PHVA, en el componente evaluación de desempeño, ítem E.2, describe:" No *se evidencia auditoria enfocada a seguridad de la información"*

[1] Manual Gobierno en Línea

Imagen No.2: ítem autoría Interna

ID	CARGO	ITEM	DESCRIPCIÓN	MSPI	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO PHVA
E.2	Control Interno	Auditoría Interna	Plan de auditoría interna	componente evaluación del desempeño	MAP804	No se evidencia Auditoria enfocadas a Seguridad de la Información.	20

Lo que indicaría que algunos temas no se trataron con los responsables del proceso, ya que, para este caso puntual, en el plan anual de auditorías, se incluye este componente y se conservan los soportes.

Lo anterior, con el fin de contar con el instrumento de evaluación acorde con los lineamientos establecidos e identificar oportunidades de mejora en el plan del Modelo de Seguridad y Privacidad de la Información, que está en curso.

6.1.2 Plan de Seguridad y privacidad de la información

Una vez realizado el diagnóstico descrito anteriormente, se formuló el plan de acción y este fue presentado en el Comité Institucional de Desarrollo Administrativo del 27/03/2017, en el punto 6 del orden del día: *"Plan para la implementación del MSPI 2017-2018"*. En esta versión inicial, se plantearon 87 actividades así:

Cuadro No.1 consolidado actividades

Vigencia	Actividades
2017	57
2018	14
2017 y 2018	16
total	87

La primera modificación fue presentada en Comité Institucional de Desarrollo Administrativo del 30/06/2017, punto "*4. Solicitud de modificación del plan MSPI…*" del orden del día. En esta instancia se propone y aprueban cambios en fecha de ejecución de 14 actividades, según justificaciones expuestas.
La segunda modificación fue presentada en Comité Institucional de Desarrollo Administrativo del 30/08/2017, punto "1. *Solicitud de Modificación del Plan del Modelo de Seguridad y Privacidad MSPI 2017-2018",* cuya acta se encuentra en elaboración a la fecha de revisión de este ítem (14/09/2017); en esta ocasión, se solicita modificación en el plazo de ejecución de:

- 16 actividades relacionadas con la actualización del MAP804 manual de Gestión de Seguridad de la Información.
- 24 actividades relacionadas con ingeniería social, migración protocolo IPV4 a IPV6, sincronización de relojes, transferencia de información, entre otros.

En este orden de ideas, el plan de actividades a corte agosto 2017, corresponde a la versión 3, en el cual, de las 87 actividades propuestas, 30 son para cumplimiento en el periodo enero a agosto 2017 y el resultado se presenta en el numeral 6.2.1 del presente informe.

En relación con el plan actual (v.3), se generan las siguientes anotaciones:

Cuadro No.2: actividades

id Act	***Actividad***	***fecha***	***Comentario***
28	Revisar y ajustar política sobre el uso de controles criptográficos y gestión de llaves	30-nov-17	Pre requisito para la actividad 29. Tener en cuenta lo descrito en el numeral 10.1 controles criptográficos- ISO 27002: "Se *debería buscar asesoría especializada para seleccionar controles criptográficos apropiados que cumplan los objetivos de la política de seguridad de la información*"
29	Diseñar procedimiento para la Gestión de llaves asociado a la Política de Criptografía	23-ago-17	Sería posterior al cumplimiento de la actividad 28 de plan MSPI. Revisar.
32	Revisar y ajustar o definir políticas sobre registro de eventos	30-nov-17	En el alcance, tener presente lo descrito en el numeral 12.4.1 *registro y gestión de eventos de actividad-ISO 27002.*
33	Definir procedimiento de Registro de Eventos, incluyendo fortalecimiento de controles.	30-jul-17	Aunque esta actividad ya está cumplida, es necesario que una vez se defina la política (actividad 32), se actualice el procedimiento PDI453 *gestión de registros de eventos para la plataforma tecnológica v.1*, ampliando su alcance. Definir nueva actividad.
34	Proponer modelo de acuerdo de confidencialidad.	31-ago-17	No se presenta una actividad posterior de retroalimentación y/o adopción del mismo.
41	Solicitar modificación del Formato FAP803 - Inventario y Clasificación de Activos incluyendo campos (Dec 103 / 2015)	28-feb-17	FAP803 V.5, tiene los campos: formato, tipo de formato y soporte de información. Se recomienda revisar la descripción (comentario) de estos y dejarlos como lo indican los literales *(d) Medio de conservación y/o soporte y (e) Formato* del dec 103/2015. Para mayor claridad en su diligenciamiento.
52	Elaborar Informes de incidentes identificados en el semestre (si aplica)	25-ago-2017	Actualizar la matriz, en la modificación presentada en Comité Institucional de Desarrollo Administrativo del 30/08/2017, esta actividad registra fecha 30/09/2017.
67	Calcular indicadores del modelo de medición	20-oct-17	Se recomienda incluir una actividad, orientada a la revisión y/o ajustes de la definición de los indicadores actuales, que tenga en cuenta: la periodicidad de medición, fuente de información, responsable, entre otros. Como también revisar la correlación entre la formula y las variables, y la retroalimentación frente a los resultados obtenidos.

79	Verificar la Sincronización de relojes, verificar única fuente referencia (Verificación controles 27002)	31-mar-18	Se considera un plazo muy extenso, dado su impacto en relación con lo mencionado en el numeral 12.4.4 ISO 27002: "*El ajuste correcto de los relojes de computador es importante para asegurar la exactitud de los registros de auditoría (Audit Logs), que pueden ser necesarios para investigaciones o como evidencia legal en casos legales o casos disciplinarios",* como también en atención al control: CTRGTIN44-Sincronización de Relojes de elementos de la infraestructura tecnológica. Por lo tanto, evaluar la pertinencia de cambio de fecha.
82	Seguimiento al avance de planes de tratamiento vulnerabilidades identificadas 2016-2017	24-mar-17	Si bien la Asesoría de Control interno, realiza seguimientos periódicos a los planes de tratamiento, sería importante que el área de PYGR, proponga una actividad de retroalimentación con los procesos.

No se identifica una actividad referente a la medición de los 114 controles de ISO/IEC 27002, el último seguimiento fue a corte diciembre 2016, siendo un insumo para la formulación del plan. Recomendación general, conservar la trazabilidad de los cambios al plan, preferiblemente identificado por versiones, para facilitar su seguimiento.

Como resumen del logro *definición del marco de seguridad y privacidad de la información y de los sistemas de información* se determina:

Cuadro No.3: resumen cumplimento logro1

Criterio	Subcriterio	Cumplimiento	Comentario
Diagnóstico de Seguridad y Privacidad	La entidad cuenta con un diagnóstico de seguridad y privacidad e identifica y analiza los riesgos existentes.	SI	La Entidad cuenta con el instrumento de evaluación MSPI, de acuerdo con los lineamientos del MINTIC. Es necesario complementarlo de acuerdo con el instructivo expedido por el MINTIC.
Plan de Seguridad y Privacidad de la Información	La entidad define las acciones a implementar a nivel de seguridad y privacidad, así como acciones de mitigación del riesgo.	SI	La Entidad tiene definido el plan de actividades para las vigencias 2017-2018. Evaluar ajustes y/o nuevas actividades según lo descrito en el cuadro No. 2

6.2 Verificar el grado de ejecución del logro: Implementación del plan de seguridad y privacidad de la información y de los sistemas de información.

Este logro busca desarrollar las acciones definidas en el plan de seguridad y privacidad[2], a través del siguiente sub criterio:

[2] Manual Gobierno en Línea

6.2.1 La entidad implementa el plan de seguridad y privacidad de la información, clasifica y gestiona controles.

En relación con la última versión del plan de seguridad y privacidad de la información, según modificaciones presentadas en Comité Institucional de Desarrollo Administrativo del 30/08/2017 (acta en elaboración):

- De las 87 actividades que lo componen, 30 registran fecha propuesta de cumplimiento **de enero a agosto 2017 (**ver detalle **Anexo No.1),** siendo el resultado:

Cuadro No.4-cumplimiento actividades

Estado	Actividades
Ejecutada	29
No ejecutada	1

El porcentaje de cumplimiento corresponde a un 96,67% para las actividades propuestas para el periodo enero-agosto 2017.
Las 29 actividades ya ejecutadas, corresponden al 33,33% del plan propuesto para las vigencias 2017 y 2018.
La actividad no cumplida es "Diseñar procedimiento para la Gestión de llaves asociado a la Política de Criptografía", sin embargo, como se menciona en el cuadro No.2, esta sería posterior a la definición de la política, con fecha propuesta 30/11/2017.

- Distribución propuesta para la vigencia 2017:

Cuadro No.5- distribución actividades

Total actividades plan 2017-2018	87	%
Propuestas para la vigencia 2017	65	74,71%
Propuestas enero a agosto 2017	30	34,48%
Propuestas septiembre a diciembre 2017	35	40,22%

Como se observa:

- ✓ Para el periodo septiembre a diciembre 2017 (4 meses), se tienen formuladas 35 actividades, cantidad superior a las actividades para el periodo enero a agosto 2017 (8 meses), por lo tanto, lograr su cumplimiento, exige mayores esfuerzos por parte de los responsables.
- ✓ Las actividades propuestas para la vigencia 2017, corresponden al 74,71% del plan, que una vez ejecutada, se presentaría una desviación del 5% frente a la meta propuesta del

80% al cierre del 2017, de acuerdo con los plazos mostrados en la imagen No.1 del presente informe.

- ✓ El cumplimiento del plan a corte agosto 2017 es del 33,33%.

Como resumen del logro *implementación del plan de seguridad y privacidad de la información y de los sistemas de información* se determina:

Cuadro No.6-Resumen logro2

criterio	subcriterio	Cumplimiento	comentarios
IMPLEMENTACIÓN DEL PLAN DE SEGURIDAD Y PRIVACIDAD	La entidad implementa el plan de seguridad y privacidad de la información, clasifica y gestiona controles.	SI	A corte 31/08/2017 presenta un cumplimiento del 33,33%. Con la ejecución de las actividades propuestas a corte 31/12/2017, se cumpliría un 74,71% del plan propuesto 2017-2018

6.3 Verificar el grado de implementación del logro: Monitoreo y mejoramiento continuo.

Este logro busca desarrollar actividades para la evaluación y mejora de los niveles de seguridad y privacidad de la información y los sistemas de información[3] .

Con referencia al *plan de Actividades 2017-2018 para la implementación del MSPI*, de las 30 actividades propuestas para ejecución en el periodo enero a agosto 2017, 11 guardan relación con el monitoreo y medición a la seguridad de la información, las cuales se encuentran ejecutadas y se identifican en el anexo No.1 con el icono ☑, en la columna monitoreo.

Al respecto se derivan las siguientes anotaciones:

- Se destacan las gestiones adelantadas para las consultorías, como apoyo al desempeño de la seguridad de la información de la entidad.

Cuadro No.7-Consultorias de apoyo a la gestión

Tema	*Comentario*
Analisis de vulnerabilidades	Ejecutado y presentados los resultados (Contrato 20161731)
Pruebas de seguridad física e ingenieria social	Contrato 20171008 , por iniciar la ejecución
Proteccion de datos personales - Ley 1581 / 2012	Contrato No.20171068, por iniciar la ejecución
Transicion protocolo IPV4 a IPV6	Solicitud de estudios previos: 20174100180133

[3] Manual gobierno en Línea

- Perfil de riesgo 2016: el perfil de riesgo residual registra los siguientes 4 riesgos, en nivel de riesgo importante, frente a los cuales a la fecha de la auditoria (14/09/2017), no se han formulado los planes de tratamiento.

Cuadro No.8-Riesgos en nivel importante

CÓDIGO	IMPACTO	NIVEL DE RIESGO
RGPRO32	Mayor	Importante
RGADM20	Mayor	Importante
RGADM57	Mayor	Importante
RGPRO50	Moderado	Importante

Llama la atención que los 2 riesgos señalados con color verde, no se encuentran en la matriz de riesgos del Sistema Administración de Riesgo Operativo-SARO, por lo tanto, no se identifican sus controles- tema objeto de revisión por parte del proceso.

- Calcular indicadores del modelo de medición: como se menciona en el cuadro No.2-Id 67, es necesario revisar y/o ajustar la definición de los indicadores; como también realizar los análisis de los resultados y generar las acciones frente a las desviaciones identificadas, conservando la trazabilidad de las mismas.
  En el archivo indicadores.xlsx, se observan por ejemplo los siguientes registros (señalados en recuadro verde), donde el valor, no guarda relación con las variables 1 y variable2.

Imagen No.3: indicadores

	Indicador	Nombre	Responsable	VARIABLE 1	VARIABLE 2	VALOR	RANGO
GOBIERNO	GO001	Cumplimiento de SGSI 27001	PYGR	25%	69%	2	Aceptable
	GO002	Manual de estrategia de GEL	PYGR-GTI	64%	5%	34%	Crítico
	GO003	PAT (Programa Anual de Trabajo) de Seguridad de la Información	PYGR	02/03/2015	80%	80%	Aceptable
	GO004	Requisitos Legales y de Continuidad	PYGR-GTI-CI	9	70%	70%	Aceptable
	GO005	Nivel de Riesgos en Seguridad de la Información	PYGR	1	75	Crítico	Crítico

Lo anterior indicaría inconsistencias en la medición.

- Informe de monitoreo a la gestión de seguridad de la información: presentado en la sesión No.45 del Comité Institucional de Desarrollo Administrativo (27/03/2017), muestra los resultados a diciembre 2016, de acuerdo con la periodicidad definida (semestral), está pendiente por emitir el informe correspondiente al primer semestre del 2017, por lo tanto, es relevante su pronta gestión, con el fin de tener mayor oportunidad en la formulación de acciones frente a los resultados.

Por otra parte, en cumplimiento al plan anual de auditorías y al procedimiento PAU001 *"Auditorías internas de control interno"*, la Asesoría de Control Interno realiza:

- Auditoria a la seguridad de la información:
-

Cuadro No.9- informes de auditoría

Vigencia	*Informe final*
2015	Radicado: 20151200320413
2016	Radicado: 20161200288023

- Seguimiento periódico a los planes de acción derivados de las auditorias (ver detalle en el punto 6.5 del presente informe).
- Seguimiento periódico a los planes de tratamiento de riesgos: resultados expuestos en comité de riesgos.

Se concluye, que si bien, se han ejecutado acciones y otras están propuestas, es necesario gestionar ante la alta dirección la asignación de los recursos requeridos que garanticen la implementación del modelo de seguridad y privacidad de la información, dentro de los tiempos establecidos.

En relación con lo anterior, en el informe preliminar se registró la observación No.3, con respuesta del área de Planeación y Gestión de Riesgos mediante memorando No.20171300211013 del 18 de octubre de 2017, donde se describe que por medio del memorando No. 20171300193723 del 19 de septiembre 2017, se formuló la solicitud de recursos en materia de Seguridad y Privacidad de la información, para la vigencia 2018. Esto contempla: contratación de dos profesionales, consultoría para el proyecto de desarrollo seguro, análisis de vulnerabilidades, actividades de sensibilización, entre otros, dicho presupuesto no ha sido aprobado a la fecha de elaboración del presente informe (24/10/2017).

6.4 Evaluar los riesgos, eventos y eficacia de los controles asociados.

Se verificó la aplicación y eficacia de controles y eventos asociados al Riesgo:

RGTIN42: Multas, sanciones e intereses de mora por parte de entidades de vigilancia y control debido a la omisión o deficiencias en la información presentada o publicada por FONADE por causa de la corrupción o pérdida de la misma; el cual, en el perfil de riesgo residual presenta impacto *mayor y* nivel de riesgo *moderado.*

Control:	Nombre del Control:
CTRGTIN39	Políticas de generación de contraseñas.
Comentarios	

Las contraseñas se asignan en concordancia con lo descrito en el manual MAP804 MANUAL DE GESTIÓN DE SEGURIDAD DE LA INFORMACION v.05B, en el Ítem: "Control de parámetros de seguridad de las contraseñas". Sincronizado desde el directorio activo- "Directivas de cuenta- Directivas de Contraseña": longitud mínima de la contraseña 8 caracteres; vigencia máxima de la contraseña 30 días.
De acuerdo con las verificaciones realizadas en la ejecución de la auditoria, se establece que no se aplican las directrices establecidas en el manual MAP804 Manual de Gestión de Seguridad de la Información V.5B:

- Solicitar al usuario el cambio obligatorio de la contraseña dada por defecto para el primer inicio de sesión.
- …" no debe contener el nombre de usuario ni la palabra FONADE"

Se registra No conformidad, para ser atendida por el proceso.

Se concluye que el control CTRGTIN39, presenta deficiencias, de acuerdo con los siguientes criterios:

1. El control realmente es utilizado	2. El control previene/mitiga el riesgo.	3. Se determinaron hallazgos sobre el control?	4. Eventos de riesgo reportados	5. Soportes de ejecución	6. ¿Se ejecuta la periodicidad definida?	7. Forma de ejecución	8. ¿Tiene responsable definido?	9. ¿Está documentado y socializado?	Evaluación de la Efectividad del Control
Casi Siempre	Parcialmente	SI	No se presentaron eventos de riesgo en la vigencia	No se generan soportes	Continuo	Automático	Lo ejecuta el responsable definido	Está en Catálogo documental y divulgado en la última vigencia	Con deficiencias

Control:	Nombre del Control:
CTRGTIN18	Seguimiento a los servicios de tecnología contratados con terceros
Comentarios	
Se observan actas de seguimiento al contrato 20161691 con radicados No.20174100000116, 20174100000186, 20174100000196, 20174100000426,20174100000576. Otras comunicaciones de seguimiento: 20174300354082. El resultado de la evaluación del control obedece al criterio *"está documentado y socializado"*	

Se concluye que el control CTRGTIN18, presenta deficiencias, de acuerdo con los siguientes criterios:

1. El control realmente es utilizado	2. El control previene/mitiga el riesgo.	3. Se determinaron hallazgos sobre el control?	4. Eventos de riesgo reportados	5. Soportes de ejecución	6. ¿Se ejecuta la periodicidad definida?	7. Forma de ejecución	8. ¿Tiene responsable definido?	9. ¿Está documentado y socializado?	Evaluación de la Efectividad del Control
Casi Siempre	Parcialmente	NO	No se presentaron eventos de riesgo en la vigencia	Se generan y se conservan los soportes	Continuo	Manual / Visual	Lo ejecuta el responsable definido	No está documentado y no está divulgado	Con deficiencias

Control:	Nombre del Control:
CTRGTIN03	Definición de derechos de acceso (perfil de autorización) de usuarios a los sistemas de información
Comentarios	
La gestión de acceso de usuarios a los sistemas de información se realiza desde el aplicativo de administración *de permisos del portal corporativo*, de acuerdo con las solicitudes realizadas por	

el usuario líder de cada uno por medio de la herramienta de gestión *Aranda (*ejemplo caso No.1564), según lo descrito en el procedimiento PDI463 Creación y administración de roles y privilegios de los usuarios de los servicios tecnológicos V.5A, sección *Agregar y autorizar permisos.*

Se concluye que el control CTRGTIN18, es eficiente de acuerdo con los siguientes criterios:

1. El control realmente es utilizado	2. El control previene/mitiga el riesgo.	3. Se determinaron hallazgos sobre el control?	4. Eventos de riesgo reportados	5. Soportes de ejecución	6. ¿Se ejecuta la periodicidad definida?	7. Forma de ejecución	8. ¿Tiene responsable definido?	9. ¿Está documentado y socializado?	Evaluación de la Efectividad del Control
Siempre	Parcialmente	NO	No se presentaron eventos de riesgo en la vigencia	Se generan y se conservan los soportes	Continuo	Manual / Visual	Lo ejecuta el responsable definido	Está en Catálogo documental y divulgado en la última vigencia	Eficiente

Control:	Nombre del Control:
CTRGTIN28	Gestión de usuarios
Comentarios	
Se aplica de acuerdo con lo descrito en el procedimiento PDI463 Creación y administración de roles y privilegios de los usuarios de los servicios tecnológicos V.5A. Se registra la legalización del contrato a través del aplicativo de Contratistas-FONADE, el cual genera un mensaje automático a los administradores que se tengan asignado, informando el nombre del usuario creado; para los funcionarios, se realiza desde el aplicativo de Nomina. Los permisos a los sistemas de información se gestionan desde el Módulo de Administración de usuarios y permisos del Portal Corporativo.	

Se concluye que el control CTRGTIN18, es eficiente de acuerdo con los siguientes criterios:

1. El control realmente es utilizado	2. El control previene/mitiga el riesgo.	3. Se determinaron hallazgos sobre el control?	4. Eventos de riesgo reportados	5. Soportes de ejecución	6. ¿Se ejecuta la periodicidad definida?	7. Forma de ejecución	8. ¿Tiene responsable definido?	9. ¿Está documentado y socializado?	Evaluación de la Efectividad del Control
Siempre	Parcialmente	NO	No se presentaron eventos de riesgo en la vigencia	Se generan y se conservan los soportes	Continuo	Manual / Visual	Lo ejecuta el responsable definido	Está en Catálogo documental y divulgado en la última vigencia	Eficiente

Control:	Nombre del Control:
CTRGTIN43	Sensibilización y entrenamiento en uso y apropiación de la tecnología y seguridad para los colaboradores de FONADE
Comentarios	
Como primera estrategia, se da inducción a los nuevos colaboradores en el marco de "JORNADA DE ORIENTACIÓN AL NUEVO SERVIDOR", coordinada por talento humano de acuerdo con lo programado en el PIC. También, en coordinación con el área de comunicaciones se genera piezas comunicacionales de distintos temas como: Uso y Apropiación de T.I: 14/06/2017 ¡Te invitamos a responder la Encuesta de Tecnología!: 05/07/2017 Agosto, mes del OneDrive en Fonade: 28/07/2017- Memorando No.20174100164873. Alerta de Phising: 19/09/2017	

Se concluye que el control CTRGTIN43, es eficiente de acuerdo con los siguientes criterios:

1. El control realmente es utilizado	2. El control previene/mitiga el riesgo.	3. Se determinaron hallazgos sobre el control?	4. Eventos de riesgo reportados	5. Soportes de ejecución	6. ¿Se ejecuta la periodicidad definida?	7. Forma de ejecución	8. ¿Tiene responsable definido?	9. ¿Está documentado y socializado?	Evaluación de la Efectividad del Control
Siempre	Parcialmente	NO	No se presentaron eventos de riesgo en la vigencia	Se generan y se conservan los soportes	Continuo	Manual / Visual	Lo ejecuta el responsable definido	Está en Catálogo documental y divulgado en la última vigencia	Eficiente

6.5 Realizar seguimiento al avance y/o cumplimiento de las acciones formuladas frente a los resultados de las auditorías anteriores y planes de mejoramiento de la Contraloría General de la Republica y Revisoría fiscal, si aplica.

- **Actividades control Interno**

De acuerdo con las actividades en término de vencimiento al último seguimiento realizado (junio 2017), se identificaron 12, con el siguiente estado:

Estado	Cantidad
Cumplida	9
Reformuladas	2
Total	11

Las dos actividades reformuladas, obedecen a la solicitud de ampliación del plazo para su ejecución y hacen referencia a: Actualización del manual MAP804 Manual de Gestión y Seguridad de la información y actualizar el perfil de riesgo operativo en SI.

- **Revisoría Fiscal**

La Revisoría Fiscal, emitió el "*Informe resultado auditoría sobre la evaluación diagnostico al Sistema de Gestión de seguridad de la Información*" mediante radicado N°2015-430-094648-2 del 04/12/2015. Según consulta realizada mediante correo electrónico (17 de agosto de 2017 09:44 a.m.) en el marco de esta auditoría, para conocer los planes de acción abiertos respecto al informe mencionado, se obtuvo la siguiente respuesta: "*seguimiento al informe de Sistema de Gestión de Seguridad de la Información del año 2015 y auditoria a la Gestión de Vulnerabilidades, el informe sobre estos dos temas se encuentra* pendiente por emitir". Sin embargo, se tomó como referencia el memorando N°20161300159001 del 22/06/2016, identificando las actividades:

- ✓ *Aprobación del documento: procedimiento gestión de LOGS: cumplida* con la publicación del PDI453 Gestión de registros de eventos para la plataforma tecnológica v.01.

- ✓ Diagnostico interno de cifrado de datos: cumplida en el plan de actividades del MSPI, actividad id:27 (anexo No.1)
- ✓ Actualización manual MAP804 *Manual de gestión de seguridad de la información:* reformulada para el 30 de noviembre 2017, según solicitud mediante correo electrónico (jueves, 31 de agosto de 2017 6:06 p. m) y alineada con actividades del plan de implementación del modelo de seguridad y privacidad de la Información 2017-2018.

Actualmente no hay planes de mejoramiento con la Contraloría General de la Republica, referentes al Seguridad de la Información.

6.6 Emitir conclusiones, especificando las No conformidades, observaciones y/o recomendaciones que según el análisis realizado sean procedentes

6.6.1 CONFORMIDADES

- Se establece que la entidad cuenta con: Diagnóstico de Seguridad y privacidad, Plan de Seguridad y Privacidad de la información, avance del 33,33% en la implementación del plan propuesto y gestiones de monitoreo y mejoramiento continuo.
- Cumplimiento de las actividades de auditorías anteriores, dentro de los términos propuestos.

6.6.2 NO CONFORMIDAD

- Se identificaron debilidades en la aplicación del control CTRGTIN39 *Políticas de generación de contraseñas*, en cuanto a las siguientes directrices establecidas en el manual *MAP804 Manual de Gestión de Seguridad de la Información V.5B:*
  - *Solicitar al usuario el cambio obligatorio de la contraseña dada por defecto para el primer inicio de sesión.*
  - *No debe contener el nombre de usuario ni la palabra FONADE.*

  También en concordancia con el literal “d) Forzar a los usuarios cambiar sus contraseñas cuando ingresan por primera vez” del *Instrumento de evaluación MSPI 2016_feb17_ajustadomar17.xlsx*-TECNICAS- ISO A.9.4.3, ITEM Sistema de gestión de contraseñas, brecha no identificada al diligenciar la matriz.

6.6.3 RECOMENDACIONES

- Revisar y complementar el instrumento de evaluación, tomando como referencia el instructivo emitido por el MINTIC en junio de 2017:” *Instructivo para el diligenciamiento de la herramienta del diagnóstico de seguridad y privacidad de la información v.01”*, debido a que se identificaron campos en blanco y/o con información muy general (ver numeral 6.1.1). Esto con el fin de contar con este documento debidamente diligenciado e

identificar oportunidades de mejora en el plan de implementación del Modelo de Seguridad y Privacidad de la Información, que está en curso.

Nota: Se consideró lo expuesto en el memorando No.20171300211013 de 18 de octubre 2017, si bien las guías e instructivos *emitidas por el MINTIC no son de forzosa aplicación*, estas brindan lineamientos que buscan fortalecer la gestión y adoptar mejores prácticas. Por lo tanto, se registra como recomendación, orientada en complementar dicho instrumento, sin que implique su diligenciamiento nuevamente.

- Revisar y acoger según se considere pertinente, aspectos descritos en los numerales 6.1.2, 6.3 y cuadro No.2 del presente informe, con miras a fortalecer el plan de actividades del modelo de seguridad y privacidad de la información 2017-2018 y el cumplimiento de las metas establecidas en el decreto 1078 de 2015.

Nota: Se consideró lo expuesto en el memorando No.20171300211013 de 18 de octubre 2017, donde se plasman comentarios a las actividades listadas en el cuadro No.2 y se hace claridad que el plazo para el registro nacional de base de datos- RNBD es 31 de enero 2019. Por lo anterior, se registra como recomendación, con el fin de tener en cuenta en el *plan de actividades*, lo expuesto en la columna "respuesta" del memorando mencionado.

- Publicar el perfil de riesgos en Seguridad de la Información 2016, en el espacio para este fin del catálogo documental de la Entidad, con el propósito que pueda ser consultado por todos los colaboradores.

Para la elaboración del presente informe se consideró lo expuesto en el memorando No.20171300211013 del 18 de octubre 2017 (sin anexos), generando los ajustes pertinentes respecto al informe preliminar.

Elaboró	Revisó	Aprobó
CELENY GONZALEZ PARRA	**ADRIANA MARIA OCAMPO LOAIZA**	**LUIS E. HERNANDEZ**
Auditora Control Interno	Líder de Auditorias SGC-SCI	Asesor de Control Interno

ANEXO No.1 SEGUIMIENTO PLAN DE ACTIVIDADES

id	actividad	fecha	Estado	Comentario	monitoreo
1	Adelantar Autodiagnóstico MSPI, acorde con requisitos Componente Seguridad y Privacidad, validar resultados con MINTIC	28-feb-17	Ejecutada	Se realizó el autodiagnóstico de acuerdo con la herramienta emitida por el MINTIC.	
2	Formular un Plan de Actividades 2017-2018 para la implementación del MSPI	28-feb-17	Ejecutada	Formulado y presentado en Comité Institucional de Desarrollo Administrativo del 27/03/2017- Punto 6 y 9. Acta No.43	
3	Presentar los resultados del diagnóstico del MSPI ante el CIDA y Alta Gerencia en el marco del Informe de Revisión por la Dirección	31-mar-17	Ejecutada	Presentado en Comité Institucional de Desarrollo Administrativo del 27/03/2017- Punto 7 y 11. Acta No.43 Comité de Gerencia No.49 del 28/03/2017- Punto 1.	
4	Formular propuesta de ajuste y/o complemento de funciones del Comité de Desarrollo administrativo respecto al MSPI	31-may-17	Ejecutada	Presentado en Comité Institucional de Desarrollo Administrativo del 21/03/2017 y 24/03/2017-punto 1. Acta No.43 y 44	
8	Definir especificaciones para la contratación de consultoría, diseño y protección de datos personales - Ley 1581 /2012	28-feb-17	Ejecutada	Mediante memorando No.20174100039673-13/02/2017	
9	Solicitar los estudios previos y de mercado para la contratación de la consultoría en materia de protección de datos personales - Ley 1581 / 2012	17-mar-17	Ejecutada	Mediante memorando No.20174100039673-13/02/2017. Contrato No.20171068.	
11	Formular propuesta de ajuste a la política de Tratamiento de Datos Personales y presentarla al Comité Institucional de Desarrollo Administrativo	31-may-17	Ejecutada	Presentado en Comité Institucional de Desarrollo Administrativo del 27/03/2017- Punto 10	
27	Realizar diagnostico Interno estado sobre cifrado	31-mar-17	Ejecutada	Se realizó el diagnostico de cifrado a los componentes: seguridad informática, desarrollo, infraestructura y bases de datos.	
29	Diseñar procedimiento para la Gestión de llaves asociado a la Política de Criptografía	23-ago-17	Por iniciar	Requiere de la ejecución de actividad 28 (30/11/2017)	
33	Definir procedimiento de Registro de Eventos, incluyendo fortalecimiento de controles.	30-jul-17	Ejecutada	PDI453GESTIÓN DE REGISTROS DE EVENTOS PARA LA PLATAFORMA TECNOLÓGICA V.1	
34	Proponer modelo de acuerdo de confidencialidad	31-ago-17	Ejecutada	Mediante memorando No.20171100148483-14/07/2017	

36	Definir plan de comunicación, sensibilización y capacitación en seguridad de la información	30-abr-17	Ejecutada	PLAN DE INDUCCIÓN, REINDUCCION Y CAPACITACIÓN EN SEGURIDAD DE LA INFORMACIÓN 2017.xlsx Las dos últimas semanas de octubre, se tiene prevista Actividad Lúdica / Celebración Día de la Seguridad de la Información, y la capacitación anual.	
39	Asesorar a áreas que requieran apoyo para la actualización de los activos de información	31-ene-17	Ejecutada	Mediante memorando No.20161300242253-14/10/2016	
40	Validar y consolidar inventario de activos de información actualizado	24-mar-17	Ejecutada	Una vez surtido el proceso de revisión con las áreas, se consolidaron 549 activos.	
41	Solicitar modificación del Formato FAP803 - Inventario y Clasificación de Activos incluyendo campos (Dec 103 / 2015)	28-feb-17	Ejecutada	FAP803 Formulario de identificación y clasificación de activos de información V.5	
42	Complementar información en inventario de activos según nuevos campos Dec 103 / 2015	31-mar-17	Ejecutada	Se incluyó el campo: Información publicada o disponible, los demás ya existían.	
43	Generar presentación con resultados de inventario de activos de información y realizar en CIDA para aprobación	30-abr-17	Ejecutada	El resultado de los activos a corte 2016, fue presentado en la sesión No.49 del Comité Institucional de Desarrollo Administrativo 30/06/2017-punto3	
44	Publicar inventario de activos de información (sujeto a ajustes posteriores según presentación en CIDA)	16-abr-17	Ejecutada	http://www.fonade.gov.co/portal/page/portal/WebSite/Fonade/AtencionalCiudadano/DatosAbiertos	
46	Instalación sistema de control de acceso biométrico	31-mar-17	Ejecutada	Mediante acta del 14/04/2017, se recibió a satisfacción el objeto contractual No.20161736.	
50	Consolidar Perfil de Riesgo 2016 en Seguridad de la Información	30-abr-17	Ejecutada	Se consolidó el perfil de riesgo 2016, sin embargo, aún no está disponible en el catálogo documental, en el espacio destinado para este fin.	☑
53	Ejecutar análisis de vulnerabilidades sobre plataforma tecnológica	31-mar-17	Ejecutada	Contrato 20161731 con password consulting services SAS.	☑
54	Consolidar y presentar resultados de análisis de vulnerabilidades	16-abr-17	Ejecutada	Informe escrito de resultados de análisis de vulnerabilidad realizado.pdf Resultados presentados en la sesión No.49 del Comité Institucional de Desarrollo Administrativo 30/06/2017-punto 8	☑
55	Formular plan de tratamiento vulnerabilidades identificadas a nivel de Infraestructura	31-may-17	Ejecutada	FAP805 plan de manejo de riesgos, con 4 actividades, para ejecución entre septiembre 2017 y febrero 2018.	☑

60	Gestionar la contratación de pruebas de seguridad física e ingeniería social	30-jun-17	Ejecutada	Contrato 20171008 con password consulting services SAS, según contratación CDI-145.	☑
64	Activar usuarios herramientas y dispositivos de seguridad	31-mar-17	Ejecutada	Herramientas informáticas de monitoreo: FIREWALL, antivirus	☑
67	Calcular indicadores del modelo de medición	31-mar-17	Ejecutada	Los resultados del segundo semestre 2016, presentados como parte del informe de monitoreo, en la sesión No.45 del Comité Institucional de Desarrollo Administrativo 27/03/2017- punto7. Respecto a los valores calculados en el archivo *indicadores.xlsx*, se observa que algunos no guardan correlación con el valor de las variables, Ej. GO005, GE0011, OPE001.	☑
68	Elaborar, revisar y presentar informe de monitoreo a la gestión de seguridad de la información	31-mar-17	Ejecutada	Resultados del 2S2016, presentados en la sesión No.45 del Comité Institucional de Desarrollo Administrativo 27/03/2017- punto7. , se tiene previsto para el mes de octubre el resultado del primer semestre 2017	☑
81	Elaborar y presentar informe Revisión por la Dirección	31-mar-17	Ejecutada	Comité de Gerencia No.49 del 28/03/2017- Punto 1.	☑
82	Seguimiento al avance de planes de tratamiento vulnerabilidades identificadas 2016-2017	24-mar-17	Ejecutada	El área de PYGR, realiza el seguimiento en el marco del monitoreo a Seguridad de la Información. La Asesoría de Control Interno, realiza seguimientos independientes cada 4 meses (ultimo a junio 2017)	☑
86	Informe Anual de Gestión de Seguridad de la Información	31/01/2017	Ejecutada	Presentado en Comité Institucional de Desarrollo Administrativo del 27/03/2017- Punto 7 y 11. Acta No.43 Comité de Gerencia No.49 del 28/03/2017- Punto 1.	☑