Al contestar por favor cite estos datos:
Radicado No.: 20161200288023

Pública [x] Privada [ ] Confidencial [ ]

Bogotá D.C, 20-12-2016

MEMORANDO

PARA: **MARY YAZMIN VERGEL CARDOZO**
Gerente área de Planeación y Gestión de Riesgos

BEATRIZ AMALIA SANCHEZ LUQUE
Gerente área Talento Humano

CARLOS ANTONIO MONROY ESCUDERO
Gerente área Tecnología de la Información

HECTOR MARIO AMAR GIL
Gerente área Servicios Administrativos

CON COPIA: **ARIEL ALFONSO ADUEN ANGEL**
Gerente General

BLANCA IRENE ECHAVARRIA LOTERO
Subgerente Administrativa

ASUNTO: **Notificación Informe Final auditoria SGSI 2016**

Respetados Doctores,

Adjunto para su conocimiento el informe final de la auditoria del asunto, realizada a las áreas Planeación y Gestión de Riesgos, Talento Humano, Tecnología de la Información y Servicios Administrativos

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, observaciones 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: Actividades, responsables y plazos, 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

AUDITORIA

Sistema de Gestión de Seguridad de la Información 2016

OBJETIVO GENERAL

Verificar la implementación del Modelo de Seguridad y Privacidad de la Información en la Entidad, en el marco normativo aplicable a FONADE y disposiciones internas vigentes.

OBJETIVOS ESPECIFICOS

1. Verificar el desarrollo de las etapas:
   - Planificación
   - Implementación
   - Evaluación del desempeño
   - Mejora continua
2. Evaluar los riesgos, eventos y eficacia de los controles asociados
3. 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.
4. Emitir conclusiones, especificando las No conformidades, observaciones y/o recomendaciones que según el análisis realizado sean procedentes

CRITERIOS

- Circular 038 de 2009 de la SUPERFINACIERA.
  Modelo de Seguridad y privacidad de la Información – MINTIC y las guías relacionadas (disponibles en http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html)
- Manual 3.2 Estrategia de Gobierno en Línea del Ministerio de las Tecnologías de la Información y las comunicaciones
- ISO/IEC 27001:2013, ISO/IEC 27002:2013.
- Norma Técnica de Calidad en la Gestión Pública (NTCGP 1000:2009).
- Disposiciones internas vigentes (Manuales, procedimientos, instructivos, guías, circulares): MAP804 Manual de gestión de seguridad de la información v.05, MAP805 Manual de Gestión de Riesgos Operativos V.06, GAP805 Guía metodológica de gestión de riesgos v.02, PAP816 Monitoreo a la gestión y al gobierno de la seguridad de la información institucional v.02
- Ley 1266 2008- Hábeas Data, Ley 1581 2012- Protección de datos personales, Ley 1712 de 2014- Transparencia y Acceso a la Información Pública.

ALCANCE

Octubre 2015- octubre 2016

METODOLOGIA

La obtención de la evidencia se realizó mediante las siguientes técnicas:

Entrevistas

Mary Yazmin Vergel	Gerente área Planeación y Gestión de Riesgos - 20/10/2016
Diana Jaidy Piñeros	Líder Gobierno en Línea - 24/10/2016
Angel Reinaldo Nuncira	Profesional Junior1 con asignación de obligaciones de la Gerencia del área de Tecnología de la Información-24/10/2016
Juan Manuel Reyes	Oficial de Seguridad Informática -24/10/2016
Johan Giovanni Millan	Profesional área Talento Humano- 27/10/2016
María del Pilar Espinel	Profesional área Talento Humano -27/10/2016
Astrid Gregoria Alvarez	Profesional área Talento Humano -27/10/2016

Revisión documental

- MAP804 Manual de gestión de seguridad de la información V.05
- InformeSemestralSegInfo1Q2015.pptx
- RF-098-2015 informe SGC de la información.pdf
- Cronograma de trabajo_2sem16.xlsx
- Actas de Comité Institucional desarrollo Administrativo
- Informe final auditoria SGSI2015.
- PERFIL DE RIESGO RESIDUAL EN SEGURIDAD DE LA INFORMACIÓN 2015

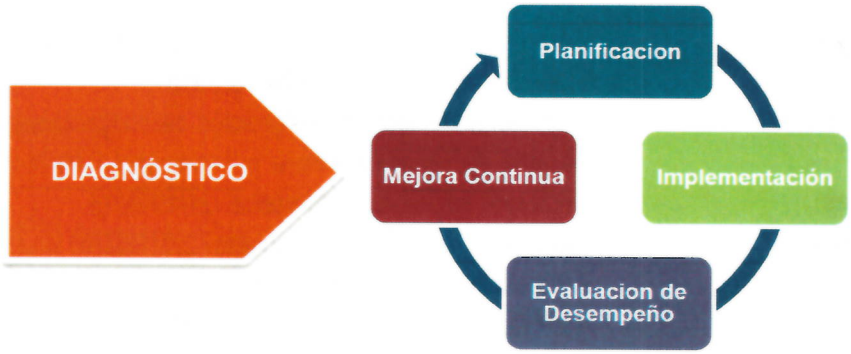
Pruebas de funcionalidad

Bloqueo y activación de cuentas de usuario, desde el aplicativo de "Nomina".

DESARROLLO

INTRODUCCIÓN

De acuerdo al Modelo de Seguridad y Privacidad de la Información – MSPI, se definen 5 etapas así:



Fuente: Modelo de Seguridad y Privacidad de la Información v.3.02

El desarrollo de cada una, permite que las entidades puedan gestionar adecuadamente la seguridad y privacidad la información, para lo cual presenta objetivos, metas y herramientas (guías) que facilitan su implementación, como componente transversal a la Estrategia de Gobierno en línea.

Respecto a la etapa de diagnóstico que pretende identificar el estado actual de la Entidad frente a los requerimientos del Modelo de Seguridad y Privacidad de la Información, el área de Planeación y Gestión de Riesgos, en el primer semestre 2015, realizó un autodiagnóstico con el objetivo:" *Evaluar el estado de cumplimiento de FONADE de los requerimientos y requisitos de la norma ISO/IEC 27001:2013 con el propósito de formular un plan para cerrar las brechas*". La conclusión general fue:"*el Índice general de cumplimiento del SGSI en FONADE del 63%*".

El detalle se presentó en el comité Institucional de Desarrollo Administrativo del 24/06/2015, en el punto 5 del orden del día, acompañado de una propuesta de actividades para atender las debilidades identificadas; lo cual no presento continuidad, dado que en lo transcurrido del año 2016, no se ha contado con el Oficial de seguridad de la información.

1. Verificar el desarrollo de las etapas

1.1 Planificación

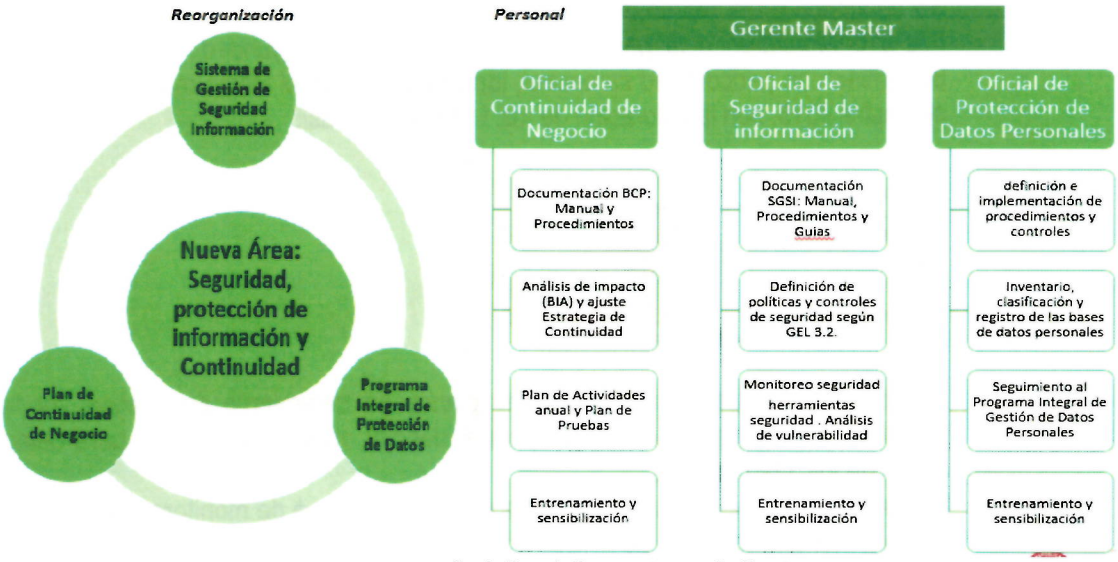
Busca definir las políticas, alcance, procedimientos, metodología para tratamiento de riesgo, roles y responsabilidades, entre otros, alineado con el objetivo misional de la Entidad, confirmando su aplicación frente a:

Aspecto	*Comentario*
Alcance	**MAP804**: Numeral 7.1.1 Alcance del SGSI: aplica para todos los procesos, según el mapa de procesos establecido en el sistema de gestión de calidad (SGC). A nivel normativo se listan las leyes aplicables. Importante revisar y complementar: Ley 1712 de 2014 y manual GEL 3.2. En esta sección se menciona:" El alcance del SGSI será revisado por la Alta Dirección anualmente para asegurar su concordancia con la orientación estratégica de la Entidad", tema que no se ha cumplido.
Políticas	**MAP804:** Numeral 7.1.2 Política institucional de seguridad de la información. En el numeral 8. Lineamientos de gestión de seguridad de la información, se describe la política y lineamientos para: • La gestión de talento humano. • A nivel de usuario final. • Seguridad física, sobre la gestión documental y comunicación oral. • Seguridad informática. • Cumplimiento de requisitos normativos sobre seguridad de la información. En el anexo 1 – política de tratamiento de la información personal de FONADE.
Inventario de activos de información	**MAP804**: Numeral 8.2.2 clasificación de información y gestión de riesgos e incidentes en seguridad de la información. Se hace uso del formato FAP803 formulario de identificación y clasificación de activos de información, de acuerdo a lo descrito en el PAP812 gestión del Riesgo, numeral 6.1 identificación, medición y control de riesgos- actividad N°2. La metodología se describe en el ANEXO No. 2: METODOLOGÍA PARA EL INVENTARIO Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN, de la GAP805 guía metodológica de gestión de riesgos
Identificación, Valoración y Tratamiento de Riesgos.	**MAP804**: Numeral 7.1.6 Identificación y valoración de riesgos en seguridad de la información, describe: "La metodología para la identificación y valoración del perfil de riesgo en seguridad de la información está integrada con la metodología del Sistema de Administración del Riesgo Operativo (SARO) y está descrita en el manual MAP805 Manual de Gestión de Riesgos Operativos y en sus procedimientos asociados", como PAP812 Gestión del Riesgo y GAP805 Guía metodológica de gestión de riesgos.
Análisis de vulnerabilidades	**MAP804**: Numeral 8.2.2 Clasificación de información y gestión de riesgos e incidentes en seguridad de la información, describe: "...por lo menos una vez al año, procesos de análisis de vulnerabilidades sobre los activos de información, infraestructura tecnológica y física que los soporta, y comportamiento de administradores y usuarios finales en relación con la seguridad de la información".
Plan de comunicaciones y sensibilización	**MAP804**: Numeral 8.1.2 Entrenamiento y sensibilización en seguridad de la información.

Información documentada	Los siguientes documentos disponibles en el catálogo del Sistema de Gestión de Calidad-SGC de la Entidad, hacen referencia a los lineamientos y procedimientos de seguridad de la Información: • MAP804 manual de gestión de seguridad de la información. • MAP452 manual de Gestión de la tecnología de la información y las comunicaciones • MAP453 Manual de continuidad del negocio y documentos relacionados. • PAP805 Gestión de incidentes en seguridad de la información • PAP816 Monitoreo a la gestión y gobierno de la seguridad de la información institucional. • PAP468 Control de cambios a infraestructura tecnológica. • PAP457 Adquisición, desarrollo y puesta en producción de software • PAP463 administración de roles y privilegios de los usuarios de los servicios tecnológicos • GAP805 Guía metodológica de gestión de riesgos Se considera importante hacer un inventario de la documentación disponible, en concordancia con lo descrito en la guía N°.3 procedimiento de seguridad del MSPI, con el fin complementar la información faltante.
Plan de transición de IPv4 a IPv6	Se incluyó en la proyección del presupuesto para la vigencia 2017 del área de TI, según memorando 20164100231113 del 30/09/2016, con descripción del proyecto "consultoría actualización protocolo IPV6".
Roles y responsabilidades	**MAP804:** Numeral 7.1.4 Roles y responsabilidades en la gestión de seguridad de la información, se describen las responsabilidades, el cual debe ser ajustado de acuerdo a la estructura organizacional actual de la Entidad.

Para el último ítem, teniendo en cuenta que desde mayo 2016, no se ha contado con el rol de Oficial de seguridad de la información, el área de PYGR, ha realizado las siguientes gestiones:

- Solicitud de personal para el desarrollo de las funciones de seguridad de la información, mediante memorando dirigido a la Gerencia General, con radicado No. 20161300144023 del 13/06/2016. No se obtuvo respuesta formal.
- Proceso de contratación del oficial de seguridad de la información de acuerdo a "solicitud de contrato de prestación de servicios", con radicado No.20161300266363 del 21/11/2016, que dio lugar al contrato N°.20161701 del 09/12/2016.
- Reunión con el Gerente General, Subgerente Administrativa, Gerente área de Tecnología de la Información y Gerente área Servicios administrativos, adelantada en 12/10/2016 con el objetivo de presentar la propuesta de reorganización y redistribución de funciones del Plan de Continuidad y Seguridad y protección de datos personales, resumida en la siguiente imagen:



Fuente: Presentación propuesta reorganización.pptx

Al respecto, la Gerente de Planeación y Gestión de Riesgos, manifiesta que se cuenta con el aval de la Gerencia General, en relación a esquema planteado, pero se está definiendo a que dependencia quedaría adscrita la nueva área.

Adicionalmente, debido a los cambios que ha surtido la Entidad a nivel organizacional y tecnológico, se confirma el proceso de actualización del manual MAP804, frente a:

- Memorando No.20151300284323 del 17/11/2015, dirigido por el área de Planeación y Gestión de Riesgos, a las áreas: Tecnología de la Información, Servicios Administrativos, Talento Humano y Asesoría de Control Interno, con el asunto "Revisión propuesta del manual…".
- Correo respuesta Asesoría de Control Interno:
  Enviado el: miércoles, 16 de diciembre de 2015 10:24 a.m.
  Para: <aalmanza@fonade.gov.co>
  CC: Mary Yazmin Vergel Cardozo <yvergel@fonade.gov.co
  Asunto: RV: Memorando Revisión propuesta de actualización del Manual de Gestión de Seguridad de la Información MAP804.
- Memorando No.20164100191933 del 10/08/2016, emitido como respuesta por el área de Tecnología de la Información.
- Borrador del documento: *MAP804 Manual de Gestión de Seguridad de la Información Ver T.I.*docx

Se manifiesta la importancia de agilizar la actualización, dado que dicho proceso se inició hace un año, como también evaluar la pertinencia de integrar las políticas, lineamientos y procedimientos de *privacidad y tratamiento de información personal*, que en la versión actual se describe en uno de sus anexos.

1.2 Implementación

Se revisaron los siguientes ítems:

- Implementación y nivel de madurez de controles.

Se establece en el marco del monitoreo a la seguridad de la información, que el procedimiento PAP816 *Monitoreo a la gestión y al gobierno de la seguridad de la información institucional*, determina con periodicidad semestral, identificando que el último realizado, corresponde al primer semestre 2015, con la valoración de los 114 controles así:

Nivel	1° semestre 2015
Satisfactorio	38
Aceptable	71
Critico	5
Total	114

Fuente: informe final auditoria SGSI2015

Al respecto, las áreas presentaron los planes de tratamiento de riesgos, mediante el formato FAP805 *Plan de manejo de riesgos*, sin evidenciar nuevas mediciones para determinar el estado actual de los 114 controles.
Se confirma el inicio de la gestión, para realizar el informe de monitoreo del primer semestre 2016, frente a memorandos No. 20161300182133 del 28/07/2016 y 20164100202653 del 26/08/2016, de solicitud de información al área de TI y su respuesta, respectivamente; a la fecha de la auditoria, el área de Planeación y Gestión de Riesgos, surte el proceso de revisión y consolidación de la información recibida; sin embargo, faltan insumos como el estado y valoración de los controles de seguridad de la información, que son suministrados por las áreas, medición de los indicadores y seguimiento a los planes de tratamiento.
Se considera pertinente mencionar que la declaración de aplicabilidad, descrita en el ANEXO 2 – "DECLARACIÓN DE APLICABILIDAD" del manual MAP804, hace referencia a los 133 controles de los 11 dominios y 39 objetivos de control que componen la norma NTC-ISO/IEC 27002:2007, lo cual se debe actualizar de acuerdo a la norma ISO/IEC 27002:2013, bajo la cual se realizó la última valoración.

- Inventario activos información

Se realiza anualmente, como insumo para los procesos de continuidad del Negocio y dar cumplimiento a los requerimientos normativos. El informe para el año 2015, se presentó en Comité Institucional de Desarrollo Administrativo el 06 de agosto 2015, en el punto 6 de la agenda, siendo el resultado 562 activos clasificados así:

Aspecto	*clasificación*	*cant*	*clasificación*	*cant*	*clasificación*	*cant*
Criticidad	Críticos	84	No críticos	478		
Ley de transparencia	Publica	256	Publica clasificada	295	Publica reservada	11
Datos personales	Si registra	134	No Registra	428		
Tratamiento datos	Si Requiere	33	No requiere	101		

Fuente: informe final auditoria SGSI2015

Para el año 2016, se inició el levantamiento de información para la identificación y clasificación de los activos, de acuerdo al memorando enviado a todas las áreas por Planeación y Gestión de Riesgos con radicado No. 20161300242253 del 14/10/2016, donde se expone el plan de trabajo, tema socializado en la capacitación a los responsables el día 11/11/2016. Posteriormente se envió

a cada proceso la documentación y fechas propuestas para revisar y diligenciar el formato FAP803 *Formulario de identificación y clasificación de activos de información*, y así concluir el inventario antes de finalizar la vigencia 2016.

- Identificación y Plan de tratamiento de riesgos

Se confirma su aplicación frente a Perfil de Riesgo en Seguridad de la información 2015, disponible en la siguiente ruta:
http://www.fonade.gov.co/CatalogoDocumental/riesgos/subversion/SAR/SARO/SGSI/Catalogo_Documental_SGSI.htm

Resumidos así:

Nivel de riesgo absoluto	Cantidad
Inaceptable	26
Importante	33
Moderado	14
Tolerable	4
Aceptable	0
Total	77

Nivel de Riesgo Residual	Cantidad
Importante	12
Moderado	39
Tolerable	19
Aceptable	7
Total	77

Como se observa:

- ✓ De los 59 riesgos en nivel "inaceptable" e "importante", una vez se aplican los controles, se pasa a 12 en "importante", lo cual indica una reducción 47 riesgos que corresponde a un 80%.
- ✓ Los 12 riesgos en nivel importante, 10 presentan consecuencia residual "mayor" y 2 "catastrófico", estos últimos se evalúan en el punto 2. del presente informe.

De acuerdo al perfil de riesgo residual y monitoreo semestral a la gestión de seguridad de la información, las áreas formularon los planes de tratamiento de riesgos, por medio del formato *FAP805 Plan de manejo de riesgos*, siendo los últimos disponibles en el espacio destinado para su publicación y divulgación, los correspondientes al año 2014.

Para el año 2016, se están realizando mesas de trabajo con las áreas, para la actualización del perfil de riesgos de la Entidad y de allí seleccionar los correspondientes a seguridad de la Información, se espera contar con esta actualización, a diciembre 2016, con el fin de presentar y publicar los resultados y formular los planes de tratamiento que de allí se generen.

Se manifiesta la importancia de considerar ampliar la descripción a "*perfil de riesgo en seguridad y privacidad de la información*", así como tener en cuenta en la actualización del perfil de riesgo, la inclusión de riesgos relacionados con la protección de datos personales, sus controles y tratamiento de riesgos; teniendo en cuenta que en la matriz, solo se identifica el riesgo RGRIE18 "*Deterioro de la imagen o reputación de la Entidad por reclamaciones de clientes, contratistas proponentes u otras partes interesadas debido a la divulgación de información confidencial relacionada con estos por causa de errores en el manejo de la misma por parte de colaboradores de la Entidad*".

- Indicadores de Gestión

  La definición de los indicadores desde el punto de vista de *Gobierno* y de *Gestión*, se describe en el numeral 5. *Modelo de medición de seguridad de la información* de la *GUÍA METODOLÓGICA MONITOREO DE SEGURIDAD DE LA INFORMACION v.01,* que se encuentra en revisión para su publicación en el catálogo documental de la Entidad.

- Análisis de vulnerabilidades

  Para la vigencia 2016, se llevó a cabo en el marco del contrato N°20151569 con la firma Olimpia.S.A, para 17 servidores y 15 aplicaciones WEB. El informe se presentó en comité institucional de desarrollo administrativo del 15 de junio 2016, en el punto 4 de la agenda. Las vulnerabilidades identificadas como "críticas" y "altas" son:

Aplicaciones			
Criticas	Suplantación de sesión	Altas	Inyección de codigo SQL
	Elevación de privilegios		Cross Site Scripting
	Validación de archivos		Cross Site Request Forgery
Total	3	Total	3

Infraesctructura			
Criticas	Acceso remoto no autorizado	Altas	Software desactualizado
	Shellshock		Acceso a servicio LDAP nulo
	Sistema operativo sin soporte		Denegación de servicio
	Acceso no autorizado		MS12.020
			MS15.034
			Oracle TNS listener remote poisoning
			Comunidad SNMP por defecto
Total	4	total	7

Al respecto el área de Tecnología de la información, presentó el plan de tratamiento de riesgos, mediante el formato FAP805 *plan de manejo de riesgos* con fecha 28/08/2016.

Dado el cambio presentado en la infraestructura tecnológica en los meses de junio y julio del presente año, referente a la migración de los servidores del centro de cómputo principal hacia la nube, está en proceso de contratación *el análisis de vulnerabilidades relacionadas con seguridad de la Información*, de acuerdo a solicitud de estudios previos mediante memorando

No.20161300234873 del 04/10/2016; respuesta con radicado No.20165000254003 del 11/01/2016, donde se requiere el CDP y definición del (los) oferentes que se van a invitar para desarrollar el proceso correspondiente.
Una vez surtido el proceso, se eligió la firma PASSWORD CONSULTING SERVICES S.A.S, con solicitud de contratación mediante memorando No.20161300267013 del 22/11/2016.

- Cumplimiento legislación relacionada con protección de datos personales.

  Se han realizado ajustes a los aplicativos, en el marco del plan de acción de la auditoria SGSI2015, de acuerdo al caso de desarrollo No.1520, que a la fecha (18/11/2016), se encuentra en espera de asignación del usuario líder para realizar las pruebas de usuario.

  Teniendo en cuenta que la aplicación de la ley 1581/2012, va más allá de los ajustes a los aplicativos, para atender este requerimiento que incluye el registro en el RNBD (Registro Nacional de Base de Datos), se está gestionando la contratación de una consultoría con el objetivo "*Diagnóstico del estado actual de la Entidad en cuanto al cumplimiento de la Ley 1581/2012 y sus decretos reglamentarios (Aspectos jurídicos y técnicos)*". Para lo cual se tiene propuesta de 3 proveedores: OLIMPIA, ETEK y ADALID, que se definirá de acuerdo a la asignación del presupuesto para la vigencia 2017. Así mismo se cuenta con el concepto de la Asesoría Jurídica, mediante memorando N°.20161100260323 del 11/11/2016, como respuesta a:" solicitud de lineamientos en materia de protección de datos personales", realizada por el área de Planeación y Gestión de Riesgos con radicado N°20151300284303; por consiguiente es prioritario atender lo descrito en dicha respuesta.

- Plan de sensibilización

  En el Plan Institucional de Capacitación-PIC 2016, se incluye en el ítem 5 "*Sensibilización en Seguridad de la Información (charlas colaboradores y/o congresos y/o cine foro y/o charlas directivos y/o campañas de difusión, etc.), utilizando como mecanismo la jornada mensual de Orientación al Nuevo Servidor- ONS*, llevadas a cabo en la siguientes fechas, según boletín de invitación enviado por el área de comunicaciones: 26/02/2016, 31/03/2016, 29/04/2016, 27/05/2016, 30/06/2016, 29/07/2016, 26/08/2016, 23/09/2016, 27/10/2016 y 25/11/2016.

  También, por los medios disponibles para comunicación interna, se han divulgado los siguientes temas:

Tema	Medio	Fecha
Capacitación Protección de Datos Personales - SIC	Presencial- auditorio	15/11/2016
Actualización del inventario y clasificación de activos de información - 2016	Presencial- auditorio	11/11/2016
¡TE INVITAMOS A DILIGENCIAR LA ENCUESTA DE SEGURIDAD DE LA INFORMACIÓN!	Correo electrónico	14/10/2016
¡TE INVITAMOS A DILIGENCIAR LA ENCUESTA DE SEGURIDAD DE LA INFORMACIÓN!	Correo electrónico	20/10/2016
PARA OBTENER 'PERMISOS' EN TU USUARIO, RECUERDA:	Correo electrónico	18/07/2016
Tú también puedes ser víctima del "Phishing".	Correo electrónico	25/05/2016
La importancia de los escritorios limpios en FONADE	Correo electrónico	15/03/2016
La importancia del respaldo de la información	Correo electrónico	07/03/2016
¿Cómo colocar contraseñas fáciles de recordar y difíciles de adivinar?	Correo electrónico	29/02/2016
Puedes ser víctima del "Phishing"	Correo electrónico	22/02/2016
¿Cómo protegerse de las estafas? - Seguridad de la Información	Correo electrónico	28/12/2015

Para la etapa de implementación, se puede concluir que es necesario: Establecer el nivel de madurez de los 114 controles, culminar la actualización del perfil de riesgo y formular los planes de tratamiento, realizar la medición de los indicadores definidos en la *GUÍA METODOLÓGICA MONITOREO DE SEGURIDAD DE LA INFORMACION* (en proceso de revisión) y generar el documento detallado con el plan de transición e implementación del protocolo IPv6.

1.3 Evaluación del desempeño

- Plan de seguimiento y evaluación

Dentro de los mecanismos, se tiene establecido el "monitoreo a la seguridad de la información", con una periodicidad semestral, de acuerdo al procedimiento PAP816 "*Monitoreo a la gestión y al gobierno de la seguridad de la información institucional*", el último informe realizado corresponde al primer semestre 2015.

- Auditoria interna

En la ejecución del plan anual de auditorías, se realiza la auditoria referente a Seguridad de la información, generando un informe final con la descripción de las no conformidades, observaciones y/o recomendaciones, el cual es notificado a las áreas. Se mencionan los dos últimos:

Radicado No.	Fecha	Año
20151200239733	21/09/2015	2014
20151200320413	30/12/2015	2015

Cabe anotar, que uno de los principales insumos para evaluar el desempeño del MSPI, es el resultado de los indicadores de la seguridad de la información, que permiten medir la efectividad, la eficiencia y la eficacia de las acciones ejecutadas, por tanto es importante contar con su medición.

1.4 Mejora continua

- Acciones correctivas- preventivas

Frente a cada informe, las áreas responsables, emiten el plan de acción, el cual es objeto de seguimiento por parte de la Asesoría de Control interno, cada 4 meses, según lo establecido en el

procedimiento PAU001 *auditorías internas de control interno.* Como también es un objetivo de la ejecución de cada auditoria, que para este caso se desarrolla en el punto **No. 3** del presente informe.

➢ Revisión por la dirección

Dentro del plan de acción de la auditoria SGSI 2015, se formularon actividades referentes al compromiso de la alta dirección: "Ejecución de la revisión por dirección del SGSI", con fecha 31/08/2016, sin confirmar su cumplimiento.

En relación con las etapas, metas y niveles de madurez del Modelo de Seguridad y Privacidad de la Información-MSPI, se establece que la Entidad, registra avance así:

Nivel	*% Alcanzado*
0 INEXISTENTE	N/A
1 INICIAL	100
2 REPETIBLE	60
3 DEFINIDO	55
4 ADMINISTRADO	MINIMO
5 OPTIMIZADO	MINIMO

De acuerdo a la revisión de los siguientes ítems:

	INICIAL	S/N	comentario	
1	Se han identificado debilidades en la seguridad de la información.	S	Se identifican mediante mecanismos como: Registro de eventos de riesgo operativo, auditorias internas y monitoreo de seguridad de la información.	100%
2	Los incidentes de seguridad de la información se tratan de forma reactiva.	S	Según procedimiento PAP805 GESTIÓN DE INCIDENTES EN SEGURIDAD DE LA INFORMACIÓN	
3	Se tiene la necesidad de implementar el MSPI, para definir políticas, procesos y procedimientos que den respuesta proactiva a las amenazas sobre seguridad de la información que se presentan en la Entidad.	S	Las áreas que lideran el tema, conocen la necesidad de implementar el MSPI, no solo en cumplimiento del marco normativo, sino para salvaguardar la información de la Entidad.	

	REPETIBLE	S/N	comentario	
1	Se identifican en forma general los activos de información.	S	Cada año la Entidad realiza el ejercicio de actualización de los activos de información.	60%
2	Se clasifican los activos de información.	S	Se clasifican en aspectos como: criticidad, ley de transparencia, datos personales y tratamiento de datos.	
3	Los servidores públicos de la entidad tienen conciencia sobre la seguridad de la información.	N	Se realizan campañas y piezas de sensibilización por los medios que la Entidad tiene definidos para la comunicación interna, pero se debe fortalecer este aspecto.	
4	Los temas de seguridad y privacidad de la información se tratan en los comités del modelo integrado de gestión.	S	Se tratan en instancias como: Comité Intitucional de Desarrollo Administrativo y Comité integral de riesgos.	
5	La entidad cuenta con un plan de diagnóstico para IPv6.	N	Incluido en el presupuesto 2017,según memorando 20164100231113 del 30/09/2016, con descripción del proyecto "consultoría actualización protocolo IPV6"	

	DEFINIDO	S/N	comentario	
1	La Entidad ha realizado un diagnóstico que le permite establecer el estado actual de la seguridad de la información.	N	Se realizó un primer ejercicio de autodiagnostico en el primer semestre 2015.	55%
2	La Entidad ha determinado los objetivos, alcance y límites de la seguridad de la información.	S	Se cuenta con la politica de seguridad, alcance y lineamientos definidos en el manual MAP804 manual de gestion de seguridad de la Información v.05, el cual esta en proceso de actualización de acuerdo a la situación actual de la Entidad.	
3	La Entidad ha establecido formalmente políticas de Seguridad de la información y estas han sido divulgadas.	N	La politica de seguridad, esta establecida en el manual MAP804 manual de gestion de seguridad de la Información v.05 -2013/11/28. Requiere ser divulgada.	
4	La Entidad tiene procedimientos formales de seguridad de la Información	S	MAP804 manual de gestion de seguridad de la Información v.05; PAP805 Gestión de incidentes en seguridad de la información;PAP816 Monitoreo a la gestión y al gobierno de la seguridad de la información institucional;MAP452 Manual de Gestión de la tecnología de la información y las comunicaciones	
5	La Entidad tiene roles y responsabilidades asignados en seguridad y privacidad de la información.	N	Se describe en el numeral 7.1.4 Roles y responsabilidades en la gestión de seguridad de la información, del manual MAP804, pero no estan actualizados.	
6	La Entidad ha realizado un inventario de activos de información aplicando una metodología.	S	En el 2015 se presento en el Comité Institucional de Desarrollo Administrativo-06/08/2016; para el 2016 se inició la actividad según lo descrito en el memorando No.20161300242253 -14/10/2016 y capacitación del 11/11/2016.	
7	La Entidad trata riesgos de seguridad de la información a través de una metodología.	S	Metodologia del Sistema de Administración de Riesgo Operativo	
8	Se implementa el plan de tratamiento de riesgos.	S	Las áreas reportan el plan, de acuerdo al formato FAP805 Plan de manejo de riesgos	
9	La entidad cuenta con un plan de transición de IPv4 a IPv6.	N	Incluido en el presupuesto 2017,según memorando 20164100231113 del 30/09/2016, con descripción del proyecto "consultoría actualización protocolo IPV6"	

Lo anterior indica que la Entidad:

- Reconoce que tiene problemas de seguridad y que estos necesitan ser resueltos.
- Cuenta con procedimientos de seguridad de la información, los cuales requieren ser revisados y actualizados de acuerdo a los cambios que van surgiendo.
- Tiene una metodología formal y documentada para el tratamiento de riesgos.
- Requiere trabajar en aspectos como: monitoreo periódico a seguridad de la Información, evaluar efectividad actual de los controles (ISO 27002:2013) y planear la migración de protocolo de IPV4 a IPV6, que atienden ítems de los niveles "administrado" y "optimizado".
- Debe realizar un diagnóstico de la seguridad y privacidad de la información, de manera que el resultado detallado, sea el insumo para determinar los aspectos a fortalecer o a incluir en la planificación y etapas posteriores, que van a permitir el cumplimiento de la meta establecida por el MINTIC, para la implementación del 100% del componente de *seguridad y privacidad* en el año 2018.

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

De acuerdo al *PERFIL DE RIESGO RESIDUAL EN SEGURIDAD DE LA INFORMACIÓN 2015*, se seleccionaron los riesgos con consecuencia residual "Catastrófico".

Código del Riesgo	Descripción
RGADM64	Impacto operacional por la falta de disponibilidad de aplicativos y/u otros servicios tecnológicos debido a fallas en el funcionamiento, conexión y/o menor rendimiento de los mismos por causa de la suplantación de privilegios de administrador por parte de colaboradores de la Entidad.
Código del control	**Descripción**
CTRGADM139	Políticas de generación de contraseñas
Comentarios	
Políticas de generación de contraseñas. Las contraseñas se asignan de acuerdo a lo descrito en el manual MAP804 MANUAL DE GESTIÓN DE SEGURIDAD DE LA INFORMACION, en el apartado: "Control de parámetros de seguridad de las contraseñas". Sincronizado desde el directorio activo, con las siguientes directivas: longitud mínima de la contraseña 8 caracteres; requisitos de complejidad habilitados; vigencia máxima de la contraseña 30 días;exigir historial de contraseñas- 8 contraseñas recordadas.	

1. Tipo de control	2. Forma de ejecución	3. Documentado	4. Soportes de ejecución	5. Frecuencia de aplicación del control	6. El control previene/mitiga el riesgo	Evaluación de la Efectividad del Control
Preventivo	Manual / Visual	Formalmente documentado	No se generan soportes	Continuo	Parcialmente	Con deficiencias

El resultado de la evaluación obedece a la forma y soportes de ejecución.

Código del Riesgo	Descripción
RGADM88	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 mediante el acceso no autorizado por parte de colaboradores a los sistemas de información.
Código del control	**Descripción**
CTRGADM038	Definición de derechos de acceso (perfil de autorización) de usuarios a los sistemas de información
Comentarios	
Se administran desde el portal corporativo, "modulo administrador de usuarios y permisos", según lo establecido en el procedimiento PAP463 "Creación y administración de roles y privilegios de los usuarios de los servicios tecnológicos" v.05 numeral 6.2 MODIFICACIÓN DE ROLES Y PERFILES DE USUARIOS	

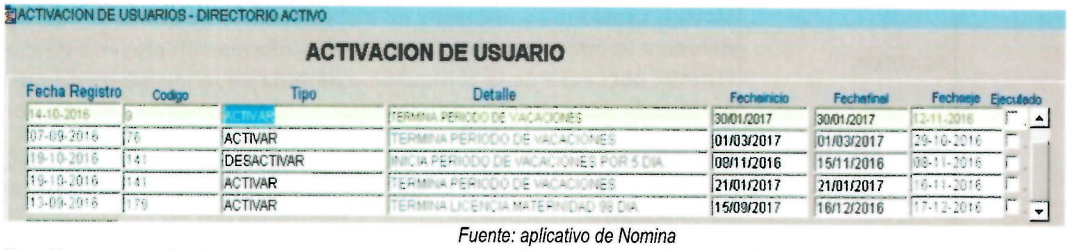
1. Tipo de control	2. Forma de ejecución	3. Documentado	4. Soportes de ejecución	5. Frecuencia de aplicación del control	6. El control previene/mitiga el riesgo	Evaluación de la Efectividad del Control
Preventivo	Semi automático	Formalmente documentado	Se generan y se conservan los soportes	Continuo	Parcialmente	Eficiente

Se recomienda revisar y actualizar el atributo 4.soportes de ejecución, dado que existen soportes como: Log de auditoria, correos electrónicos y casos registrados en la herramienta de gestión "Aranda" en la categoría "seguridad de la información "solicitud de permisos sobre recursos informáticos".

Código del Riesgo	Descripción
RGADM88	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 mediante el acceso no autorizado por parte de colaboradores a los sistemas de información
Código del control	**Descripción**
CTRGADM117	Gestión de usuarios
Comentarios	
De acuerdo a lo descrito en el procedimiento PAP463 Creación y administración de roles y privilegios de los usuarios de los servicios tecnológicos. Con profesional del área de Talento Humano, se confirma la funcionalidad "Activación de usuario" del aplicativo Nomina, que aplica para novedades: vacaciones, licencias de maternidad y retiros.	

1. Tipo de control	2. Forma de ejecución	3. Documentado	4. Soportes de ejecución	5. Frecuencia de aplicación del control	6. El control previene/mitiga el riesgo	Evaluación de la Efectividad del Control
Preventivo	Semi automático	Formalmente documentado	Se generan y se conservan los soportes	Continuo	Parcialmente	Eficiente

Importante revisar funcionalidad "Activación de usuario" del aplicativo de nómina para novedades: " Incapacidad/Licencia/Compensatorios/Comisiones" de acuerdo a lo descrito en el numeral 7.2 Anexo No. 2, del procedimiento PAP463 v05.


ACTIVACION DE USUARIOS - DIRECTORIO ACTIVO

ACTIVACION DE USUARIO

Fecha Registro	Codigo	Tipo	Detalle	Fechainicio	Fechafinal	Fecheeje	Ejecutado
14-10-2016	5	ACTIVAR	TERMINA PERIODO DE VACACIONES	30/01/2017	30/01/2017	12-11-2016	
07-09-2016	76	ACTIVAR	TERMINA PERIODO DE VACACIONES	01/03/2017	01/03/2017	28-10-2016	
19-10-2016	141	DESACTIVAR	INICIA PERIODO DE VACACIONES POR 5 DIA	08/11/2016	15/11/2016	08-11-2016	
19-10-2016	141	ACTIVAR	TERMINA PERIODO DE VACACIONES	21/01/2017	21/01/2017	16-11-2016	
13-09-2016	179	ACTIVAR	TERMINA LICENCIA MATERNIDAD 98 DIA	15/09/2017	16/12/2016	17-12-2016	

Fuente: aplicativo de Nomina

3. **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.**

3.1 Actividades control Interno

De acuerdo a las actividades en término de vencimiento a la fecha de la auditoría (octubre 2016), se identificaron 27 actividades así (**ver detalle anexo N°1**):

Estado	*Cantidad*
CUMPLIDAS	✓ *25*
NO CUMPLIDAS	✗ *2*
TOTAL	*27*

Las actividades no cumplidas tienen relación con:

- ✓ Seguridad física: puesta en operación del sistema de control de acceso biométrico.

✓ Revisión por la alta dirección al SGSI.

La actividad "Pruebas de usuario", para la funcionalidad de tratamiento de datos en los aplicativos, se cumplió el 22/11/2016 y el soporte fue anexado a la respuesta del informe preliminar mediante memorando No.20161300283973 del 15/12/2016.

3.2 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.

Las áreas de Tecnología de la Información y Planeación y Gestión de Riegos, emitieron respuesta mediante memorando N°20151300373941 del 21/12/2015, con los comentarios y plan de acción correspondiente.

Mediante memorando N°20161300159001 del 22/06/2016, las áreas responsables solicitaron modificación de plazos al plan de acción; por lo cual las actividades en término de vencimiento a corte octubre 2016, son:

ACTIVIDAD	*FECHA*	*ESTADO*	*COMENTARIO*
Relacionadas con el control de acceso físico	23/12/2016	En avance	Actividades alieneadas con el plan de acción de la auditoria SGSI 2015 de la Asesoría de control interno y el detalle se muestra en el anexo N°1 Es importante unificar el plan respecto a las actividades y fechas.
Generar mesas de trabajo con los lideres del área de Tecnologia de la información, para definición del procedimiento para la gestión de LOGS	30/08/2016	cumplida	Se confirma frente a FAP601 control de asistencia, en las siguientes fechas:10/12/2015, 18/02/2016, 13/01/2016
Radicar el formatao FDI310 solicitud de cambio a la documentación del SGC, en el que se solicite la creación del procedimiento para la gestión de logs al área de OYM	15/10/2016	cumplida	Se confirma con el área de Ornaginzación y Metodos, la radicación de solicitud N° 121683: 31/10/2016, para la creación del documento:PROCEDIMIENTO DE GESTION DE LOGS. Se estan adelantando mesas de trabajo para la aprobación.
Realizar un proceso de diagnostico interno relacionado con los temas de cifrado de datos acorde con los requerimientos de la ISO27002 y la forma de aplicación, que deba ser incluida dentro del modelo de desarrollo de sistemas de información de la Entidad.	31/10/2016	No cumplida	Actividad a desarrollar por el oficial de Seguridad de la Información, que desde mayo 2016 no se contaba con este rol. El 09/12/2016 se genero el contrato N°20161701 , fecha posterior al vencimiento de la actividad.

Se identifican actividades próximas a vencer relacionadas con:

- ✓ Cifrado de información.
- ✓ Aprobación del documento: procedimiento gestión de LOGS.
- ✓ Actualización manual MAP804 *Manual de gestión de seguridad de la información.*

A la fecha de conclusión de la auditoria (noviembre 2016) no hay planes de mejoramiento con la Contraloría General de la Republica, referentes al Sistema de Gestión de Seguridad de la Información-SGSI.

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

4.1 Conformidades

- En las etapas de planificación, implementación, evaluación del desempeño y mejora continua, se cuenta con ítems implementados, que a criterio de la auditoria permiten establecer que la Entidad se encuentra en un nivel de madurez "inicial" al 100%, "repetible" al 60% y "definido" al 55%.
- Procedimientos documentados, que describen los principales lineamientos en Seguridad de la información.
- Proceso de actualización de Activos de información y perfil de riesgo, de acuerdo a periodicidad definida.

4.2 No conformidades

- No se evidenciaron los informes de monitoreo a la seguridad de la información para el segundo semestre 2015 y primer semestre 2016, de acuerdo a lo descrito en el procedimiento PAP816 *Monitoreo a la gestión y al gobierno de la seguridad de la información institucional*, que menciona: *"El monitoreo a la Gestión y el Gobierno de la seguridad de la información Institucional se realizará con periodicidad semestral sobre las actividades ejecutadas en el semestre inmediatamente anterior…"*, por consiguiente no se cuenta con el insumo para : *"Con base en los resultados del monitoreo, las Áreas responsables de implementar sus controles, deben formular y formalizar los planes de tratamiento necesarios…"*, descrito en este mismo procedimiento.

- Según lo detallado en el punto 3 y anexo No.1 del presente informe, se evidencia incumplimientos en actividades de los planes de acción propuestos para atender auditorias de Control Interno y Revisoría Fiscal, referentes a:

  *Puesta en operación del control de acceso biométrico (reiterativo) que atiende el numeral *8.3.1-seguridad física* del manual MAP804"Manual de Gestión de Seguridad de la Información"; *Fortalecer el compromiso de la alta dirección con el Sistema, de acuerdo a lo descrito en el numeral *7.3.1 Revisión por la Dirección al SGSI* del manual MAP804; y *Diagnóstico de cifrado de la información (Revisoría Fiscal), en consecuencia las debilidades identificadas no han sido subsanadas.

Nota: Se recuerda que los incumplimientos en los planes de acción de las auditorías, se pueden trasladar a la secretaria de transparencia de acuerdo a la directiva 01 de 2015, establecida en el procedimiento PAU001 auditorías internas de control interno, numeral 5.5. "En caso de que se presente una presunta irregularidad administrativa, clasificado de acuerdo a la tipología de la Directiva 01 de 2015, se dará traslado a la Secretaria de Transparencia".

4.3 Observaciones

- Realizar y documentar el diagnóstico al Modelo de Seguridad y Privacidad de la información-MSPI, con el objetivo de establecer su estado actual y utilizar los resultados para proceder con los ajustes de la planificación y ejecución de etapas posteriores, así como estimar el tiempo y

recursos en el marco de las metas establecidas por el MINTIC, *numeral 12.1 Sujetos obligados del orden nacional* del MSPI V.3.0.2, que plantea para el componente de *Seguridad y Privacidad*, este implementado al 100% para el año 2018, y así evitar el incumplimiento.

- Actualizar y publicar el manual MAP804 *Manual de gestión de seguridad de la información*, para contar con los lineamientos en materia de seguridad y privacidad aplicables a la Entidad, teniendo en cuenta: el concepto de la asesoría jurídica descritos en el memorando N°20161100260323 del 11/11/2016, retroalimentación de las áreas a la revisión del documento preliminar, declaración de aplicabilidad de los controles (ISO 27002:2013), aspectos técnicos, roles y responsabilidades, plan de acción abierto con la Revisoría Fiscal; en razón a que este proceso se inició hace un año, según memorando N°20151300284323 del 17/11/2015. Evaluando la pertinencia de integrar las políticas, lineamientos y procedimientos de *privacidad y tratamiento de información personal*, que en la versión actual se describe en uno de sus anexos

- Adoptar lo referido por la Asesoría Jurídica en el memorando N°20161100260323 del 11/11/2016, respecto al tratamiento de datos personales, como también gestionar ante la alta dirección, la contratación para la consultoría "*Diagnóstico del estado actual de la Entidad en cuanto al cumplimiento de la Ley 1581/2012 y sus decretos reglamentarios (Aspectos jurídicos y técnicos)*", con el fin de evitar incumplimientos de los marcos normativos aplicables a la Entidad.

- Revisar el aplicativo de nómina y ajustarlo de considerarse necesario, para incluir el control de manejo de cuentas de usuarios, para las siguientes novedades: "Incapacidad/Licencia/Compensatorios/Comisiones" de acuerdo a lo descrito en el numeral 7.2 Anexo No. 2, del procedimiento PAP463, dado que no se confirmó su aplicación, en pruebas de funcionalidad realizadas con el usuario líder, para la evaluación del control "CTRGADM117-Gestión de usuarios", y así evitar el uso de cuentas de usuarios que no estén activos en la Entidad, con las implicaciones que esto conlleva.

4.4 Recomendaciones

- Se recomienda actualizar perfil de riesgo operativo, incluyendo riesgos relacionados con la protección de datos personales, en aspectos operativos y financieros, debido a que el riesgo **RGRIE18**, hace referencia exclusivamente al impacto reputacional.

Nota1: Para la generación del presente informe se consideró lo expuesto en la mesa de trabajo del día 15/12/2016 y el memorando No.20161300283973 del 15/12/2016 y sus anexos, como respuesta al informe preliminar.

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

ANEXO N°1

Descripción del Hallazgo	Responsable	Actividades	Estado de la actividad	Fecha limite	comentario
Implementar mecanismos técnicos para el monitoreo de la seguridad física y detección de intrusos como Circuito Cerrado de Televisión, y la conservación de los registros de monitoreo correspondientes, por lo menos para las áreas seguras dado que en visita de recorrido no se identifica este control para las áreas de Pagaduría y Negociación de inversiones, lo cual pone en riesgo los activos de la información que allí se manejan, como lo consigna el manual MAP804 "Manual de Gestión de Seguridad de la Información",, en su numeral 8.3.1-seguridad física.	Gerente Área de Servicios Administrativos	Realizar recorridos por los pisos de FONADE con los proveedores de controles de Acceso, para determinar especificaciones y/o características de los servicios a contratar.	cumplida	15/11/2015	Cumplida a octubre 2015. Se dio cumplimiento a la actividad con dos proveedores SECURITYGLOBAL y SOFTWAREONE. La propuesta seria para los pisos: 2,19,21,22,25,26,27,28,29,30 en los pisos 22 y 30 hay doble puerta de acceso principal(las de vidrio de los ascensores)
Implementar mecanismos técnicos para el monitoreo de la seguridad física y detección de intrusos como Circuito Cerrado de Televisión, y la conservación de los registros de monitoreo correspondientes, por lo menos para las áreas seguras dado que en visita de recorrido no se identifica este control para las áreas de Pagaduría y Negociación de inversiones, lo cual pone en riesgo los activos de la información que allí se manejan, como lo consigna el manual MAP804 "Manual de Gestión de Seguridad de la Información",, en su numeral 8.3.1-seguridad física.	Gerente Área de Servicios Administrativos	Elaborar el documento de solicitud de estudio previo y de mercado para la instalación y puesta en operación del sistema de control de acceso	cumplida	20/05/2016	Memorando 20164300134783
Implementar mecanismos técnicos para el monitoreo de la seguridad física y detección de intrusos como Circuito Cerrado de Televisión, y la conservación de los registros de monitoreo correspondientes, por lo menos para las áreas seguras dado que en visita de recorrido no se identifica este control para las áreas de Pagaduría y Negociación de inversiones, lo cual pone en riesgo los activos de la información que allí se manejan, como lo consigna el manual MAP804 "Manual de Gestión de Seguridad de la Información",, en su numeral 8.3.1-seguridad física.	Gerente Área de Servicios Administrativos	Realizar solicitud de CDP acorde con el POE , resultado del estudio previo y estudio de mercado	cumplida	30/06/2016	Se remiten los CDP 3800, 3801 y 3802 cuyo objeto es: Adquisición de un sistema de control de acceso biométrico para FONADE, incluyendo el diseño, la implementación, las adecuaciones locativas, el soporte y mantenimiento del mismo; con fecha de expedición 28 de octubre de 2016.
Implementar mecanismos técnicos para el monitoreo de la seguridad física y detección de intrusos como Circuito Cerrado de Televisión, y la conservación de los registros de monitoreo correspondientes, por lo menos para las áreas seguras dado que en visita de recorrido no se identifica este control para las áreas de Pagaduría y Negociación de inversiones, lo cual pone en riesgo los activos de la información que allí se manejan, como lo consigna el manual MAP804 "Manual de Gestión de Seguridad de la Información",, en su numeral 8.3.1-seguridad física.	Gerente Área de Servicios Administrativos	4. Solicitar la apertura del proceso para la selección del contratista que ejecutará la instalación y puesta en operación del sistema de control de accesos biométrico.	cumplida	08/07/2016	Se evidencia memorando No 20164300251053 del 31 de octubre de 2016 donde el Gerente del Área de Servicios Administrativos solicita al Gerente del Área de Gestión Contractual se de apertura al proceso para la contratación: Adquisición de un sistema de control de acceso biométrico ... Adjunto al memorando se envían los CDP que respaldan el proceso

Implementar mecanismos técnicos para el monitoreo de la seguridad física y detección de intrusos como Circuito Cerrado de Televisión, y la conservación de los registros de monitoreo correspondientes, por lo menos para las áreas seguras dado que en visita de recorrido no se identifica este control para las áreas de Pagaduría y Negociación de inversiones, lo cual pone en riesgo los activos de la información que allí se manejan, como lo consigna el manual MAP804 "Manual de Gestión de Seguridad de la Información",, en su numeral 8.3.1-seguridad física.	Gerente Área de Servicios Administrativos	Gestionar el proceso de selección para elección del contratista que ejecutará la instalación y puesta en operación del sistema de Control de Acceso.	cumplida	10/08/2016	Se remiten los documentos: Reglas de participación y Acta de apertura, del proceso de contratación del Sistema de Control de Acceso Biométrico, el cual se identifica como: Proceso de Convocatoria Simplificada CSI 016-2016.
Implementar mecanismos técnicos para el monitoreo de la seguridad física y detección de intrusos como Circuito Cerrado de Televisión, y la conservación de los registros de monitoreo correspondientes, por lo menos para las áreas seguras dado que en visita de recorrido no se identifica este control para las áreas de Pagaduría y Negociación de inversiones, lo cual pone en riesgo los activos de la información que allí se manejan, como lo consigna el manual MAP804 "Manual de Gestión de Seguridad de la Información",, en su numeral 8.3.1-seguridad física.	Gerente Área de Servicios Administrativos	Realizar la supervisión del contrato para la instalación y puesta en operación del sistema de control de acceso.	no cumplida	01/09/2016	Respecto a la actividad anterior y dando continuidad al proceso, el día 09 de diciembre 2016 el comité evaluador recomienda al ordenador del gasto o su delegado de FONADE, aceptar la oferta presentada por el oferente SAUTH LTDA. Sin embargo, la actividad hace referencia a la puesta en operación en la fecha propuesta, sin solicitud a la Asesoría de C. I de modificación de la misma.
Aunque se evidencian programas de sensibilización y capacitación en temas relacionados con Seguridad de la Información, se considera necesario reforzarlos enfocados a: dar a conocer la política de seguridad de la entidad, identificar y reportar eventos y/o incidentes, generar back up periódicamente a información de la estación de trabajo, y funcionalidades de la herramienta Office 365, siendo estos los puntos detecta-dos en el desarrollo de la Auditoria a fortalecer con los colaboradores, dado que se identificó que el 53% de los eventos de riesgo están relacionados con el error humano en el manejo de la información y/o documentación (informe de monitoreo segundo semestre 2014).	Gerente Área de Planeación y Gestión de Riesgos - Gerente Área de Tecnología de la Información - Oficial de Seguridad de la Información y Oficial de Seguridad Informática	Ejecutar las actividades de sensibilización de los tópicos identificados	cumplida	30/06/2016	Cumplida seguimiento junio 2016 Sensibilización mediante boletines por correo electrónico y cartelera virtual de los siguientes temas: contraseña segura-19/11/2015; Siete pasos para tener una computadora segura-17/12/2015; como protegerse de las estafas-28/12/2015; Puedes ser víctima del "Phishing" 22/02/2016;¿Cómo colocar contraseñas fáciles de recordar y difíciles de adivinar?-29/02/2016; La importancia del respaldo de la información-07/03/2016; La importancia de los escritorios limpios en FONADE -15/03/2016; Tú también puedes ser víctima del "Phishing"-25/05/2016;
Aunque se evidencian avances en la gestión para cumplimiento a la actividad "Implementar medidas de salud ocupacional en coordinación con el área de Talento Humano", formulada para atender hallazgo de la auditoria 2012 con fecha limite 31/12/2013, aun no se han implementado los elementos que brinden a los colaboradores condiciones ergonómicas apropiadas para el desempeño de sus funciones, por tanto están expuestos a desarrollar enfermedades laborales, relacionadas con trastornos musculo esqueléticos.	Área de Talento Humano	Solicitar el estudio previo de la contratación directa para la compra de los pad mouse para los funcionarios de la Entidad.	cumplida	31/12/2015	Cumplida seguimiento febrero 2016 mediante memorando 20154400306643 del 15/12/2015 :"SOLICITUD DE ESTUDIOS DE MERCADO Y ESTUDIOS PREVIOS PARA CONTRATAR ELEMENTOS DE CONFORT POSTURAL "
Aunque se evidencian avances en la gestión para cumplimiento a la actividad "Implementar medidas de salud ocupacional en coordinación con el área de Talento Humano", formulada para atender hallazgo de la auditoria 2012 con fecha limite 31/12/2013, aun no se han implementado los elementos que brinden a los colaboradores condiciones ergonómicas apropiadas para el desempeño de sus funciones, por tanto están expuestos a desarrollar enfermedades laborales, relacionadas con trastornos musculo esqueléticos.	Área de Talento Humano	Gestionar la Realizar el proceso de contratación directa, de acuerdo con lo establecido en el Manual de Contratación de la Entidad.	cumplida	30/04/2016	Cumplida seguimiento junio 2016 Se celebró el contrato No. 2016722 el 13/04/2016. Para adquirir 70 apoya muñecas-mouse y 70 descansa pie ajustable.

Aunque se evidencian avances en la gestión para cumplimiento a la actividad "Implementar medidas de salud ocupacional en coordinación con el área de Talento Humano", formulada para atender hallazgo de la auditoria 2012 con fecha limite 31/12/2013, aun no se han implementado los elementos que brinden a los colaboradores condiciones ergonómicas apropiadas para el desempeño de sus funciones, por tanto están expuestos a desarrollar enfermedades laborales, relacionadas con trastornos musculo esqueléticos.	Área de Talento Humano	Realizar la entrega del pad mouse, con las respectivas indicaciones de uso, a cada uno de los funcionarios de la Entidad. Se solicita ampliar plazo mediante memorando 20164400056603	cumplida	30/04/2016	Cumplida seguimiento junio 2016 Se celebró el contrato No. 2016722 el 13/04/2016. Para adquirir 70 apoya muñecas-mouse y 70 descansa pie ajustable. Se confirma la entrega con funcionarios y asistencia a charla de uso y cuidado de estos elementos, de acuerdo lista de asistencia del 06/05/2016.
Reformular y formalizar el plan de trabajo planteado para incluir la funcionalidad de aviso de privacidad en los aplicativos restantes, según memorando 20154100260263 del 10 de octubre del 2015 emitido por la Gerencia de TI, donde se planteó la primera actividad para el 20 de octubre del 2015, sin confirmar su ejecución, por tanto se puede incurrir el incumplimiento de la normatividad aplicable y las consecuencias que esto conlleva.	Área de Planeación y Gestión de Riesgos y Área de Tecnología de la Información	Identificación de los sistemas información para incluir la funcionalidad aviso de privacidad.	cumplida	15/02/2016	cumplida febrero 2016 Mail con listado de aplicaciones y componentes a incluir: PQR ORFEO- Certificaciones ORFEO; (PSE) Pago de Facturación con cargo a Convenios de la Subgerencia Técnica- Pago de Derechos de Participación- Pago de Certificaciones de Contratación Técnica Derivada- Pago de Otros Conceptos;(SARLAFT)Formulario de vinculación a clientes;(TH) encuestas;(Portal Web)ADUnlockUser- Certificados de Retenciones-Registro Contratistas- SMS Desembolsos
Reformular y formalizar el plan de trabajo planteado para incluir la funcionalidad de aviso de privacidad en los aplicativos restantes, según memorando 20154100260263 del 10 de octubre del 2015 emitido por la Gerencia de TI, donde se planteó la primera actividad para el 20 de octubre del 2015, sin confirmar su ejecución, por tanto se puede incurrir el incumplimiento de la normatividad aplicable y las consecuencias que esto conlleva.	Área de Planeación y Gestión de Riesgos y Área de Tecnología de la Información	Notificación mediante memorando a las áreas dueñas de las aplicaciones informándole sobre las modificaciones en los sistemas de información basado en los requerimientos legales de la ley 1581	cumplida	29/02/2016	Cumplida seguimiento febrero 2016 Memorando No.20161300056573 a para Gerentes: TI, SA, PAGADURIA, CONTABILIDAD y TALENTO HUMANO, con asunto "Notificación de ajustes al aviso de privacidad, para el ingreso a las aplicaciones de FONADE". Se envió por correo electrónico el 08/03/2016.
Reformular y formalizar el plan de trabajo planteado para incluir la funcionalidad de aviso de privacidad en los aplicativos restantes, según memorando 20154100260263 del 10 de octubre del 2015 emitido por la Gerencia de TI, donde se planteó la primera actividad para el 20 de octubre del 2015, sin confirmar su ejecución, por tanto se puede incurrir el incumplimiento de la normatividad aplicable y las consecuencias que esto conlleva.	Área de Planeación y Gestión de Riesgos y Área Responsable	Radicación solicitud FAP 094 " Solicitud de adquisición, desarrollo y puesta en producción de software"	cumplida	30/03/2016	Cumplida seguimiento junio 2016 Se realizó el 31/03/2016, mediante el formato FAP094 con consecutivo No.1520. De acuerdo al memorando 201613000565713 que lista los aplicativos a ajustar.
Reformular y formalizar el plan de trabajo planteado para incluir la funcionalidad de aviso de privacidad en los aplicativos restantes, según memorando 20154100260263 del 10 de octubre del 2015 emitido por la Gerencia de TI, donde se planteó la primera actividad para el 20 de octubre del 2015, sin confirmar su ejecución, por tanto se puede incurrir el incumplimiento de la normatividad aplicable y las consecuencias que esto conlleva.	Área de Planeación y Gestión de Riesgos, Área de Tecnología de la Información y Área responsable	Documento de análisis FAP 113 "Definición de requerimientos de software"	cumplida	30/05/2016	FAP113 del 14/07/2016 para el caso 1520. De acuerdo a lo descrito en el memorando 20161300056573 -29/02/2016
Reformular y formalizar el plan de trabajo planteado para incluir la funcionalidad de aviso de privacidad en los aplicativos restantes, según memorando 20154100260263 del 10 de octubre del 2015 emitido por la Gerencia de TI, donde se planteó la primera actividad para el 20 de octubre del 2015, sin confirmar su ejecución, por tanto se puede incurrir el incumplimiento de la normatividad aplicable y las consecuencias que esto conlleva.	Área de Tecnología de la Información	Diseño lógico y físico de la solución	cumplida	30/06/2016	Se confirma en sitio, en entrevista al coordinador de desarrollo y soporte de cumplimiento de la actividad "pruebas de calidad". Visita en sitio con el ingeniero de desarrollo encargado, donde se confirma la creación de la tabla ACEPTA TERMINOS, la cual en el formato FAP113 se había propuesto con el nombre:VC_CONFIRMACION_LEY_PDP

Reformular y formalizar el plan de trabajo planteado para incluir la funcionalidad de aviso de privacidad en los aplicativos restantes, según memorando 20154100260263 del 10 de octubre del 2015 emitido por la Gerencia de TI, donde se planteó la primera actividad para el 20 de octubre del 2015, sin confirmar su ejecución, por tanto se puede incurrir el incumplimiento de la normatividad aplicable y las consecuencias que esto conlleva.	Área de Tecnología de la Información	Desarrollo de la solicitud	cumplida	30/07/2016	De acuerdo lo definido en el formato FAP113 Definición de requerimientos de software. Visita en sitio con el ingeniero de desarrollo encargado, donde se observa el link para ambiente de pruebas.
Reformular y formalizar el plan de trabajo planteado para incluir la funcionalidad de aviso de privacidad en los aplicativos restantes, según memorando 20154100260263 del 10 de octubre del 2015 emitido por la Gerencia de TI, donde se planteó la primera actividad para el 20 de octubre del 2015, sin confirmar su ejecución, por tanto se puede incurrir el incumplimiento de la normatividad aplicable y las consecuencias que esto conlleva.	Área de Tecnología de la Información	Pruebas de Calidad	cumplida	30/09/2016	De acuerdo al formato FAP457 pruebas de calidad de software, con fecha 01/11/2016 con resultado del 100% para cada uno de los 3 atributos: funcionalidad, mantenibilidad y usabilidad. Caso No.1520
Reformular y formalizar el plan de trabajo planteado para incluir la funcionalidad de aviso de privacidad en los aplicativos restantes, según memorando 20154100260263 del 10 de octubre del 2015 emitido por la Gerencia de TI, donde se planteó la primera actividad para el 20 de octubre del 2015, sin confirmar su ejecución, por tanto se puede incurrir el incumplimiento de la normatividad aplicable y las consecuencias que esto conlleva.	Área de Planeación y Gestión de Riesgos, Área de Tecnología de la Información y Área responsable	Pruebas de Usuario	cumplida	15/10/2016	El día 03/11/2016, el área de TI envió correo a la gerente de PYGR, solicitando la asignación del usuario líder para realizar las pruebas de usuario para el caso No.1520. A la fecha del seguimiento 09/11/2016 no se han iniciado las pruebas de usuario. Se confirma el paso a producción el día 22/11/2016, frente a formato FAP094 para el caso No.1520, aportado como anexo de la respuesta al informe preliminar, mediante memorando No.20161300283973 15/12/2016 y mesa de trabajo de esta misma fecha.
Crear mecanismo para dar a conocer a todos los colaboradores la importancia de generar periódicamente el Back up de las estaciones de trabajo y revisar la disponibilidad del recurso para tal fin, dado que según sondeo realizado solo 3 de los 26 PC's revisados, contaban con un back up mínimo de 2 meses atrás; que aunque se está trabajando en la actualización de este procedimiento , alineado a la actividad No.5 *"Fortalecimiento en el esquema de backup del usuario final y actualización de la guía GAP 477 " Elaboración de backups en puestos de trabajo"* del plan de tratamiento de riesgos con fecha de ejecución 30/08/2015 al 30/08/2016, se considera urgente generar sensibilización al respecto, para evitar perdida de información de los usuarios finales.	Área de Tecnología de la Información	Realizar pieza de sensibilización para los colaboradores de la Entidad sobre el backup en puestos de trabajo.	cumplida	29/02/2016	cumplida seguimiento febrero 2016 Correo enviado por COMUNICACIONES, con el asunto :" La importancia del respaldo de la información - Área de Tecnología de la Información"
Revisar la sincronización de relojes de elementos de la infraestructura tecnológica en aplicación del control "***CTRGADM145**: Sincronización de Relojes de elementos de la infraestructura tecnológica"*, toda vez que se evidenciaron diferencias en equipos de la asesoría de control interno, lo cual no garantiza la exactitud de los registros de las transacciones que pueden ser necesarios para seguimientos, evidencias en casos legales o disciplinarios, así como la confiabilidad de la información.	Tecnología de la Información	Reunión con personal de la Superintendencia de Industria y Comercio SIC y el Instituto Nacional de Metrología INM.	Cumplida	30/03/2016	Cumplida seguimiento junio 2016 Se confirma que la gestión se realizó mediante comunicaciones por correo electrónico. Recibiendo respuesta: De: Silvia Adriana Garcia Panqueva [mailto:sagarcia@inm.gov.co] Enviado el: martes, 22 de diciembre de 2015 04:00 p.m. Para: Milton Jesus Vera Contreras <mvera@fonade.gov.co>

Revisar la sincronización de relojes de elementos de la infraestructura tecnológica en aplicación del control "***CTRGADM145**: Sincronización de Relojes de elementos de la infraestructura tecnológica",* toda vez que se evidenciaron diferencias en equipos de la asesoría de control interno, lo cual no garantiza la exactitud de los registros de las transacciones que pueden ser necesarios para seguimientos, evidencias en casos legales o disciplinarios, así como la confiabilidad de la información.	Tecnología de la Información	Realizar la configuración de sincronización de reloj con la asistencia de personal del Instituto Nacional de Metrología INM.	cumplida	30/04/2016	Cumplida seguimiento junio 2016 Se confirma frente a documento: Sincronización de relojes – Directorio Activo FONADE, V.1.0. Sin embargo según las consideraciones registradas en el documento, se presentan diferencias, que serán consultadas al INM, pese a que la actividad lo consideraba. Se continua seguimiento con la siguiente actividad "Verificación correcto funcionamiento" del mismo plan.
Revisar la sincronización de relojes de elementos de la infraestructura tecnológica en aplicación del control "***CTRGADM145**: Sincronización de Relojes de elementos de la infraestructura tecnológica",* toda vez que se evidenciaron diferencias en equipos de la asesoría de control interno, lo cual no garantiza la exactitud de los registros de las transacciones que pueden ser necesarios para seguimientos, evidencias en casos legales o disciplinarios, así como la confiabilidad de la información.	Tecnología de la Información	Verificación correcto funcionamiento	cumplida	30/05/2016	Se adelantaron las siguientes acciones: *Instalación de la herramienta Net Time en el servidor controlador de dominio principal Servidor: FONSRVMDC01. *Ejecución del comando w32tm /query /status: 31/10/2016: sincronización de hora correcta. *Se observa la hora en equipos que presentaban diferencias de 17 S, pasando dicha diferencia a 1S (lserrano - cgonzal1)-09/11/2016. Pruebas de observación y comparación de la hora del INM: http://horalegal.inm.gov.co/
Verificar el back up de la base de datos SEVINPRO, en cuanto a la generación de reportes, debido a que se confirmó que no los genera acorde a la información del back up restaurado, como se describe en el desarrollo del presente informe, lo cual afecta la confiabilidad y disponibilidad de la información de este aplicativo.	Tecnología de la Información	Instalación ambiente de pruebas de la versión Sevinpro 4 con sistema de reportes locales, suprimiendo el re porteador que utiliza JBOSS instalado en IAS_SERVER	cumplida	18/12/2015	Cumplida seguimiento febrero 2016 Se confirma solución en entrevista a usuario HRUIZ, con quien se había identificado el problema en la ejecución de la auditoria.
Verificar el back up de la base de datos SEVINPRO, en cuanto a la generación de reportes, debido a que se confirmó que no los genera acorde a la información del back up restaurado, como se describe en el desarrollo del presente informe, lo cual afecta la confiabilidad y disponibilidad de la información de este aplicativo.	Tecnología de la Información	Pruebas de funcionamiento por parte de los usuarios que intervienen en el ciclo de información de la herramienta (Inversiones, pagaduría y Planeación)	cumplida	22/12/2015	Cumplida seguimiento febrero 2016 Se confirma solución en entrevista a usuario HRUIZ, con quien se había identificado el problema en la ejecución de la auditoria.
Verificar el back up de la base de datos SEVINPRO, en cuanto a la generación de reportes, debido a que se confirmó que no los genera acorde a la información del back up restaurado, como se describe en el desarrollo del presente informe, lo cual afecta la confiabilidad y disponibilidad de la información de este aplicativo.	Tecnología de la Información	Instalación de la versión en ambiente productivo	cumplida	07/01/2016	Cumplida seguimiento febrero 2016 Se confirma solución en entrevista a usuario HRUIZ, con quien se había identificado el problema en la ejecución de la auditoria.
Fortalecer el Compromiso de la alta dirección, con la implementación y mejora continua del SGSI, que aunque ya se realizó la primera revisión, no se identificaron decisiones relacionadas con las oportunidades de mejora, necesidades de cambio en el sistema o asignación de recursos.	Planeación y Gestión de Riesgos	Proceso de sensibilización a la alta dirección en cuanto a la responsabilidad del mismo en el SGSI	cumplida	30/04/2016	cumplida seguimiento junio 2016 La Gerente de Organización y Métodos, encargada de las obligaciones del Área de Planeación y Gestión de Riesgos realizó presentación al Comité de Gerencia, sobre el Compromiso de la Alta Dirección en el SGSI en sesiones de abril y mayo de 2016. Acta comité de gerencia No536 del 18/04/2016 (punto3) y No.537 del 02/05/2016 (desarrollo punto 1)

Fortalecer el Compromiso de la alta dirección, con la implementación y mejora continua del SGSI, que aunque ya se realizó la primera revisión, no se identificaron decisiones relacionadas con las oportunidades de mejora, necesidades de cambio en el sistema o asignación de recursos.	Planeación y Gestión de Riesgos	Ejecución de la revisión por dirección del SGSI.	no cumplida	31/08/2016	La actividad propuesta no se ha ejecutado. Se han realizado gestiones como: dar a conocer a la alta dirección el compromiso frente al SGSI. Así como la solicitud del área de PYGR al área de OYM, para incluir ajustes relacionados con la revisión al SGSI, al procedimiento PDI305 Revisión por la Dirección del Sistema de Gestión de Calidad - SGC; El procedimiento fue actualizado el 01 de julio/2016, en el cual no se identifica la inclusión de la revisión por la dirección del SGSI