PLAN DE MEJORAMIENTO

No. Plan: PM-20-00014 **Fecha plan:** 2020-06-08 11:57:29 AM

IDENTIFICACIÓN PROCESO/DEPENDENCIA

Fuente del hallazgo: Revisión por la dirección

Tipo de plan: Proceso

Proceso: Direccionamiento Estratégico **Responsable:** CELMIRA FRASSER ACEVEDO **Cargo:** Jefe Oficina Asesora

ANÁLISIS DE CAUSAS Y FORMULACIÓN PLAN DE MEJORAMIENTO

Tipo de hallazgo: No conformidad **Metodología:** 5 Por ques? **Anexo análisis-causa:**

Hallazgo: H1: Hallazgo Transversal Auditoria Oficina Tecnologías de la Información AU-1926. La Agencia no cumple con los requisitos de la Norma ISO 27001: 2013 – SGSI abajo descritos, tal y como se evidenció en la revisión de la implementación de dicha norma en la evaluación que se realizó al Proceso de Gestión de Tecnología de la Información (resultado presentado en el informe de auditoría). Los numerales de la norma que se incumplen son los siguientes, a saber: 6.1.2 Valoración de riesgos de Seguridad de la Información; 6.1.3 Tratamiento de riesgos de Seguridad de la Información; 8.2 VALORACIÓN DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN; 8.3 TRATAMIENTO DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN.

Nro	CAUSA	ACCIÓN	
1	En cuanto a la Valoración y el Tratamiento de riesgos de la Seguridad de la Información, no se cuenta con lineamientos que cumplan totalmente los requisitos especificados en la Norma ISO 27001:2013, en términos de valoración y tratamiento de riesgos de seguridad.	AC1: Apoyar en la actualización del Manual de Gestión de Riesgos Institucional, dando los aportes técnicos en la identificación, valoración y tratamiento de los riesgos de Seguridad de la Información, de acuerdo con lo exigido por la norma ISO 27001:2013. Producto: Acta de reunión con los lineamientos de valorización y tratamiento de riesgos de Seguridad de la Información.	**Tipo de acción:** Correctiva **Fecha:** 2020-07-01 (Inicio) 2020-09-30 (Fin) **Responsable:** LUZ MARCELA RAMIREZ VELEZ

Nro	CAUSA	ACCIÓN	
2	En cuanto a la Valoración y el Tratamiento de riesgos de la Seguridad de la Información, no se cuenta con lineamientos que cumplan totalmente los requisitos especificados en la Norma ISO 27001:2013, en términos de valoración y tratamiento de riesgos de seguridad.	AC2: Apoyar en la actualización del Manual de Gestión de Riesgos Institucional, dando los aportes técnicos en la identificación, valoración y tratamiento de los riesgos de Seguridad de la Información, de acuerdo con lo exigido por la norma ISO 27001:2013. Producto: Acta de reunión con los lineamientos de valorización y tratamiento de riesgos de Seguridad de la Información.	**Tipo de acción:** Correctiva **Fecha:** 2020-07-01 (Inicio) 2020-09-30 (Fin) **Responsable:** CELMIRA FRASSER ACEVEDO

"TODA IMPRESIÓN FÍSICA DE ESTE DOCUMENTO SE CONSIDERA DOCUMENTO NO CONTROLADO"

PLAN DE MEJORAMIENTO

No. Plan: PM-20-00014 **Fecha plan:** 2020-06-08 11:57:29 AM

Nro	CAUSA	ACCIÓN	
3	En cuanto a la Valoración y el Tratamiento de riesgos de la Seguridad de la Información, no se cuenta con lineamientos que cumplan totalmente los requisitos especificados en la Norma ISO 27001:2013, en términos de valoración y tratamiento de riesgos de seguridad.	AC3: Apoyar en la actualización del Manual de Gestión de Riesgos Institucional, dando los aportes técnicos en la identificación, valoración y tratamiento de los riesgos de Seguridad de la Información, de acuerdo con lo exigido por la norma ISO 27001:2013. Producto: Acta de reunión con los lineamientos de valorización y tratamiento de riesgos de Seguridad de la Información.	**Tipo de acción:** Correctiva **Fecha:** 2020-07-01 (Inicio) 2020-09-30 (Fin) **Responsable:** EDUARDO ANTONIO SANGUINETTI ROMERO

Tipo de hallazgo: No conformidad **Metodología:** 5 Por ques? **Anexo análisis-causa:**

Hallazgo: H2: Hallazgo Transversal Auditoria Oficina Tecnologías de la Información AU-1926. La Agencia no cumple con los requisitos de la Norma ISO 27001: 2013 – SGSI abajo descritos, tal y como se evidenció en la revisión de la implementación de dicha norma en la evaluación que se realizó al Proceso de Gestión de Tecnología de la Información (resultado presentado en el informe de auditoría). Los numerales de la norma que se incumplen son los siguientes, a saber: 6.1.1 Generalidades y 7.5.1 Generalidades.

Nro	CAUSA	ACCIÓN	
1	Respecto de las Generalidades a las que hace referencia el numeral 6.1.1. y 7.5.1, la política de riesgos de la Entidad no cuenta con un instrumento o lineamientos definidos para la evaluación de la eficacia de las acciones.	AC1: Actualizar el Manual de Gestión de Riesgos institucional, determinando y especificando los lineamientos para la evaluación de la eficacia de las acciones de los riesgos de la Entidad. Producto: Acta de reunión con los lineamientos para la evaluación de eficacia de las acciones de riesgo.	**Tipo de acción:** Correctiva **Fecha:** 2020-07-01 (Inicio) 2020-09-30 (Fin) **Responsable:** CELMIRA FRASSER ACEVEDO

Nro	CAUSA	ACCIÓN	
2	Respecto de las Generalidades a las que hace referencia el numeral 6.1.1. y 7.5.1, la política de riesgos de la Entidad no cuenta con un instrumento o lineamientos definidos para la evaluación de la eficacia de las acciones.	AC2: Apoyar la actualización del Manual de Gestión de Riesgos institucional, determinando y especificando los lineamientos para la evaluación de la eficacia de las acciones de los riesgos de la Entidad. Producto: Acta de reunión con lineamientos para la evaluación de eficacia de las acciones de riesgo.	**Tipo de acción:** Correctiva **Fecha:** 2020-05-26 (Inicio) 2020-09-30 (Fin) **Responsable:** EDUARDO ANTONIO SANGUINETTI ROMERO

Nro	CAUSA	ACCIÓN
3	Respecto de las Generalidades a las que hace referencia el	AC3: Gestionar la aprobación del Manual de Gestión de Riesgos

"TODA IMPRESIÓN FÍSICA DE ESTE DOCUMENTO SE CONSIDERA DOCUMENTO NO CONTROLADO"

PLAN DE MEJORAMIENTO

No. Plan: PM-20-00014 **Fecha plan:** 2020-06-08 11:57:29 AM

	numeral 6.1.1. y 7.5.1, la política de riesgos de la Entidad no cuenta con un instrumento o lineamientos definidos para la evaluación de la eficacia de las acciones.	actualizado con los lineamientos para valoración y tratamiento de riesgos de Seguridad de la información y lineamientos para la evaluación de la eficacia, que debe ser presentado en la Mesa de seguridad, y posteriormente en el Comité Institucional de Gestión y Desempeño y el Comité de Coordinación de Control Interno. Producto: Actas de Comité	**Tipo de acción:** Correctiva **Fecha:** 2020-10-01 (Inicio) 2020-10-30 (Fin) **Responsable:** CELMIRA FRASSER ACEVEDO

Nro	CAUSA	ACCIÓN	
4	Respecto de las Generalidades a las que hace referencia el numeral 6.1.1. y 7.5.1, la política de riesgos de la Entidad no cuenta con un instrumento o lineamientos definidos para la evaluación de la eficacia de las acciones.	AC4: Realizar acciones de socialización de la actualización de la política de gestión de riesgos, enmarcada en el Manual de Gestión de Riesgos. Producto: Evidencias de socialización	**Tipo de acción:** Correctiva **Fecha:** 2020-11-02 (Inicio) 2020-11-30 (Fin) **Responsable:** CELMIRA FRASSER ACEVEDO

Tipo de hallazgo: No conformidad **Metodología:** 5 Por ques? **Anexo análisis-causa:**

Hallazgo: H3: Hallazgo Transversal Auditoria Oficina Tecnologías de la Información AU-1926. La Agencia no cumple con los requisitos de la Norma ISO 27001: 2013 – SGSI abajo descritos, tal y como se evidenció en la revisión de la implementación de dicha norma en la evaluación que se realizó al Proceso de Gestión de Tecnología de la Información (resultado presentado en el informe de auditoría). Los numerales de la norma que se incumplen son los siguientes, a saber: 7.2 COMPETENCIA, 9.3 REVISIÓN POR LA DIRECCIÓN y 10.1 NO CONFORMIDADES Y ACCIONES CORRECTIVAS de la norma NTC ISO 27001:2013.

Nro	CAUSA	ACCIÓN	
1	Respecto del numeral 7.2 de la norma ISO 27001: Competencia, la Entidad cuenta con un Oficial de Seguridad designado y aprobado por el Director General, sin embargo no se han tenido en cuenta la totalidad de competencias, con las que debe cumplir el servidor de la Entidad, que realice las funciones correspondientes al rol de Oficial de Seguridad.	AC1: Adelantar sesión de la Mesa de Seguridad, en la que se deben presentar las competencias con las que debe cumplir el servidor designado por el Director General para cumplir el rol de Oficial de Seguridad y definir terna de posibles servidores de la ARN aspirantes a Oficial de Seguridad que cumplen las competencias. Producto: Acta de reunión	**Tipo de acción:** Correctiva **Fecha:** 2020-06-01 (Inicio) 2020-07-30 (Fin) **Responsable:** LUZ MARCELA RAMIREZ VELEZ

Nro	CAUSA	ACCIÓN
2	Respecto del numeral 7.2 de la norma ISO 27001:	AC2: Presentar en sesión del Comité Institucional de Gestión y

"TODA IMPRESIÓN FÍSICA DE ESTE DOCUMENTO SE CONSIDERA DOCUMENTO NO CONTROLADO"

PLAN DE MEJORAMIENTO

No. Plan: PM-20-00014 **Fecha plan:** 2020-06-08 11:57:29 AM

	Competencia, la Entidad cuenta con un Oficial de Seguridad designado y aprobado por el Director General, sin embargo no se han tenido en cuenta la totalidad de competencias, con las que debe cumplir el servidor de la Entidad, que realice las funciones correspondientes al rol de Oficial de Seguridad.	Desempeño la terna de posibles servidores de la ARN aspirantes a Oficial de Seguridad que cumplen las competencias, esto con el fin que en marco del Comité se defina el aspirante a presentarle al Director General para su designación oficial. Producto: Acta de comité	**Tipo de acción:** Correctiva **Fecha:** 2020-08-03 (Inicio) 2020-08-31 (Fin) **Responsable:** CELMIRA FRASSER ACEVEDO

Tipo de hallazgo: No conformidad **Metodología:** 5 Por ques? **Anexo análisis-causa:**

Hallazgo: H4: Hallazgo Transversal Auditoria Oficina Tecnologías de la Información AU-1926. La Agencia no cumple con los requisitos de la Norma ISO 27001: 2013 – SGSI abajo descritos, tal y como se evidenció en la revisión de la implementación de dicha norma en la evaluación que se realizó al Proceso de Gestión de Tecnología de la Información (resultado presentado en el informe de auditoría). Los numerales de la norma que se incumplen son los siguientes, a saber:s; 7.5.2 Creación y actualización.

Nro	CAUSA	ACCIÓN	
1	Respecto del punto 7.5.2 Creación y actualización, se debe a que existen documentos relacionados con el Sistema de Seguridad de la Información que no están formalizados y no hacen parte del Sistema de Gestión y no se encuentran aprobados ni cargados en el Software para la Administración de la Planeación y Gestión - SIGER.	AC1: Seleccionar, definir y coordinar con la OAP, estableciendo la documentación que debe estar en el Software para la Administración de la planeación y la Gestión que harían parte del Sistema de Gestión Integral sobre la documentación de la OTI de Sistema de Gestión de Seguridad de la Información Producto: Documentos aprobados y publicados en SIGER	**Tipo de acción:** Correctiva **Fecha:** 2020-07-01 (Inicio) 2020-12-31 (Fin) **Responsable:** LUZ MARCELA RAMIREZ VELEZ

Anexos:

ACTAS ASOCIADAS

Número(s) de acta:

Elaborado por: FABIAN ANDRES PORTILLO SALAZAR

"TODA IMPRESIÓN FÍSICA DE ESTE DOCUMENTO SE CONSIDERA DOCUMENTO NO CONTROLADO"