INFORME SEGUIMIENTO AL PLAN DE MEJORAMIENTO DE LA AUDITORÍA AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI

OFICINA DE CONTROL INTERNO

UNIDAD DE SERVICIOS PENITENCIARIOS Y CARCELARIOS – USPEC

Bogotá D.C., marzo de 2021

1. OBJETIVO

Realizar seguimiento al Plan de Mejoramiento de la Auditoría al Sistema de Gestión de Seguridad de la Información - SGSI de la Unidad de Servicios Penitenciarios y Carcelarios – USPEC, en el periodo comprendido entre julio de 2020 y diciembre de 2020.

2. ALCANCE

Verificar mediante el presente seguimiento las mejoras realizadas al cumplimiento de las funciones de la Oficina de Tecnología en el Sistema de Gestión de Seguridad de la Información - SGSI.

3. NORMATIVIDAD

Artículo 209 y 269 de la Constitución Nacional; Decreto 1069 de 2015; Ley 87 de 1993; Decreto No. 4150 de 2011 y demás normas concordantes y complementarias.

4. METODOLOGÍA

Se tendrán en cuenta las observaciones y recomendaciones descritas en el informe de auditoría, por el equipo auditor a la Oficina de Tecnología. Se solicitará evidencias de los avances realizados por la OTEC tendientes a la mitigación de los hallazgos, se realizaran mesas de trabajo con la Oficina de Tecnología para el estudio de los hallazgos y las actividades realizadas para mitigarlos.

5. DESARROLLO DEL SEGUIMIENTO

Mediante comunicación telefónica y correo electrónico el 26 de febrero de 2021, a la Oficina de Tecnología se solicitó avances realizados para mitigar los hallazgos de la Auditoría al Sistema de Gestión de Seguridad de la Información – SGSI, que se realizó en la vigencia 2019, posteriormente, el día 9 de marzo de 2021 la Oficina de Control Interno mediante correo electrónico dio respuesta a la solicitud mediante memorando I-2021-001034 asunto avances auditoria vigencia 2019.

Se solicitó información a la Oficina de Tecnología para verificar información relacionada con los siguientes hallazgos:

1. No se evidencia el cumplimiento del Plan de tratamiento de riesgos de seguridad de información
2. No se evidencia apropiada gestión de cuentas de usuario de los aplicativos Humano, INFODOC y Tienda Virtual.
3. No se evidencia el conocimiento de políticas, procedimientos, roles y responsabilidades y demás lineamientos de seguridad de información por parte de todo el personal de la Entidad.
4. No se evidencia la definición de un plan de comunicación y sensibilización en seguridad de la información.
5. No se evidencia el etiquetado de información

6. No se evidencian controles de seguridad física que permitan prevenir el acceso físico no autorizado, el daño y la interferencia de información, así como la identificación de zonas seguras y sus respectivos controles físicos.
7. No se evidencia el cumplimiento de todas las acciones definidas en los planes de mejoramiento producto de las Auditorías internas de seguridad de información.
8. No se evidencia el cumplimiento de las políticas y procedimientos de seguridad de información documentados, realizada en enero de 2019.
9. No se evidencia publicado el seguimiento a los procesos de contratación de la entidad en el portal del SECOP.
10. No se evidencia una evaluación de todos los incidentes de seguridad de información, ni una respuesta oportuna de acuerdo a procedimiento estableció por la Entidad.
11. No se evidencia la firma del acuerdo de confidencialidad de la información para todos los funcionarios de la Entidad.
12. No se cuenta con documento unificado donde establezcan los requisitos para seguir un proceso formal de adquisición y pruebas para la elaboración de los contratos y acuerdos con terceras partes donde se fije consideración a los requisitos de seguridad de la organización.

De acuerdo al seguimiento realizado por parte de la Oficina de Control Interno, en reunión la Oficina de Tecnología manifestó los siguientes avances de los hallazgos:

1. **No se evidencia el cumplimiento del Plan de tratamiento de riesgos de seguridad de información - PTR**

Respuesta Oficina de Tecnología:

"Los riesgos se actualizaron en el primer semestre del año 2020, Por parte de la OTEC se inició la ejecución del plan desde el primer trimestre del año, por parte de los demás procesos se inició la implementación en el segundo trimestre teniendo en cuenta las fechas de aprobación del PTR. La Oficina de Tecnología solicitó el avance del PTR, mediante correos electrónicos a las otras dependencias de la Entidad requirió información con el objetivo de hacer seguimiento, la OTEC manifiesta que la implementación del Plan de Tratamiento de Riesgos de Seguridad de la Información no depende de la OTEC, sino que esta se encuentra presta a apoyar a las aéreas para el cumplimiento, sin embargo, cada líder debe responder por las evidencias, dicha gestión está avalada por la Oficina Asesora de Planeación, donde consta que cada dependencia es responsable de la implementación la OTEC solo hace seguimiento, además de implementar en su misma área y aportar sus propias evidencias para su proceso como se especifica el Informe de seguimiento al Plan de Tratamiento de Riesgos Cuarto Trimestre de 2020. Evidencia No. 1".

Respuesta Oficina Control Interno:

La Oficina de Control Interno de acuerdo a los soportes allegados por la Oficina de Tecnología, evidenció que el Plan de Tratamiento de Riesgos fue actualizado con fecha 24 de diciembre de 2020 y publicado en la página web de la Entidad, lo cual evidencia el seguimiento realizado por a OTEC

para el cumplimiento del mismo por parte de todas las dependencias de la Entidad, por lo tanto, la actividad por parte de la Oficina de Tecnología es subsanada.

2. **No se evidencia apropiada gestión de cuentas de usuario de los aplicativos Humano, INFODOC y Tienda Virtual.**

Respuesta Oficina de Tecnología:

"La oficina de Tecnología actualizó el procedimiento de Gestión de acceso a usuario con el fin de minimizar los hallazgos. La gestión de las cuentas de usuario del aplicativo INFODOC se encuentra a cargo del Grupo de Gestión Documental, Tienda Virtual con el área de Contractual y Humano web con el área de administración de personal. El procedimiento actualizado y el formato de trazabilidad de cuentas de usuario se socializó mediante correo electrónico a los roles administradores de estas herramientas el día 29 de septiembre de 2020. Evidencia No. 2".

Respuesta Oficina Control Interno:

La Oficina de Control Interno de acuerdo a los soportes allegados por la Oficina de Tecnología, evidenció que el Procedimiento *Gestión de Acceso a Usuarios* fue actualizado con la versión 02 fecha 26 de junio de 2020, código A3-PR-08 y publicado en la página web de la Entidad, el procedimiento Gestión de Acceso a Usuarios, así como el formato A3-FO-49 Trazabilidad de cuentas de Usuarios fueron socializados mediante correo electrónico el día 29 de septiembre de 2020, sin embargo, aunque se evidencia que la OTEC adoptó medidas planteando *lineamientos para gestionar los diferentes usuarios, las responsabilidades de cada uno, y lineamientos para actualización y/o habilitación de las cuentas de usuarios, se continua sin la* apropiada gestión de cuentas de usuario de los aplicativos Humano, INFODOC y Tienda Virtual, por lo anterior el hallazgo no es subsanado.

3. **No se evidencia el conocimiento de políticas, procedimientos, roles y responsabilidades y demás lineamientos de seguridad de información por parte de todo el personal de la Entidad.**

Respuesta Oficina de Tecnología:

"La Oficina de Tecnología trabajó en la actualización de los documentos propios del SGSI, se actualizó la Política de Seguridad y Privacidad de la información mediante la Resolución No. 683 del 17 de diciembre de 2020 en la cual se definen las políticas, procedimientos, roles y responsabilidades y demás lineamientos frente al Sistema de Seguridad de información. Se realiza la socialización de la resolución a todos los funcionarios de la entidad mediante correo electrónico el día 4 de marzo de 2021. Evidencia No. 3".

Respuesta Oficina Control Interno:

La Oficina de Control Interno de acuerdo a los soportes allegados por la Oficina de Tecnología, evidenció que se dio cumplimiento a la actualización de la Política de Seguridad y Privacidad de la

información mediante la Resolución No. 683 del 17 de diciembre de 2020 en la cual se definen las políticas, procedimientos, roles y responsabilidades y demás lineamientos frente al Sistema de Seguridad de información, además, se realizó la socialización de la resolución a todos los funcionarios de la Entidad mediante correo electrónico el día 4 de marzo de 2021. Por lo anterior el hallazgo es subsanado.

4. **No se evidencia la definición de un plan de comunicación y sensibilización en seguridad de la información.**

Respuesta Oficina de Tecnología:

"La Oficina de Tecnología realizó el Plan de Comunicación y sensibilización en seguridad de la información el cual se encuentra publicado en la página web, el Plan fue elaborado con el aval de la Subdirección Administrativa y Financiera, Entre las actividades que contempla este plan se encuentran el envío de píldoras "Tips de Seguridad semanales", Usuario Seguro del mes "Se realiza un reconocimiento del o los funcionarios que reportan activamente posibles casos de ciberseguridad mediante correo electrónico y se realiza la socialización de Políticas, procedimientos del SGSI.
Evidencia No. 4".

Respuesta Oficina Control Interno:

La Oficina de Control Interno de acuerdo a los soportes allegados por la Oficina de Tecnología, evidenció que se encuentra definido el Plan de comunicación y sensibilización en seguridad de la información, por parte de la OTEC la versión del documento 01 de fecha 12 mayo de 2020, además, se está dando cumplimiento con el envío de píldoras "Tips de Seguridad semanales" por lo anterior el hallazgo es subsanado.

5. **No se evidencia el etiquetado de información.**

Respuesta Oficina de Tecnología:

"Con el fin de cumplir este objetivo fue necesario actualizar el Manual de Clasificación de Activos de la Información, para lo cual se realizaron mesas de trabajo en conjunto entre la Oficina de Tecnología, el Grupo de Gestión Documental y la Oficina Asesora Jurídica, conllevando a que su segunda versión fuese aprobada y publicada el pasado 28 de agosto de 2020.
Luego de la actualización del Manual de Clasificación de Activos, es necesario la actualización de las Tablas de Retención documental y el Índice de Información Clasificada y Reservada cuyo resultado se obtuvo de las mesas de trabajo que se han venido desarrollando desde el 3er trimestre del 2020 y aún se continúan realizando.
Luego de culminar la actualización Tablas de Retención Documental, es posible realizar el desarrollo del Índice de Información Clasificada y Reservada, con estos insumos se realiza el Etiquetado de la información quien es responsable es el Grupo de Gestión Documental además de establecer los lineamientos para orientar y sensibilizar a las diferentes dependencias para llevar a cabo el etiquetado

de información tanto física como digital El etiquetado de la información física se realiza a través del manejo del formato asignado para las carpetas A1-S6-FO-11 Identificación de Carpetas de Archivo y está a cargo del líder de proceso según la información registrada en sus inventarios de activos. Evidencia No. 5".

Respuesta Oficina Control Interno:

La Oficina de Control Interno de acuerdo a los soportes allegados por la Oficina de Tecnología, evidenció que se tomaron en cuenta las recomendaciones realizadas en el primer informe de seguimiento a la Auditoría, y que se encuentra gestionando lo respectivo que conlleve a la mitigación del hallazgo, sin embargo, se continua sin etiquetado de información por lo que no es subsanado.

6. **No se evidencian controles de seguridad física que permitan prevenir el acceso físico no autorizado, el daño y la interferencia de información, así como la identificación de zonas seguras y sus respectivos controles físicos.**

Respuesta Oficina de Tecnología:

"El Grupo administrativo de personal envía evidencias realizadas para las actividades que se han realizado en cuanto a los controles de seguridad física, entre ellos están la implementación de un Sistema Biométrico en el Grupo de Gestión documental. De igual manera se establece un responsable para el monitoreo del CCTV de la USPEC y la socialización de las circulares 0047 del 15 de diciembre de 2020 Asunto: Control de Servidores, contratistas y visitantes y Circular 0048 del 15 de diciembre de 2020 Asunto: Zonas seguras y circular Respuesta de administrativa. Evidencias No. 6"

Respuesta Oficina Control Interno:

La Oficina de Control Interno de acuerdo a los soportes allegados por la Oficina de Tecnología, evidenció las actividades realizadas con respecto a los controles de seguridad física que permitan prevenir el acceso físico no autorizado, el daño y la interferencia de información, así como la identificación de zonas seguras y sus respectivos controles físicos, por lo tanto, el hallazgo es subsanado.

7. **No se evidencia el cumplimiento de todas las acciones definidas en los planes de mejoramiento producto de las Auditorías internas de seguridad de información.**

Respuesta Oficina de Tecnología*:*

"El Informe presentado a la Dirección General sobre el Sistema de Gestión de Seguridad de la Información en el segundo semestre de 2020, se incluyen las actividades ejecutadas entre 01 de julio de 2020 hasta el 22 de diciembre de 2020 de las No conformidades y acciones correctivas (Avances del plan de mejoramiento auditoria SGSI)

En resumen, se evidenciaron doce (12) no conformidades, las cuales se derivan de la auditoría interna

de seguridad de información realizada en octubre de 2019. Con corte a la fecha de presentación de este informe, se han ejecutado acciones para subsanar ocho (8) no conformidades las cuales aún se encuentran en proceso, dos (2) no conformidades se ejecutaron en su totalidad y dos (2) se encuentran pendientes por iniciar las gestiones requeridas para su mitigación. Evidencia No. 7".

Respuesta Oficina Control Interno:

La Oficina de Control Interno de acuerdo a los soportes allegados por la Oficina de Tecnología, evidenció el Informe de Revisión por la Dirección General Sistema de Gestión de Seguridad de Información SGSI, en el cual se muestran los avances sobre el cumplimiento de las acciones definidas en los planes de mejoramiento, sin embargo, con corte del presente seguimiento, de las 12 no conformidades la Oficina de Tecnología ejecutó para subsanar 8, por lo que se continua con el incumplimiento de todas las acciones definidas en los planes de mejoramiento producto de las Auditorías internas de seguridad de información, por lo tanto el hallazgo no es subsanado.

8. **No se evidencia el cumplimiento de las políticas y procedimientos de seguridad de información documentados, realizada en enero de 2019.**

Respuesta Oficina de Tecnología*:*

"La OTEC ha realizado la gestión para la actualización de la documentación propia del SGSI, de la siguiente manera:
● *Documentos Actualizados (10)*

o A3-PR-01 Gestión de Solicitudes de Soporte Técnico
o A3-GU-01 Guía Manejo de Contraseñas Seguras
o A3-GU-02 Guía de Desarrollo Seguro
o A3-PO-03 Política de Generación y Restauración de Copias de Restauración
o A3-PR-02 Procedimiento Configuración de Redes
o A3-PR-04 Gestión de eventos e Incidentes de Seguridad de la Información
o A3-PR-08 Gestión Acceso de Usuarios
o A3-PR-09 Instalación del Software Operacional
o A3-PR-11 Ciclo de Vida del Software
o A3-PR-13 Control de Cambios

https://www.uspec.gov.co/sistema-de-gestion-de-seguridad-de-la-informacion/

● *Política de Seguridad y Privacidad de la Información: Política de Seguridad y Privacidad de la Información: Evidencia*

ttps://www.uspec.gov.co/wp-content/uploads/2020/12/Politica-de-seguridad-y-privacidad-deinformacion.pdf

● *Documentos en proceso de actualización (1)*

o Procedimiento reutilización, borrado y destrucción segura de medios"

Respuesta Oficina Control Interno:

La oficina de Control Interno de acuerdo a los soportes allegado por la Oficina de Tecnología evidencia que algunos de los procedimientos establecidos por la OTEC se encuentran publicados, a continuación, las novedades evidenciadas:

Procedimientos actualizados:

- A3-GU-01 Guía Manejo de Contraseñas Seguras de fecha 30 de junio de 2020, versión 02
- A3-GU-02 Guía de Desarrollo Seguro de fecha 7 de enero de 2021, versión 02
- A3-PO-03 Política de Generación y Restauración de Copias de Restauración de fecha 14 de agosto 2020, versión 03
- A3-PR-02 Configuración de redes de fecha 8 de marzo de 2021, versión 02
- A3-PR-04 Gestión de eventos e Incidentes de Seguridad de la Información de fecha 29 de junio de 2020
- A3-PR-08 Gestión Acceso de Usuarios de fecha 26 de junio de 2020, versión 02
- A3-PR-09 Instalación del Software Operacional de fecha 30 de abril de 2020, versión 02
- A3-PR-11 Ciclo de vida del Software de fecha 20 de enero de 2021, versión 03
- A3-PR-13 Control de Cambios de fecha 7 de enero de 2021, versión 02

Lo anterior fue constatado en la página web https://www.uspec.gov.co/sistema-de-gestion-de-seguridad-de-la-informacion/

La Política de Seguridad y Privacidad de la Información, fue constatada mediante el siguiente link https://www.uspec.gov.co/wp-content/uploads/2020/12/Politica-de-seguridad-y-privacidad-deinformacion.pdf, el documento data del 17 de diciembre de 2020 resolución número 000683.

Los siguientes documentos reportados por la Oficina de Tecnología como actualizados presentan la siguiente novedad en la página de la entidad:

- A3-PR-01 Gestión de Solicitudes de Soporte Técnico, no se evidencia en la página web de la entidad junto a los demás procedimientos https://www.uspec.gov.co/?page_id=4477

Ahora bien, con respecto de los documentos en proceso de actualización o creación que manifestó la OTEC en el seguimiento del primer semestre tales como:

- Procedimiento desarrollo de software
- Procedimiento de transferencia de información
- Manual de políticas de seguridad de información
- Procedimiento de control de cambios
- Procedimiento reutilización, borrado y destrucción segura de medios (en proceso)

No se evidenció avances, tales como borradores de los mismos.

Es importante el cumplimiento de todas las políticas y procedimientos de seguridad de información documentados, realizada en enero de 2019, para mitigar el presente hallazgo.

9. **No se evidencia publicado el seguimiento a los procesos de contratación de la entidad en el portal del SECOP.**

Respuesta Oficina de Tecnología*:*

"La Dirección de Gestión Contractual periódicamente reitera mediante memorando dirigido a los supervisores, la obligación que tienen estos de cargar en la plataforma SECOP, la información que se produzca con ocasión de la ejecución contractual de la entidad. Así mismo se hace periódicamente un control aleatorio para hacer seguimiento a la labor de los supervisores y de acuerdo a los resultados de este, se les envía memorando resaltando sus falencias y recordando los compromisos que se despliegan de su actividad. La próxima fecha de control es el 19 de marzo Se anexa evidencia del último control realizado. Evidencia No. 11"

Respuesta Oficina Control Interno:

La Oficina de Control Interno evidenció la gestión realizada por la Oficina de Tecnología en cuanto al control de seguimiento a los procesos de contratación específicamente a la labor que deben realizar los supervisores de la entidad en el portal del SECOP, la evidencia anexada es la numero 9 por lo tanto el hallazgo es subsanado con respecto a la actividad que debe realizar la OTEC.

10. **No se evidencia una evaluación de todos los incidentes de seguridad de información, ni una respuesta oportuna de acuerdo a procedimiento establecido por la Entidad.**

Respuesta Oficina de Tecnología*:*

"Todos los eventos que los funcionarios y contratistas que se han reportado se han evaluado conforme su criticidad de acuerdo a lo establecido en el Procedimiento de Gestión de incidentes publicado en la página web el cual fue actualizado en junio de la vigencia 2020. Por otro lado, los incidentes de seguridad que se detectan a través de herramientas de seguridad son gestionados e informados con los implicados y a su vez se documentan en la herramienta Unificada de Gestión de Seguridad (USM) Alien Vault.

La respuesta a los eventos es oportuna en función del posible impacto de los eventos o incidentes. De igual forma, con la actualización del procedimiento se reforzó las partes débiles de la gestión, estableciendo los responsables y las acciones específicas a ejecutar en cada fase de la gestión de eventos e incidentes. Se anexa evidencia # 10 tickets de herramienta de seguridad, registro consolidado de seguimiento a eventos e incidentes y Procedimiento de Gestión de eventos e Incidentes de seguridad de la Información".

Respuesta Oficina Control Interno:

De acuerdo a las evidencias enviadas por la OTEC y la verificación en la página web de la Entidad, la Oficina de Tecnología verificó el documento Gestión de las Tecnologías de la Información, el cual data fecha de actualización 29 de junio de 2020, versión 02 código A3-PR-04, además, se evidencia una evaluación de todos los incidentes de seguridad de información, por parte de la OTEC, por lo anterior el hallazgo es subsanado.

11. **No se evidencia la firma del acuerdo de confidencialidad de la información para todos los funcionarios de la Entidad.**

Respuesta Oficina de Tecnología*:*

"El Grupo de Administración de Personal envía documento en el cual certifican que a la fecha se encuentran debidamente firmadas las actas de compromiso de seguridad de la información por parte de funcionarios de la USPEC, las cuales son firmadas por los servidores públicos al momento de ser posesionado el servidor público. Se anexa evidencia No. 11"

Esta es una actividad a cargo del Grupo de Administración de Personal, es importante mencionar que para realizar dicha actividad se cuenta con plazo hasta el 31 de diciembre del presenta año, sin embargo, a la fecha no se tienen avances, toda vez que se debe verificar en las carpetas físicas de cada funcionario quienes tienen firmado el acuerdo de confidencialidad de la información y con ocasión al teletrabajo por motivos de aislamiento preventivo por el estado de emergencia de salud decretado por la pandemia de Covid-19, esta actividad se demora. (Sin evidencia)".

Respuesta Oficina Control Interno:

La Oficina de Control Interno evidenció certificado firmado por la Coordinación de Administración de Personal en el cual consta que desde de mes de abril de 2020 a la fecha se encuentran tramitadas y debidamente firmadas las actas de compromiso de seguridad de la información por parte de funcionarios de la USPEC A4-FO-42 Versión: 02, por los servidores públicos que han ingresado desde esta fecha, la cual debe ser firmada al momento de ser posesionado el servidor público, sin embargo, no hay constancia de que todos los funcionarios hayan firmado el compromiso de seguridad de la información antes del mes de abril de 2020, por lo tanto, el hallazgo no es subsanado.

12. **No se cuenta con documento unificado donde establezcan los requisitos para seguir un proceso formal de adquisición y pruebas para la elaboración de los contratos y acuerdos con terceras partes donde se fije consideración a los requisitos de seguridad de la organización.**

Respuesta Oficina de Tecnología*:*

"Se aprobó y se publicó en la Página web de la USPEC en el mes de enero de 2021, A3-GU-02 Guía

de Desarrollo Seguro y A3-PR-11 Ciclo de Vida del Software, dentro de las Disposiciones Generales se establece los acuerdos entre terceras partes como derechos de autor, propiedad intelectual del código fuente a nombre de la USPEC, ambientes de prueba y producción además de los estándares, buenas prácticas o modelos de madurez de desarrollo seguro, basándose en (o publicadas por) OWASP, NIST, SANS, SAMM, BSIMM o MICROSOFT.

Evidencia:
● *A3-GU-02 Guía de Desarrollo Seguro: https://www.uspec.gov.co/wp-content/uploads/2021/01/A3-GU02_Guia_de_Desarrollo_Seguro_V02.pdf*
● *A3-PR-11 Ciclo de Vida del Software: https://www.uspec.gov.co/wp-content/uploads/2021/01/A3-PR11_Ciclo_de_Vida_del_Software_V03.pdf".*

Respuesta Oficina Control Interno:

La Oficina de Control Interno evidenció mediante la página web de la Entidad la publicación de los documentos A3-GU-02 Guía de Desarrollo Seguro y A3-PR-11 Ciclo de Vida del Software, los cuales establecen requisitos para seguir un proceso formal de adquisición y pruebas para la elaboración de los contratos y acuerdos con terceras partes donde se fija consideración a los requisitos de seguridad de la organización, por lo tanto, el hallazgo es subsanado.

6. CONCLUSIONES

- ✓ Se evidencia las gestiones realizadas por parte de la Oficina de Tecnología en cuanto al cumplimiento del Plan de tratamiento de riesgos de seguridad de información.

- ✓ La Oficina de tecnología tomó medidas al actualizar el procedimiento Gestión de Acceso a Usuarios, ahí plantea lineamientos para gestionar los diferentes usuarios.

- ✓ Se evidencia que la Oficina de Tecnología trabajó en un Plan de Sensibilización, capacitación y comunicación de seguridad de información, mediante el cual los funcionarios de la Entidad tengan conocimiento sobre lo relacionado con la Seguridad de la Información, de esta manera el hallazgo quedaría subsanado.

- ✓ Se evidencia la elaboración del Plan de Comunicación y sensibilización en seguridad de la información, por lo tanto, se da por subsanado el hallazgo.

- ✓ Se evidencia que la OTEC viene realizando actividades de actualización del Manual de Clasificación de Activos de la Información de la Entidad, sin embargo, debido a esto el formato para la identificación de archivos, que debe utilizar el Grupo de Gestión Documental continua con los campos de Información confidencial o privada sin uso hasta que la OTEC actualice el Manual de Clasificación.

- ✓ Se evidencia acciones por parte de la Oficina de Tecnología para prevenir el acceso físico no autorizado, el daño y la interferencia de información, así como la identificación de zonas seguras y sus respectivos controles físicos, además, el área responsable en la implementación el Grupo Administrativo reportó avances y las actividades desarrolladas para mitigar el hallazgo.

- ✓ Se evidencia que la Oficina de Tecnología realizó seguimiento al plan de mejoramiento producto de la auditoría interna realizada en el mes de octubre de 2019, sin embargo, se continua sin el cumplimiento de todas las acciones definidas en los planes de mejoramiento producto de las Auditorías internas de seguridad de información.

- ✓ La Oficina de Tecnología, ha realizado avances en la actualización de políticas, procedimientos, guía y manuales, es importante indicar que actualmente continúa actualizando y creando algunos de los cuales no reportó avances como borradores.

- ✓ La OTEC, reportó control de seguimiento a los procesos de contratación de la entidad en el portal del SECOP.

- ✓ La OTEC actualizó el Procedimiento de Gestión Eventos e Incidentes de Seguridad de Información, además actualmente está dando respuesta oportuna a los eventos e incidentes de seguridad de información, se evidencia una buena gestión por parte de la Oficina de Tecnología.

- ✓ Es importante que se certifique que todos los funcionarios de la Uspec hayan firmado el compromiso de seguridad de la información, pues hasta el momento solo se ha certificado la firma del documento por parte de los nuevos funcionarios desde la fecha abril de 2020 a la actualidad.

- ✓ Se evidencia la gestión de la OTEC, con la creación y publicación del documento A3-GU-=" Guía de Desarrollo seguro y A3-PR-11 Ciclo de Vida del Software, donde se unifican y establecen los requisitos para seguir un proceso formal de adquisición y pruebas para la elaboración de los contratos y acuerdos con terceras partes donde se fije consideración a los requisitos de seguridad de la organización, tampoco se evidencia avances del documento, por lo tanto, el hallazgo 12 es subsanado.

- ✓ Se evidencia que la Oficina de tecnología reporta un avance del 58,33% en su plan de mejoramiento.

7. RECOMENDACIONES

- ✓ Se recomienda que la Oficina de Tecnología continúe realizando seguimiento a las dependencias para el cumplimiento del Plan de tratamiento de riesgos de seguridad de información en la Entidad.

- ✓ Se recomienda, realizar acompañamiento al Grupo de Gestión Documental, y a la Dirección de Gestión Contractual para la implementación de lineamientos del procedimiento Gestión de Acceso a Usuarios, para minimizar los hallazgos.

- ✓ Se recomienda la socialización periódica del Plan de Comunicación y sensibilización en seguridad de la información, a los funcionarios de la Uspec mediante correo electrónico.

- ✓ Una vez actualizado el Manual de Clasificación de Activos de la Información de la Entidad, para que el Grupo de Gestión Documental, pueda trabajar en el formato Identificación de Archivos, los campos de Información confidencial o privada, los cuales son importantes tratándose de información sensible, se debe continuar con las actividades necesarias apoyando el Grupo de Gestión Documental para que el hallazgo se pueda subsanar.

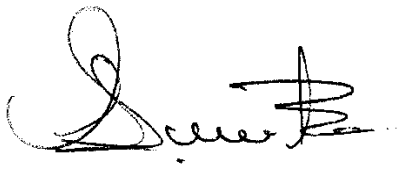
- ✓ Es importante que la Oficina de Tecnología realice cumplimiento de todas las acciones definidas en los planes de mejoramiento producto de las Auditorías internas de seguridad de información.

- ✓ Se recomienda terminar la actualización de políticas, procedimientos, guía y manuales, a cargo de la Oficina de Tecnología y que a la fecha no se evidencian publicados en la página web de la Entidad.

- ✓ Se recomienda dar continuidad a la evaluación de todos los incidentes de seguridad de información y dar respuesta de manera oportuna.

- ✓ Solicitar al Grupo de Administración de Personal, constancia de que todos los funcionarios y contratistas de la Entidad hayan firmado el acuerdo de confidencialidad de la información sin excepción alguna, desde antes de abril de 2020.

Atentamente,



ALEXI MAUREDY PERDOMO BAMBAGUE
Coordinadora Grupo Evaluación de la Gestión Institucional

Anexos: se adjuntan 2 copias

Elaboró: Natali Padrón Aguilar- Profesional Universitario
Revisó: Alexi Maureli Perdomo Bambague- Coordinadora Grupo Evaluación de la Gestión Institucional