Proceso y/o tema auditado:	Gestión de TIC	No. Auditoria 04/2020
Nombre y Cargo de los Auditados:	**NOMBRE** / **CARGO** CR(RA) Sonia Dolly Gutierrez Carrillo / Jefe Oficina de TIC's Ing. Sis. Cesar Adolfo Gonzalez Peña / Coordinador Grupo Ing. Sis. Yuri Daianny Ruiz Franco / Coordinadora Grupo Informática	
Equipo auditor:	**NOMBRE** / **ROL** Yuby Elizabeth Aguacía Hernández / Auditor	
Objetivo auditoría:	Verificar Riesgos, controles y cumplimiento a instrucciones por parte de la Dirección General durante la vigencia 2019	
Alcance auditoría:	Evaluar efectividad de los puntos de controles para la gestión del Riesgo y cumplimiento a instrucciones por parte de la Dirección General	

Introducción y Contextualización

Mediante memorando No. 20191200723583 ALOCI-GSE-120 de fecha 30-12-2019, se informó la apertura de la Auditoria a la efectividad de los puntos de control para la gestión del Riesgo y cumplimiento a instrucciones por parte de la Dirección General, del Proceso de Gestión de Tecnologías de la Información y Comunicaciones (TIC).

La Jefe de la oficina de TIC's, suscribió la Carta de representación de la presente auditoria de Gestión al Proceso de TIC el 30 de diciembre de 2019.

En la auditoria No. 01 de 2020 se dejó contemplado el cumplimiento a instrucciones por parte de la Dirección General con relación al proceso de TIC's

DESARROLLO DE AUDITORIA

La auditoría se llevó a cabo teniendo en cuenta el siguiente marco normativo:

- Guía para la administración del riesgo y el diseño de controles en entidades públicas V4 emitido por el Departamento Administrativo de la Función Publica (DAFP)
- Manual de Administración del Riesgo V8 Código No. GI-MA-01 (ALFM), publicado en la suite visión.
- Política de Riesgos Institucionales y Corrupción vigencia 2019:
  Directiva Permanente No. 11 ALDG-ALOAP11-110 de 05 de julio del 2019.
- Mapa de riesgos de la Agencia Logística de las Fuerzas Militares (Institucional y de Corrupción) Gestión TIC vigencia 2019

A continuación se desarrolla la auditoría efectividad de los puntos de controles para la gestión del Riesgo de TICs, teniendo como soportes lo establecido en el mapa de riesgos de la entidad y sus registros consignados en la SUITE VISION de conformidad con la Directiva Permanente No. 11 ALDG-ALOAP11-110 de 05 de julio del 2019, así:

Monitoreo a los planes de mitigación

Periodo: Sin agrupar Desde: Hasta: 12/02/2020 Valores vigentes

Monitoreo a los planes de mitigación
De riesgos

Cumplimiento Consolidado

Nombre	Total de tareas	Tareas finalizadas	Avance real	Tareas planificadas	Tareas finalizadas a tiempo	Efectividad	Tareas en desarrollo	Tareas canceladas
PLAN DE MITIGACION DE RIESGOS 2019	1964	1953	99,44%	1952	1156	100,05%	10	0
Administrativa	91	80	87,91%	79	40	101,27%	10	0
Desarrollo Organizacional	14	14	100,00%	14	10	100,00%	0	0
Direccionamiento Estrategico	36	36	100,00%	36	11	100,00%	0	0
Financiera	441	441	100,00%	441	302	100,00%	0	0
Gestión de Contratación	518	518	100,00%	518	305	100,00%	0	0
Gestión del Talento Humano	49	49	100,00%	49	34	100,00%	0	0
Innovacion	41	41	100,00%	41	31	100,00%	0	0
Juridica	3	3	100,00%	3	1	100,00%	0	0
Operaciones Logisticas	615	615	100,00%	615	331	100,00%	0	0
Planificacion del abastecimiento	69	69	100,00%	69	43	100,00%	0	0
Seguimiento y Evaluación	49	49	100,00%	49	15	100,00%	0	0
Tecnologia	36	36	100,00%	36	33	100,00%	0	0

Fuente: Mapa de Riesgos – Suite Visión Empresarial 12-02-2020

Se efectuó verificación al mapa de riesgos institucionales y de corrupción con sus respectivos controles, así:

1. <u>Riesgo de Corrupción:</u>

1.1. Alteración o manipulación de sistemas y datos

DE CORRUPCIÓN (TOTAL CONTROLES = 5)								
GESTIÓN DE TIC (NMO) (TOTAL CONTROLES = 5)								
CONTROL	**CLASE DE CONTROL**	**ESCALA**	**DESCRIPCIÓN**	**RIESGO**	**CLASE DE RIESGO**	**ÁREA**	**PROCESO**	**INST**
Restricción de acceso a la información de acuerdo al perfil del	Preventivo	Probabilidad	Restricción de acceso a la información de acuerdo al perfil del	Alteración o manipulación de sistemas y datos	Riesgo de Tecnología	Oficina TIC's	Gestión de TIC (NMO)	

usuario.			usuario.					
Realización de mantenimientos preventivos a la plataforma tecnológica.	Preventivo	Probabilidad	Realización de mantenimientos preventivos a la plataforma tecnológica.		Riesgo de Tecnología	Oficina TIC's	Gestión de TIC (NMO)	
Instalación y actualización de antivirus en todos los equipos de la empresa.	Preventivo	Probabilidad	Instalación y actualización de antivirus en todos los equipos de la empresa.		Riesgo de Tecnología	Oficina TIC's	Gestión de TIC (NMO)	
Instalación de parches y actualizaciones de software.	Preventivo	Probabilidad	Instalación de parches y actualizaciones de software.		Riesgo de Tecnología	Oficina TIC's	Gestión de TIC (NMO)	
Realización de backups de la información contenida en los servidores y bases de datos.	Preventivo	Impacto	Realización de backups de la información contenida en los servidores y bases de datos.		Riesgo de Tecnología	Oficina TIC's	Gestión de TIC (NMO)	

Fuente: Reporte De Controles De Riesgos – Vigencia 2019, Suite Vision Empresarial

A continuación se detalla los controles asociados al riesgo, conforme a los soportes presentados en la SUITE VISION:

Restricción de acceso a la información de acuerdo al perfil del usuario.

Verificación OCI: Se anexan formato de creación de usuario, con perfiles de usuario. Configuración del directorio activo y demás aplicativos. Acceso con usuario y contraseña del IV Trimestre.

Realización de mantenimientos preventivos a la plataforma tecnológica.

Verificación OCI: Se adjuntan en la Suite Visión las evidencias de los mantenimientos realizados en la Oficina Principal, Regionales Amazonia, Caribe, Centro, Nororiente, Suroccidente, Sur, Tolima Grande.

No se evidencia los mantenimientos preventivos a la plataforma tecnológica de las Regionales Antioquia Choco, Llanos Orientales y Norte.

Instalación y actualización de antivirus en todos los equipos de la empresa.

Verificación OCI: Se adjunta el acta y recibo a satisfacción del contrato No. 001-116-2019 "*Adquisición y puesta en funcionamiento de la plataforma "web application firewall" para la Agencia Logística de las Fuerzas Militares*". Así mismo se evidencia documento con los pantallazos generados por la consola de administración del antivirus Kaspersky.

Instalación de parches y actualizaciones de software

Se presenta documento en el que se detalla la Configuración del servidor WSUS, para el manejo de actualizaciones de los sistemas operativos, el cual se sincroniza con el árbol de dominio del controlador de dominio y la configuración del horario (día-hora) en el cual la máquina procederá a realizar el respectivo despliegue de Actualizaciones.

Realización de backups de la información contenida en los servidores y bases de datos.

Verificación OCI: En lo reportado en la Suite Visión, se adjuntan evidencias de capturas de pantalla de la programación de backup de los servidores, backup a cintas de SAP-ERP y backup de servicios IPV6 por router.

Se recomienda adjuntar el diligenciamiento del formato almacenamiento periódico de Backups GTI-FO-03 V. 1, en el cual se registra el almacenamiento en medio externo.

Conforme a novedades presentadas en la Regional Amazonia en el mes de noviembre de 2019, en referencia a la utilización del usuario YDORADO en el aplicativo ERP/SAP, en diferentes equipos, se solicitó por medio de memorando N° 20201200115343 ALOCI-GSE-120 del 06 de marzo de 2020, las acciones tomadas por la jefatura de las TIC en razón a que en su comunicación a la regional, en el mes de noviembre de 2019, cita *"Lo anterior con el fin de establecer si se están prestando el usuario conectándose a otros equipos, teniendo en cuenta que el usuario YDORADO posee permisos amplios que permiten crear, anular y mover mercancías entre otras, generando inminente riesgo para faltantes riesgo para faltantes y sobrantes por administradores quien pueda hacer uso de este usuario".* Este riesgo no se ve identificado en el mapa de riesgos institucionales, ni de corrupción. Se debe incluir en la identificación del contexto del riesgo, la posibilidad que hay de que se presten los usuarios y contraseñas entre funcionarios de la Entidad y el impacto que este tendría de acuerdo a los perfiles y permisos que tiene cada uno.

2. <u>Riesgos institucionales:</u>

2.1. Pérdida, daño, manipulación o sustracción de información o de equipos tecnológicos

2.2. Interrupción del servicio de la plataforma tecnológica

NO CORRUPCIÓN (TOTAL CONTROLES = 9)									
GESTIÓN DE TIC (NMO) (TOTAL CONTROLES = 9)									
CONTROL	**CLASE DE CONTROL**	**ESCALA**	**DESCRIPCIÓN**	**RIESGO**	**CLASE DE RIESGO**	**ÁREA**	**PROCESO**	**INSTITUCIONAL**	**CORRUPCIÓN**
Restricción de acceso a la información de acuerdo al perfil del usuario.	Preventivo	Probabilidad	Restricción de acceso a la información de acuerdo al perfil del usuario.	Pérdida, daño, manipulación o sustracción de información o de equipos tecnológicos	Riesgo de Tecnología	Oficina TIC's	Gestión de TIC (NMO)	Si	No
Restricción de acceso al datacenter.	Preventivo	Probabilidad	Restricción de acceso al datacenter.		Riesgo de Tecnología	Oficina TIC's	Gestión de TIC (NMO)	Si	No
Revisión de la configuración del sistema de seguridad perimetral de la red de datos.	Preventivo	Probabilidad	Revisión de la configuración del sistema de seguridad perimetral de la red de datos.		Riesgo de Tecnología	Oficina TIC's	Gestión de TIC (NMO)	Si	No
Instalación de parches y actualizaciones de software.	Preventivo	Probabilidad	Instalación de parches y actualizaciones de software.	Interrupción del servicio de la plataforma tecnológica	Riesgo de Tecnología	Oficina TIC's	Gestión de TIC (NMO)	Si	No
Realización de mantenimientos preventivos a la plataforma tecnológica.	Preventivo	Probabilidad	Realización de mantenimientos preventivos a la plataforma tecnológica.		Riesgo de Tecnología	- Oficina TIC's	- Gestión de TIC (NMO)	Si	No
Instalación y actualización de antivirus en todos los equipos de la empresa.	Preventivo	Probabilidad	Instalación y actualización de antivirus en todos los equipos de la empresa.		Riesgo de Tecnología	- Oficina TIC's	- Gestión de TIC (NMO)	Si	No
Mantenimiento de equipos de respaldo (UPS) para el fluido	Preventivo	Probabilidad	Mantenimiento de equipos de respaldo (UPS) para el fluido eléctrico.		Riesgo de Tecnología	- Oficina TIC's	- Gestión de TIC (NMO)	Si	No

eléctrico.									
Verificación del Data Center alterno para Sistemas de Información Críticos.	Preventivo	Probabilidad	Verificación del Data Center alterno para Sistemas de Información Críticos.		Riesgo de Tecnología	- Oficina TIC's	- Gestión de TIC (NMO)	Si	No
Revisión de la configuración del sistema de seguridad perimetral de la red de datos.	Preventivo	Probabilidad	Revisión de la configuración del sistema de seguridad perimetral de la red de datos.		Riesgo de Tecnología	- Oficina TIC's	- Gestión de TIC (NMO)	Si	No

Fuente: Reporte De Controles De Riesgos – Vigencia 2019, Suite Vision Empresarial

A continuación, se detalla los controles asociados a los riesgos institucionales, así:

2.1 Pérdida, daño, manipulación o sustracción de información o de equipos tecnológicos

Restricción de acceso a la información de acuerdo al perfil del usuario.

Verificación OCI: Se anexan formato de creación de usuario, con perfiles de usuario. Configuración del directorio activo y demás aplicativos. Acceso con usuario y contraseña del IV Trimestre.

Este control está identificado en el riesgo de corrupción. Se debe identificar de manera puntual las causas del origen del riesgo, ya que de está depende su actividad de control, como se encuentra en la actualidad está más acorde en su tipología a un riesgo de corrupción.

Conforme a novedades presentadas en la Regional Amazonia en el mes de noviembre de 2019, en referencia a la utilización del usuario YDORADO en el aplicativo ERP/SAP, en diferentes equipos, se solicitó por medio de memorando N° 20201200115343 ALOCI-GSE-120 del 06 de marzo de 2020, las acciones tomadas por la jefatura de las TIC en razón a que en su comunicación a la regional, en el mes de noviembre de 2019, cita *"Lo anterior con el fin de establecer si se están prestando el usuario conectándose a otros equipos, teniendo en cuenta que el usuario YDORADO posee permisos amplios que permiten crear, anular y mover mercancías entre otras, generando inminente riesgo para faltantes riesgo para faltantes y sobrantes por administradores quien pueda hacer uso de este usuario."*. Este riesgo no se ve identificado en el mapa de riesgos institucionales, ni de corrupción. Se debe

incluir en la identificación del contexto del riesgo, la posibilidad que hay de que se presten los usuarios y contraseñas entre funcionarios de la Entidad y el impacto que este tendría de acuerdo a los perfiles y permisos que tiene cada uno.

Restricción de acceso al Datacenter

Verificación OCI: Se anexan el formato de control de acceso al data center**.**

Revisión de la configuración del sistema de seguridad perimetral de la red de datos

Verificación OCI: Se adjunta el acta de recibo a satisfacción del contrato No. 001-116-2019**.** En la ALFM se tiene implementado un sistema de seguridad perimetral mediante el cual se controlan los diferentes accesos a sistemas de información propios de la entidad y la salida a sitios en Internet.

Es preciso indicar que los controles asociados al riesgo no incluyen controles para la pérdida daño, manipulación de equipos tecnológicos.

2.2 Interrupción del servicio de la plataforma tecnológica

Instalación de parches y actualizaciones de software:

Verificación OCI: Se presenta documento en el que se detalla la Configuración del servidor WSUS para el manejo de actualizaciones de los sistemas operativos el cual se sincroniza con el árbol de dominio del controlador de dominio y la configuración del horario (día-hora), en el cual la máquina procederá a realizar el respectivo despliegue de Actualizaciones.

Este control está identificado en el riesgo de corrupción. Se debe identificar de manera puntual las causas del origen del riesgo, ya que de está depende su actividad de control, como se encuentra en la actualidad está más acorde en su tipología a un riesgo institucional.

Realización de mantenimientos preventivos a la plataforma tecnológica.

Verificación OCI: Se adjuntan en la Suite Visión las evidencias de los mantenimientos realizados en la Oficina Principal, Regionales Amazonia, Caribe, Centro, Nororiente, Suroccidente, Sur, Tolima Grande.

No se evidencia los mantenimientos preventivos a la plataforma tecnológica de las Regionales Antioquia Choco, Llanos Orientales y Norte.

Este control está identificado en el riesgo de corrupción. Se debe identificar de manera puntual las causas del origen del riesgo, ya que de está depende su actividad de control, como se encuentra en la actualidad está más acorde en su tipología a un riesgo institucional.

Instalación y actualización de antivirus en todos los equipos de la empresa.

Verificación OCI: Se adjunta el acta y recibo a satisfacción del contrato No. 001-116-2019. Así mismo se evidencia documento con los pantallazos generados por la consola de administración del antivirus Kaspersky.

Este control está identificado en el riesgo de corrupción. Se debe identificar de manera puntual las causas del origen del riesgo, ya que de está depende su actividad de control, como se encuentra en la actualidad está más acorde en su tipología a un riesgo institucional.

Mantenimiento de equipos de respaldo (UPS) para el fluido eléctrico.

Verificación OCI: Se adjuntan en la Suite Visión las evidencias de la ejecución de contrato de mantenimiento de respaldo (UPS) de la Oficina Principal, Regionales Amazonia, Caribe, Centro, Llanos Orientales, Norte, Suroccidente, Sur, Tolima Grande.
No se evidencia contrato de mantenimiento de respaldo (UPS) para el fluido eléctrico de las Regionales Antioquia Choco, Nororiente y Pacifico

Verificación del Data Center alterno para Sistemas de Información Críticos.

Verificación OCI: Se adjuntan los archivos de las capturas de las pantallas de pruebas DPR, pruebas de baja de servicios data center alterno y pruebas DPR.

Revisión de la configuración del sistema de seguridad perimetral de la red de datos.
Verificación OCI: Se adjunta el acta de recibo a satisfacción del contrato No. 001-116-2019. En la ALFM se tiene implementado un sistema de seguridad perimetral mediante el cual se controlan los diferentes accesos a sistemas de información propios de la entidad y la salida a sitios en Internet.

Este control está identificado en el riesgo de corrupción. Se debe identificar de manera puntual las causas del origen del riesgo, ya que de está depende su actividad de control, como se encuentra en la actualidad está más acorde en su tipología a un riesgo institucional.

Análisis de la información reportada:

De acuerdo a la información reportada a través de la Suite Visión, se debe tener en cuenta lo establecido en la Guía para la administración del riesgo y el diseño de controles en entidades públicas versión No 4 del Departamento Administrativo de la Función pública – riesgo de gestión, corrupción y seguridad, se define:

Riesgo de seguridad digital: ***"****Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas"* y

Riesgo de corrupción: ***"****posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado".*

En la guía para la administración del riesgo, precisa la identificación de riesgos de corrupción para evitar que se presenten confusiones entre un riesgo de gestión y uno de corrupción, se debe implementar de la **matriz de definición de riesgo de corrupción**, que incorpora cada uno de los componentes de su definición. Lo anterior de conformidad a la siguiente grafica

MATRIZ: DEFINICIÓN DEL RIESGO DE CORRUPCIÓN

Descripción del riesgo	Acción u omisión	Uso del poder	Desviar la gestión de lo público	Beneficio privado
Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros con el fin de celebrar un contrato.	X	X	X	X

Fuente: Secretaría de Transparencia de la Presidencia de la República.

Así mismo, no se observa la identificación de los riesgos de seguridad digital que se basan en la afectación de tres criterios en un activo o un grupo de activos dentro del proceso: "Integridad, confidencialidad o disponibilidad", incluidos en los lineamientos dados en la guía para la administración del riesgo y el diseño de controles en entidades públicas versión No 4 del Departamento Administrativo de la Función pública – riesgo de gestión, corrupción y seguridad.

De otra parte en el anexo 4 lineamientos para la gestión de riesgos de seguridad digital en entidades públicas, establece en numeral 4.1.3 *"Alineación o creación de la política de gestión de riesgo de seguridad digital. Es necesario que la entidad pública establezca una política de gestión de riesgo integral, donde se incluya el compromiso en la gestión de los riesgos de seguridad digital en todos sus niveles…".* Lo anterior no se evidencia en la política de administración del riesgo publicada en la página web de la entidad, URL: https://www.agencialogistica.gov.co/es/pagina/vigencia-2019-2, visualizada el 28-02-2020.

APLICACIÓN PROCEDIMIENTO GSE-PR-02

Con memorandos No. 20201200125443 ALOCI – GSE-120 dirigido al jefe de la Oficina Asesora de Planeación y Memorando N° 20201200124773 ALOCI –GSE-120 dirigido a la jefa de las TIC´s de fecha del 09 de marzo de 2020, se remitió informe preliminar de la Auditoria de Gestión del Proceso de Gestión de Tecnologías de la Información y comunicaciones.

Con memorando No. 20201320137613 ALDG -ALGTI -GI-132 de marzo 13 del 2020, la Jefe Oficina de Tecnologías de la Información y Comunicaciones -TIC´s dio respuesta a las observaciones y recomendaciones así:

"*Los mantenimientos preventivos a la plataforma tecnológica de las Regionales Antioquia Choco, Llanos Orientales y Norte, fueron realizados de acuerdo a los contratos suministrados por cada Regional, es de resaltar que por error no se subieron los contratos a la plataforma Suite Visión en la fecha indicada, sin embargo, en este momento ya se encuentran cargados en la herramienta y se adjuntan al presente informe.*

Respecto a las recomendaciones a continuación me permito precisar:

1. Implementar lo establecido en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas versión No. 4 del Departamento Administrativo de la Función Pública – Riesgo de Gestión, Corrupción y Seguridad Anexo No.4 Lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas.

***Respuesta**: Respecto a la aplicación de los lineamientos para la Gestión de Riesgos de Seguridad Digital de la Guía de Administración del DAFP, me permito informar que la entidad viene desarrollando e implementando el análisis de riesgos indicado en la mencionada guía, la entidad tiene actividades de Control documentadas en la Directiva Permanente No.11 del 2019 -"Política de Administración de Riesgos de la Agencia Logística de las Fuerzas Militares" y en el procedimiento de Gestión de Seguridad Informática.*

Además, se tiene identificados los riesgos de seguridad digital, con las actividades de controles preventivos y detectivos, soportados en las herramientas y protocolos de seguridad digital que posee la ALFM, los cuales se evidencian con pantallazos de configuración y en los informes generados de los aplicativos de seguridad, Forti analyzer, Fortiweb, Forti Mail, Forti Gate, Forti Sandbox, el SIEM del comando General, Antimalware, las políticas de acceso y administración de los usuarios y servicios del dominio, entre otros.

2. Pregunta: Se recomienda adjuntar el diligenciamiento del formato almacenamiento periódico de Backups GTIFO-03 V. 1, en el cual se registra el almacenamiento en medio externo.

***Respuesta**: Teniendo en cuenta la recomendación de adjuntar el formato almacenamiento periódico de Backups GTIFO- 03 V. 1, en el cual se registra el almacenamiento en medio externo, se sube a la plataforma SUITE VISION y se adjunta al presente informe.*

3. Pregunta: Establecer controles en el manejo de las claves de usuario que permitan visualizar su trazabilidad y manejo en tiempo real.

***Respuesta**: Existen controles que permiten manejar la autenticación (login) de los usuarios a la red, a las aplicaciones, a internet y a todos los servicios tecnológicos que maneja la entidad en tiempo real, para ello se tiene en el Directorio Activo y en SAP configurados los siguientes lineamientos:*

- *Política de contraseñas y seguridad de la información.*
- *Política y acciones para construir contraseñas seguras.*
- *Procedimiento de Gestión de Usuarios.*

- *Caducidad de las contraseñas.*
- *Formatos de Creación de Usuario con las políticas de uso, aval del superior inmediato y Jefe de Área.*
- *Logs de Auditoria.*
- *Sensibilización de los usuarios en temas de seguridad digital.*
- *Bloqueo de usuario, por novedades de vacaciones y excusas médicas, reportadas por el área administrativa.*
- *Manejo de excepciones de seguridad.*
- *Niveles de acceso a internet.*

En este sentido, de acuerdo a los controles que recomienda el Departamento Administrativo de la Función Pública en el Anexo No. 4 "Lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas, la Entidad lo aplica en las políticas antes enunciadas.

Ahora bien, dando alcance al caso presentado con un usuario SAP (YDORADO) logueado en varios equipos, ingreso a la plataforma en diferentes momentos, pero ***no de forma simultánea o multilogon****, lo cual corresponde a la configuración establecido en el Sistema SAP.*
La mayoría de las herramientas tecnológicas de la ALFM permiten la visualizar la trazabilidad de acceso de los usuarios a través de las funcionalidades de auditoria que ellas tienen.

4. Pregunta: Implementar los controles y los sistemas de protección de la información necesarios para prevenir la materialización de riesgos y poder llevar trazabilidad a la ejecución de sus actividades de control.

Respuesta*: Respecto a la verificación efectuada a los riesgos: para el riesgo 2.1 Pérdida, daño, manipulación o sustracción de información o de equipos tecnológicos, la auditora manifiesta: "Este riesgo no se ve identificado en el mapa de riesgos institucionales de corrupción. Se debe incluir en la identificación del contexto del riesgo, la posibilidad que hay de que se presten los usuarios y contraseñas entre funcionarios de la Entidad y el impacto que este tendría de acuerdo a los perfiles y permisos que tiene cada uno"*

Para la Oficina TIC, el riesgo está bien identificado como un riesgo institucional, debido a que se puede materializar en cualquiera de los servicios tecnológicos de la entidad, a nivel institucional un usuario podría hacer uso de sus credenciales para el manejo de información de acuerdo a intereses personales.

Es de resaltar que la observación es válida, debido a que también puede ser identificado como un riesgo de corrupción; porque en el evento que un usuario suministre o haga entrega de información a personal externo a la entidad para favorecer o alertar, se convierte en corrupción.

De acuerdo a lo anterior, se coordinará con Desarrollo Organizacional y Gestión Integral, para incluirlo en el mapa de riesgos de la Entidad. Así mismo, se gestionó una mesa de trabajo, para la propuesta de ajustes pertinentes a la Política de Riesgos, que exprese tácitamente que la entidad administra los Riesgos asociados a la Seguridad Digital.

5. Pregunta: Para el riesgo "Pérdida, daño, manipulación o sustracción de información o de equipos tecnológicos", se recomienda establecer actividades de control en referencia a los equipos tecnológicos, ya que este concepto es genérico o delimitar su alcance conforme a la redacción del

Riesgo. "Incluir controles en cuento al monitoreo de usuario que tienen conectados en más de un computador".

***Respuesta**: A lo anterior la Oficina de Tecnología, se permite informar que dicho riesgo está contemplado en el mapa riesgos para el área administrativa, en razón a que son los que tienen el proceso de seguridad física de la Entidad y son quienes controlan el ingreso y salida de equipos, en este orden de ideas es el proceso de Gestión Administrativa quien dentro de sus responsabilidades ha identificado un riesgo con su respectivo tratamiento para la perdida de activos de la entidad.*

Cabe resaltar, que Oficina TIC, tiene identificado dos riesgos que aplican tanto en la clasificación de corrupción como de institucionales, con los mismos controles, dado que se puede materializar en ambos y es válido, lo anterior lo determina es el fin que se le dé al bien y/o información"

Por lo anterior la Oficina de Control Interno, no evidencia soportes técnicos que desvirtúen las observaciones y recomendaciones comunicadas en el informe preliminar por tal razón se ratifica en las recomendaciones dadas en cuanto:

1. Implementar lo establecido en la Guía para la administración del riesgo y el diseño de controles en entidades públicas versión No 4 del Departamento Administrativo de la Función pública – riesgo de gestión, corrupción y seguridad Anexo No. 4 lineamientos para la gestión de riesgos de seguridad digital en entidades públicas.

2. Establecer de manera puntual las causas de los riesgos de corrupción y de los de gestión de acuerdo a las políticas y lineamientos de la Entidad.

3. Para el riesgo "*Pérdida, daño, manipulación o sustracción de información o de equipos tecnológicos",* se recomienda establecer actividades de control en referencia a los equipos tecnológicos, ya que este concepto es genérico o delimitar su alcance conforme a la redacción del Riesgo.

De otra parte, en referencia al memorando No. 20201200125443 ALOCI –GSE-120 de 09-03-2020, en el cual se comunica el informe preliminar a la Oficina Jefe de la Oficina Asesora de Planeación e Innovación Institucional, no dio respuesta las observaciones y recomendaciones comunicadas en el informe preliminar por tal razón se ratifica en las recomendaciones dadas en cuanto:

4. Alinear la política de gestión de riesgo, donde se incluya el compromiso en la gestión de los riesgos de seguridad digital en todos los niveles de la entidad (Desarrollo organizacional y Gestión Integral).

Hallazgos

Omitido

Recomendaciones:

1. Implementar lo establecido en la Guía para la administración del riesgo y el diseño de controles en entidades públicas versión No 4 del Departamento Administrativo de la Función pública – riesgo de gestión, corrupción y seguridad Anexo No. 4 lineamientos para la gestión de riesgos de seguridad digital en entidades públicas.

2. Establecer de manera puntual las causas de los riesgos de corrupción y de los de gestión de acuerdo a las políticas y lineamientos de la Entidad.

3. Para el riesgo "*Pérdida, daño, manipulación o sustracción de información o de equipos tecnológicos",* se recomienda establecer actividades de control en referencia a los equipos tecnológicos, ya que este concepto es genérico o delimitar su alcance conforme a la redacción del Riesgo.

4. Alinear la política de gestión de riesgo, donde se incluya el compromiso en la gestión de los riesgos de seguridad digital en todos los niveles de la entidad (Desarrollo organizacional y Gestión Integral).

Fortalezas

Omitido

Fecha de informe de Auditoria

Informe preliminar: 09-03-2020
Informe Final: 18-03-2020

Nombre, cargo y firma del equipo auditor:

NOMBRE	CARGO	FIRMA
Yuby Elizabeth Aguacía Hernández	Técnica para Apoyo Seguridad y Defensa	Yuby Elizabeth Aguacia Hernández Firmado digitalmente por Yuby Elizabeth Aguacia Hernández Fecha: 2020.03.18 08:03:12 -05'00'