1. DESCRIPCIÓN GENERAL	
Objetivo de la Auditoria:	Verificar el cumplimiento del proceso Gestión de tecnologías de Información y su articulación con la estrategia definida por el área de TICs respecto a Gestión de Solicitudes de Soporte Técnico, Configuración de Redes y Gobierno Digital: ▪ Validar el cumplimiento Normativo de acuerdo con los procesos de gestión TICs: Relación de contratos, informes, relación de formatos procedimientos de gestión, implementación de políticas de seguridad informática, controles físicos y lógicos, Backus y evidencias documentales de sus procedimientos. ▪ Adaptar controles, medidas, procedimientos para adaptar un plan de contingencia donde la entidad pueda evaluar su nivel de riesgo. Corroborar que la información de la entidad se encuentre disponible, integra, confiable y actualizada acorde al Decreto 1151 de 2018.
Alcance de la Auditoria:	La auditoría considera validación y cumplimiento de las normas que rigen al área de Tecnología como proceso de apoyo en la Unidad de servicios Penitenciarios y carcelarios – USPEC De acuerdo al Check List basado en los procesos que Gestión de solicitudes de soporte técnico: mantenimiento correctivo y preventivo, Políticas y procedimientos de seguridad de la información, Licencias y software en la entidad: autorización y uso PETI 2015 -2018: formulación, desarrollo y evaluación Plan de acción, mapa de riesgos, planes de mejoramiento, indicadores, otros planes compromisos y Gobierno en línea (GEL).
Procedimiento de la Auditoria	AUDITORIAS INTERNAS Código: E1-PR-01, Versión: 01, Vigencia: 07/06/2016
Auditor Líder	JOSE JORGE ROCA MARTÍNEZ
Equipo Auditor:	JHONNIER YESID ZÚÑIGA MOSQUERA
Fecha de la Auditoria	Diciembre de 2018
Dependencia a cargo del proceso auditado	Oficina de Tecnología.

Procesos Auditados	1) . Proceso gestión de las Tecnologías de la información 2) . Gobierno en línea (GEL)

2. ANÁLISIS Y EVALUACIÓN DE DATOS

2.1 MARCO NORMATIVO

- **Nomograma:** https://www.uspec.gov.co/wp-content/uploads/2018/09/Normograma_2018-1.pdf
- **MINITIC:** https://www.mintic.gov.co/portal/604/articles-3643_documento.pdf
- **Decreto 1151 de 2018:** Estrategia del Gobierno para lograr inclusión social y competitiva. "El objeto del decreto pretende lograr un salto en la inclusión social y en la competitividad del país a través de la apropiación y el uso adecuado de las Tecnologías de la Información y las Comunicaciones (T.I.C). Esta estrategia pretende contribuir a mejorar la eficiencia y transparencia del Estado Colombiano a través de la construcción gradual de un gobierno electrónico, además de promover la actuación del gobierno como usuario modelo y motor de la utilización de las TIC.
- **Decreto 1151 de 2018:** Estrategia del Gobierno para lograr inclusión social y competitiva. "El objeto del decreto pretende lograr un salto en la inclusión social y en la competitividad del país a través de la apropiación y el uso adecuado de las Tecnologías de la Información y las Comunicaciones (T.I.C). Esta estrategia pretende contribuir a mejorar la eficiencia y transparencia del Estado Colombiano a través de la construcción gradual de un gobierno electrónico, además de promover la actuación del gobierno como usuario modelo y motor de la utilización de las TIC.
- **Ley 1712 de 2014:** Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional
- **Decreto Único Reglamentario 1081 de 2015:** Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República Título 1 Disposiciones generales en materia de transparencia y del derecho de acceso a la información pública nacional.
- **Resolución MinTIC 3564 de 2015:** Por la cual se reglamentan aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública. ARTÍCULO 1o. OBJETO. La presente resolución tiene por objeto establecer los lineamientos respecto de los estándares para publicación y divulgación de la información, accesibilidad en medios electrónicos para población en situación de discapacidad, formulario electrónico para la recepción de solicitudes de acceso a información pública, condiciones técnicas para la publicación de datos abiertos y condiciones de seguridad de los medios electrónicos (...)
- **Decreto 4150 de 2011:** Por el cual se crea la Unidad de Servicios Penitenciarios y Carcelarios, se determina su objeto y estructura.

Artículo 16°. OFICINA DE Tecnología.
12. Implementar las acciones necesarias para asegurar la organización, administración, seguridad y control del hardware, software y de la información institucional.

2.2 ACTIVIDADES DESARROLLADAS

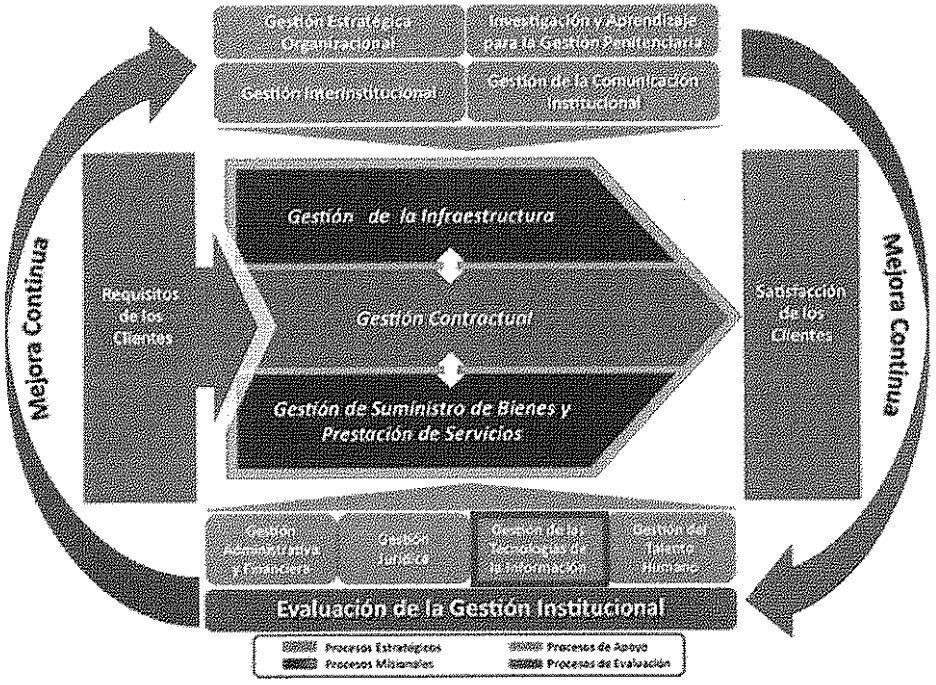
1. En reunión de apertura de auditoría al proceso Gestión de las Tecnologías de la Información, se comunicó sobre el seguimiento a los procesos de la Oficina de Tecnología.

2. En la planeación de la auditoría se tuvo en cuenta la información soporte suministrada por cada uno de los funcionarios que manejan las diferentes actividades que le dan vida a los procesos.
3. La revisión se realiza mediante el Check list de los procesos que tiene la oficina de tecnología, validando desde su normatividad hasta las gestión de solicitudes de soporte técnico: mantenimiento correctivo y preventivo, Políticas y Procedimientos de Seguridad de la información, Licencias y software en la Entidad: autorización y uso PETI 2015 -2018: formulación, desarrollo y evaluación Plan de acción, mapa de riesgos, planes de mejoramiento, indicadores, otros planes compromisos y Gobierno en línea (GEL) y soportes documentados de cada una de las actividades..
4. Se informan los aspectos relevantes y los aspectos por mejorar sobre la gestión, cumplimiento, robustez e insipiencia de cada uno de los puntos establecidos en el Check List.

2.2.1 Revisión Documentada

En el mapa de procesos gestión organizacional en el ciclo de mejora continua tenemos los procesos estratégicos, procesos misionales, procesos de apoyo "Gestión de las Tecnologías de la información en el cual está inmerso esta auditoria" y los procesos de evaluación el cual debe cumplir con manuales, procedimientos, formatos, instructivos y políticas de seguridad que garanticen eficiencia en el rendimiento institucional.

MAPA DE PROCESOS



Fuente: https://www.uspec.gov.co/?page_id=309

2.2.2 Check List procesos OTEC

Procedimiento Gestión de Solicitudes de Soporte Técnico y Configuración de Redes

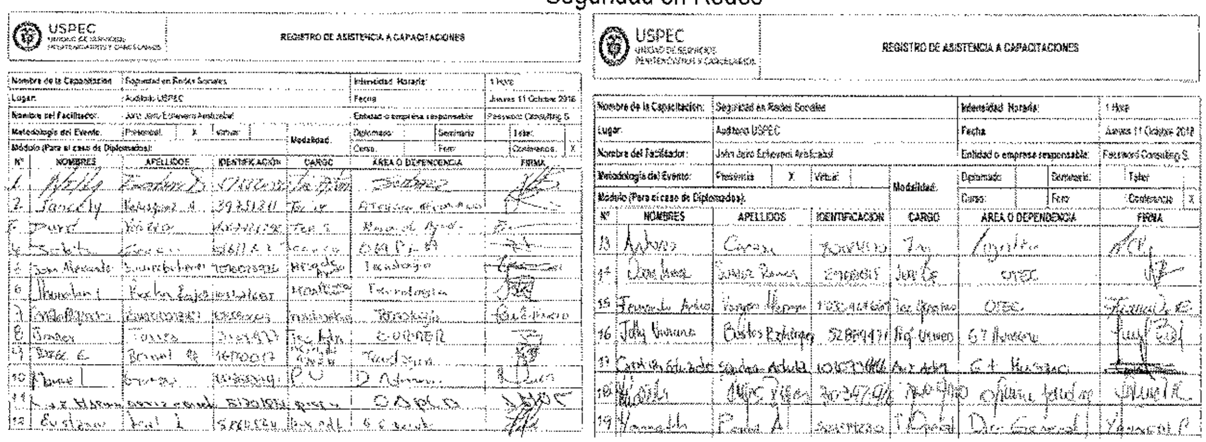
Fortalezas

- Se tiene definido el marco normativo del proceso Gestión de TIC´s y se ha socializado. Se evidencia en Página web SIGI el Normograma del proceso: https://www.uspec.gov.co/wp-content/uploads/2018/09/Normograma_2018-1.pdf

- Los servidores y /o contratistas responsables del proceso Gestión TIC´s han recibido capacitación relacionada sobre las políticas de seguridad informática entre los que se relacionan:

    - **Cybersecurity IMS ACADEMY desde el 29/10/2018 hasta 31/10/2018,**
    - **Conferencia Seguridad en Redes Sociales** (Anexo Listado de Asistencia)
    - **Conferencia Ingeniería Social** (Anexo Listado de Asistencia),
    - **Certificados ISO_22701 LL-C Services Colombia desde 24/09/2018 hasta 01/10/2018**
    - **Continuidad del Negocio IMS ACADEMY desde 16/10/2018 hasta 23/10/2018** (Auditor Interno ISO 22301:2012 Business Continuity)

Seguridad en Redes


USPEC — REGISTRO DE ASISTENCIA A CAPACITACIONES

Nombre de la Capacitación:	Seguridad en Redes Sociales	Intensidad Horaria:	1 Hora
Lugar:	Auditorio USPEC	Fecha:	Jueves 11 Octubre 2018
Nombre del Facilitador:	John Jairo Echeverri Arbeláez	Entidad o empresa responsable:	Password Consulting S.
Metodología del Evento:	Presencial X Virtual	Modalidad:	Diplomado / Seminario / Taller / Curso / Foro / Conferencia X
Módulo (Para el caso de Diplomados):			

Nº	NOMBRES	APELLIDOS	IDENTIFICACIÓN	CARGO	ÁREA O DEPENDENCIA	FIRMA
1	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
2	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
3	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
4	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
5	[illegible]	[illegible]	[illegible]	[illegible]	Tecnología	[illegible]
6	[illegible]	[illegible]	[illegible]	[illegible]	Tecnología	[illegible]
7	[illegible]	[illegible]	[illegible]	[illegible]	Tecnología	[illegible]
8	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
9	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
10	[illegible]	[illegible]	[illegible]	[illegible]	D. Admin.	[illegible]
11	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
12	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

Nº	NOMBRES	APELLIDOS	IDENTIFICACIÓN	CARGO	ÁREA O DEPENDENCIA	FIRMA
13	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
14	[illegible]	[illegible]	[illegible]	[illegible]	OTEC	[illegible]
15	[illegible]	[illegible]	[illegible]	[illegible]	OTEC	[illegible]
16	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
17	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
18	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
19	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

Fuente: OTEC

- Se cuenta con el procedimiento actualizado para la GESTIÓN DE SOLICITUDES DE SOPORTE TÉCNICO, se maneja el procedimiento escalando las solicitudes por responsable o funcionario encargado. Enlace: https://www.uspec.gov.co/wp-content/uploads/2018/02/A3-PR-01_Gestion_Solicitudes_Soporte_Tecnico_V02.pdf
- Se describe los contratos, estado, observaciones relacionados con la Implementación de las políticas de seguridad información que ha suscrito la entidad. Se anexan los últimos informes de supervisión.

    - Tres contratos 229 de 2015 Liquidado
    - 332 de 2016 Liquidado

- 160 de 2018 Ejecución (Anexo en carpeta soportes OTEC)

- Se actualiza el Formato Único de Inventario Documental FUID con los temas relacionados con los procedimientos de GESTIÓN DE SOLICITUDES DE SOPORTE TÉCNICO y CONFIGURACIÓN DE REDES WIFI dispositivos móviles, asistencia técnica donde se incluyen los mantenimientos. Y se encuentra en SIGI: https://www.uspec.gov.co/wp-content/uploads/2018/02/A3-PR-01_Gestion_Solicitudes_Soporte_Tecnico_V02.pdf (Anexo en carpeta soportes OTEC) No se ha reportado al Grupo Gestión Documental.
- Se cuenta con Tabla de Retención Documental de la Oficina de Tecnología que está actualizada con las series y tipos documentales de los temas relacionados con los procedimientos y la implementación de las políticas de seguridad informática; el archivo se dispone de forma local y cuando cumple el tiempo se almacena en el archivo central. Series, sub series, Donde se alojan las carpetas de acuerdo a los ítems. (Anexo en carpeta soportes OTEC)
- Avance de la definición de documentación del proceso Gestión de TIC´s (caracterización, manual, procedimientos, instructivos, formatos, indicadores, riesgos y normatividad). Los cuales se encuentran en el proceso de sistema de gestión donde se suben políticas procedimientos y manuales para la seguridad de la información Enlace: https://www.uspec.gov.co/?page_id=4477
- Los avances en cuanto a la definición e implementación de la política de seguridad información se encuentran publicados en la página web Información de Interés Políticas de seguridad de la información. https://www.uspec.gov.co/wp-content/uploads/2018/11/Politica_seguridad_informacion_USPEC.pdf
- Los Servicios de informática y tecnología que se encuentra tercerizados son los siguientes y se controlan de acuerdo al personal asignado

BACKUP DAR Soluciones. Mesa de ayuda, impresión, telefonía, cada funcionario tiene asignada un contrato: (Anexo en carpeta soportes OTEC)

Reporte BackUp DAR Soluciones

Log Backup IDRIVE

Activity Log ---------- SCAN REPORT ----------

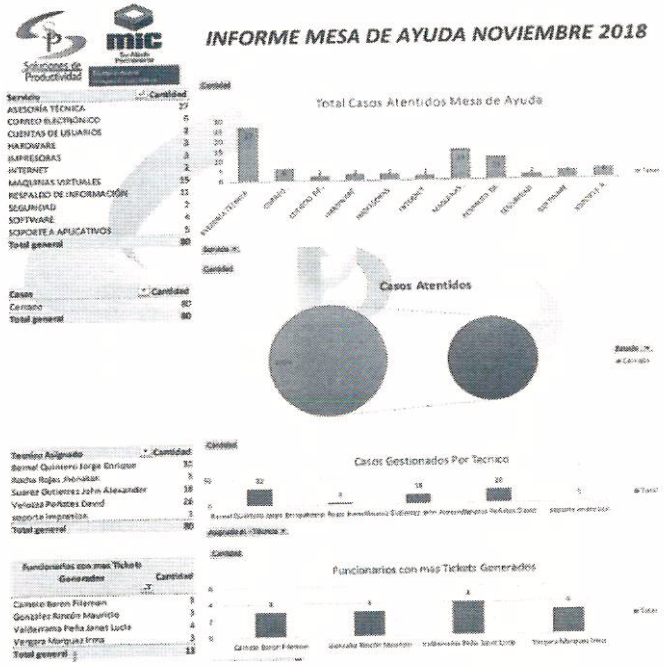
Operation	Date	Time In	Time Out	Status
Backup	1-6-2018	18:30:00	0:51:55	Successful
Backup	2-6-2018	18:30:00	1:07:09	Successful
Backup	3-6-2018	18:30:00	0:30:08	Successful
Backup	4-6-2018	18:30:00	0:59:13	Successful
Backup	5-6-2018	18:30:00	23:39:10	Successful
Backup	6-6-2018	18:30:00	1:34:38	Successful
Backup	7-6-2018	18:30:00	23:37:21	Successful
Backup	8-6-2018	18:30:00	22:47:35	Successful
Backup	9-6-2018	18:30:00	23:38:29	Successful
Backup	10-6-2018	18:30:00	0:38:54	Successful
Backup	11-6-2018	18:30:00	23:50:12	Successful
Backup	12-6-2018	18:30:00	0:43:09	Successful
Backup	13-6-2018	18:30:00	1:10:55	Successful
Backup	14-6-2018	18:30:00	0:21:08	Successful
Backup	15-6-2018	18:30:00	23:23:38	Successful
Backup	16-6-2018	18:30:00	23:40:48	Successful
Backup	17-6-2018	18:30:00	1:07:10	Successful
Backup	18-6-2018	18:30:00	22:58:59	Successful
Backup	19-6-2018	18:30:00	23:05:43	Successful
Backup	20-6-2018	18:30:00	1:48:35	Successful
Backup	21-6-2018	18:30:00	1:24:29	Successful
Backup	22-6-2018	18:30:00	23:44:09	Successful
Backup	23-6-2018	18:30:00	0:07:15	Successful
Backup	24-6-2018	18:30:00	0:30:53	Successful
Backup	25-6-2018	18:30:00	0:05:20	Successful
Backup	26-6-2018	18:30:00	1:37:46	Successful
Backup	27-6-2018	18:30:00	1:35:05	Successful
Backup	28-6-2018	18:30:00	1:18:27	Successful
Backup	29-6-2018	18:30:00	1:13:58	Successful
Backup	30-6-2018	18:30:00	22:47:48	Successful
Backup	1-7-2018	18:30:00	23:29:52	Successful
Backup	2-7-2018	18:30:00	23:37:28	Successful
Backup	3-7-2018	18:30:00	1:48:27	Successful
Backup	4-7-2018	18:30:00	0:04:04	Successful
Backup	5-7-2018	18:30:00	23:23:46	Successful
Backup	6-7-2018	18:30:00	0:18:42	Successful
Backup	7-7-2018	18:30:00	23:26:29	Successful
Backup	8-7-2018	18:30:00	1:57:08	Successful
Backup	9-7-2018	18:30:00	23:37:50	Successful
Backup	10-7-2018	18:30:00	23:54:55	Successful
Backup	11-7-2018	18:30:00	1:05:16	Successful
Backup	12-7-2018	18:30:00	22:56:29	Successful
Backup	13-7-2018	18:30:00	23:56:05	Successful
Backup	14-7-2018	18:30:00	0:30:40	Successful
Backup	15-7-2018	18:30:00	0:11:34	Successful
Backup	16-7-2018	18:30:00	0:32:40	Successful
Backup	17-7-2018	18:30:00	0:34:05	Successful
Backup	18-7-2018	18:30:00	22:49:45	Successful
Backup	19-7-2018	18:30:00	1:35:06	Successful
Backup	20-7-2018	18:30:00	1:58:03	Successful

Reporte Impresión

Contractual	3693	3693	1087
Control Interno	2	2	1
Dir.Financiera	130	130	15
Gestion Documental	14	14	6
Juridica 2 P4	24	24	7
P3_Bienes	565	565	134
Tecnologia	16	16	3
Tesoreria	2	2	2
Contractual	1167	1167	221
Control Interno	510	510	204
Infraestructura	2189	2189	488
Juridica 2 P4	3	3	2
P3_Bienes	4	4	3
Contractual	5	5	2
Control Interno	1265	1265	250
Dir.Financiera	115	115	3
Infraestructura	3940	3940	1033
P3_Bienes	4	4	1
Tecnologia	5	5	2
Tesoreria	41	41	6
Contractual	1845	1845	484
Juridica 2 P4	55	55	18
P3_Bienes	33	33	18
Contractual	3665	3665	445
Dir.Financiera	571	571	134
Juridica 2 P4	3	3	3
P3_Bienes	1658	1658	345
Contractual	1197	1197	338
Control Interno	373	373	137
Infraestructura	2985	2985	968
Juridica P4	12	12	1
P3_Bienes	7	7	3
Tesoreria	40	40	3
Contractual	7	7	2
Dir.Financiera	37	37	2
Tesoreria	171	171	50
Contractual	7	7	3
Dir.Financiera	2289	2289	720
Juridica 2 P4	15	15	8
Tesoreria	561	561	311
Infraestructura	26	26	4
Juridica 2 P4	3265	2509	848
Juridica P4	559	559	148
Contractual	50	50	28
Dir.Financiera	11	11	5
P3_Bienes	3990	3990	932
Tecnologia	30	30	17
P3_Bienes	7	7	3
ImpDirgen_Color	1	1	1
Juridica 2 P4	4	0	4
Tecnologia	1	0	1
-	**2023819**	**1995565**	**486168**
-	**4.163**	**4.105**	**-**

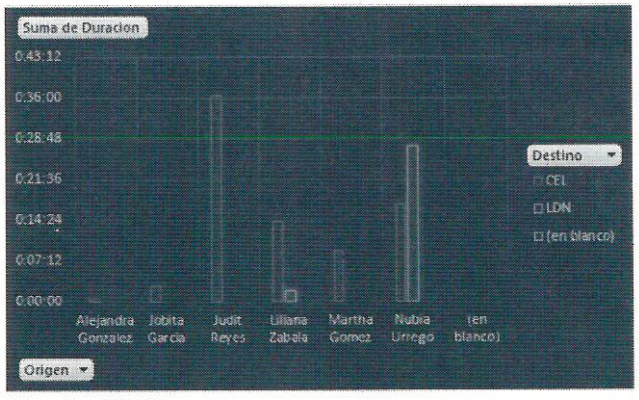
Fuente: OTEC

Reporte Mesa de Ayuda



Reporte Telefonía

Suma de Duracion	Etiquetas de columna			
Etiquetas de fila	CEL	LDN	(en blanco)	Total general
Alejandra Gonzalez	0:00:14			0:00:14
Jobita Garcia	0:02:47			0:02:47
Judit Reyes	0:36:24			0:36:24
Liliana Zabala	0:14:05	0:01:54		0:15:59
Martha Gomez	0:08:54			0:08:54
Nubia Urrego	0:17:09	0:27:23		0:44:32
(en blanco)				
Total general	**1:19:33**	**0:29:17**		**1:48:50**



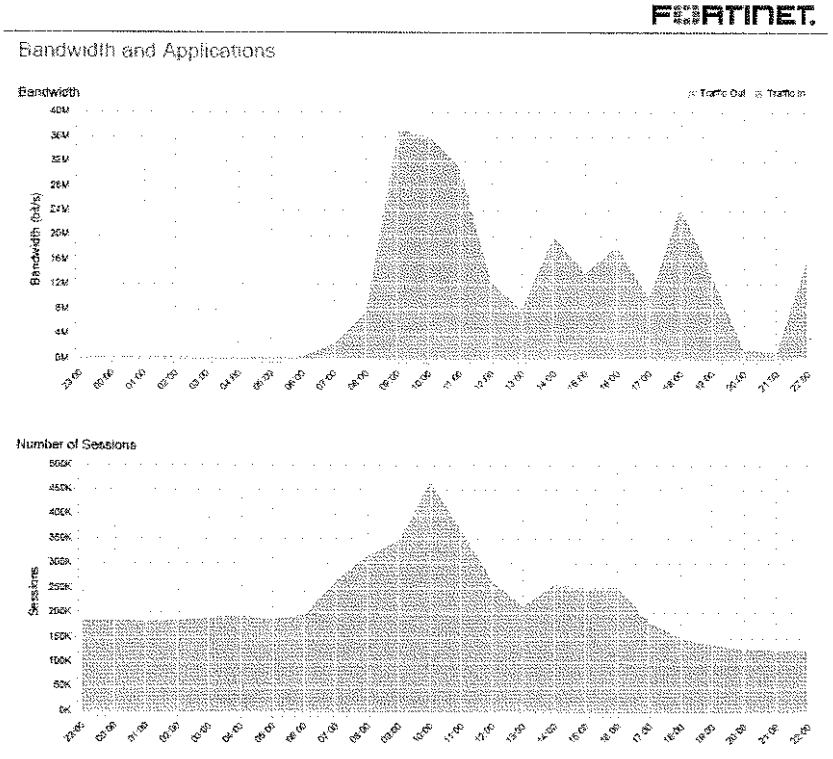
Fuente: OTEC

- Los controles físicos y lógicos se utilizaran para restringir y delimitar el acceso a la información sensible de la entidad son del edificio y el grupo administrativo, sin embargo mediante las políticas tiene controles lógicos por parte de la oficina de tecnología. Control de accesos a internet, que se definan por riesgos, categorías y se miden su desempeño mediante informes. ((Anexo en carpeta soportes OTEC)
- El resguardo de la información se realiza por La empresa **Dar Soluciones** la cual envía soportes de Backus diarios y copias de seguridad (Anexo en carpeta soportes OTEC)
- Se poseen las evidencias de control de redes (Anexo en carpeta soportes OTEC) se recomienda tener todos los nombres de los HostName definidos por aplicativos y responsables.

- Los controles establecidos para la implementación de políticas de seguridad informática de la entidad son los siguientes:

  - Fortigate – Filtra las conexiones de internet y redirige el tráfico y configuración de las reglas por los diferentes puertos VPN acceso a todo y los tipos de conexiones y accesos 3 VPN a sitios Millenium, Fiduprevisora, SCIEN Gobierno (Anexo en carpeta soportes OTEC)

Categoría Ancho de banda y Aplicaciones



Fuente: Reporte Fortinet

Categoría Sitios Web

Web Usage

Top Allowed Websites

Website	Requests
google.com	776.9 K
gstatic.com	155.0 K
m3hweb.com	82.3 K
live.com	57.5 K
doubleclick.net	18.4 K
fbcdn.net	16.1 K
gvt2.com	14.2 K
clientservices.googleapis.com	13.9 K
safebrowsing.googleapis.com	10.2 K
microsoft.com	10.0 K

Top Websites by Bandwidth

Website	Traffic Out / Traffic In
google.com	8.0 GB
googleusercontent.com	1.5 GB
googlevideo.com	1.1 GB
gvt1.com	943.2 MB
microsoft.com	847.4 MB
office.net	513.5 MB
fbcdn.net	413.2 MB
gstatic.com	379.3 MB
live.com	365.1 MB
facebook.com	286.6 MB

Top Blocked Websites

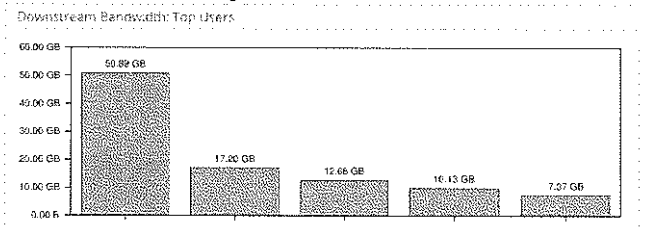
Website	Requests
facebook.com	14.7 K
youtube.com	6.4 K
dynamicyield.com	3.9 K
caracoltv.com	3.0 K
gvt3.com	2.3 K
gvt2.com	2.3 K
facebook.net	1.8 K
google.com	1.7 K
atwola.com	1.6 K
doubleclick.net	1.6 K

Fuente: Reporte Fortinet

- Reglas de seguridad filtrado web y aplicaciones de escritorio.

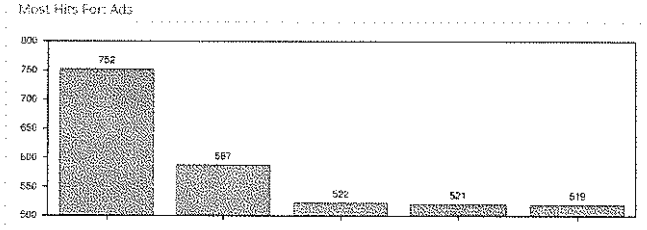
- I boss – Reglas de seguridad criterios por palabras categorías contenidos correos juegos sistema de prevención de intrusos. (Anexo en carpeta soportes OTEC)

Categoría Ancho de Banda



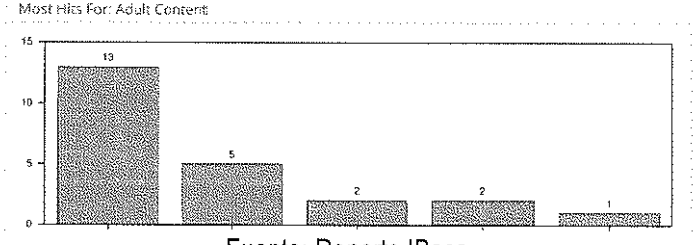
Fuente: Reporte IBoss

Categoría Anuncios



Fuente: Reporte IBoss

Categoría Adultos



Fuente: Reporte IBoss

- Correlacionado de eventos para anomalías de seguridad. (Faltan Anexar Evidencias)

Se recomienda sensibilizar mediante capacitaciones o charlas a los funcionarios que aportaron el mayor número de visitas web a la categoría contenido para adultos, los usuarios que pasaron la mayor parte del tiempo en la categoría Anuncios, los usuarios que consumieron el mayor ancho de banda descendente y ascendente durante ciertos periodos en los diferentes escenarios.

Se recomienda validar las solicitudes de acceso a las páginas para habilitar o denegar de acuerdo a su clasificación o servicio.

- Las acciones preventivas y correctivas que se tienen previstas para mejorar la implementación de las políticas de seguridad información en la entidad atienden las situaciones de acuerdo a los incidentes; gestión de vulnerabilidades se genera informe y se atienden de acuerdo a la complejidad. (Anexo en carpeta soportes OTEC)
-

Gestión de Vulnerabilidades

Responsable(s)	Cantidad de Activos	Vulnerabilidades Identificadas
Diana Cardenas / Jhonatan Rocha (MdA)	7	1271
Wilmer Abril	22	538
Gran Imagen (Juan Lizarazo)	13	331
ITS	1	236
Fernando Vargas	6	170
BIDDA / Natali Pedron	3	132
Ricardo Diaz	2	69
Alvaro Camargo / Ricardo Diaz	3	43
Alvaro Camargo	2	24
Ricardo Diaz / Fernando Vargas	2	22
Xertica (Proveedor GSuite)	1	3
Total	**61**	**2839**

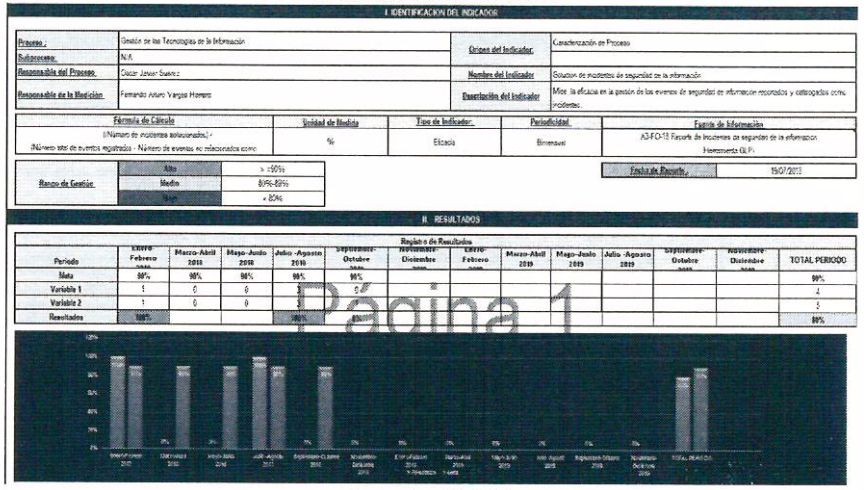
Nivel	Cantidad de Activos	Vulnerabilidades Identificadas
1. Bajo	59	511
2. Medio	55	1284
3. Alto	58	976
4. Extremo	18	68
Total	**61**	**2839**

TOTAL VULNERABILIDADES EXTREMAS Y ALTAS	
1044	
OTEC PASSWORD - (70%)	TERCEROS
775 - 543	269
TOTAL VULNERABILIDADES EXTREMAS Y ALTAS NO SOLUCIONADAS	
709	
USPEC PASSWORD	TERCEROS
574	135

Fuente: OTEC

- Se evalúa el impacto de la implementación de políticas de seguridad informática en materia de beneficios para la entidad mediante el cuadro de indicadores: Ejecución de proyectos, Solución de incidentes, Solución de soportes técnicos, solución de vulnerabilidades.

Solución de Incidentes



I. IDENTIFICACION DEL INDICADOR

Proceso :	Gestión de las Tecnologías de la Información	Origen del Indicador:	Caracterización de Proceso
Subproceso:	N.A.	Nombre del Indicador:	Solucion de incidentes de seguridad de la información
Responsable del Proceso:	Oscar Javier Suarez	Descripción del Indicador	Mide la eficacia en la gestión de los eventos de seguridad de información recortados y catalogados como incidentes.
Responsable de la Medición:	Fernando Arturo Vargas Herrera		

Fórmula de Cálculo	Unidad de Medida	Tipo de Indicador:	Periodicidad	Fuente de Información
(Número de incidentes solucionados) / (Número total de eventos registrados - Número de eventos no relacionados como	%	Eficacia	Bimestral	A3-FO-18 Reporte de Incidentes de seguridad de la información Herramienta GLPI

Rango de Gestión:		
	Alto	> 90%
	Medio	80%-89%
	Bajo	< 80%

Fecha de Reporte: 15/07/2019

II. RESULTADOS

Región de Resultados

Periodo	Enero-Febrero 2019	Marzo-Abril 2019	Mayo-Junio 2019	Julio -Agosto 2019	Septiembre-Octubre 2019	Noviembre-Diciembre 2019	Enero-Febrero 2019	Marzo-Abril 2019	Mayo-Junio 2019	Julio -Agosto 2019	Septiembre-Octubre 2019	Noviembre-Diciembre 2019	TOTAL PERIODO
Meta	80%	80%	80%	80%	80%								80%
Variable 1	1	0	0	1	0								4
Variable 2	1	0	0	1	0								5
Resultados	100%			100%									80%

Fuente: OTEC

2.2.3 Gobierno en Línea Segmentación Elementos Habilitantes: Arquitectura

- La entidad posee y mantiene actualizado el catálogo de servicios de TI con los Acuerdos de Nivel de Servicio (ANS) asociados.

Catálogo de servicios

USPEC	CATÁLOGO DE SERVICIOS DE TECNOLOGÍAS DE INFORMACIÓN		
Fecha de Actualización:	03 Noviembre de 2017	**Versión:**	1
Responsable:	Oficina de Tecnología		

CATEGORÍA	NOMBRE DEL SERVICIO	DESCRIPCIÓN
Internet	PUBLICACIÓN DE PÁGINA WEB	Publicación de contenido digital para usuarios internos y externos (informes, imágenes, videos, noticias, audios) en el portal web de la Entidad, emitido por las diferentes áreas de la USPEC.
	INTERNET	Habilitación de la conexión que permite un acceso controlado a la red mundial de datos desde los equipos de cómputo u otros dispositivos autorizados, para propósitos institucionales de la USPEC.
	CONEXIÓN INALAMBRICA WIFI	Autorización de la conexión de un dispositivo (PC, Celular, tablet, etc) a la red inalambrica de la Entidad.
	INTRANET	Servicio de difusión interna sobre la plataforma WEB de la Entidad, que permite la publicación de información institucional tal como circulares, políticas de seguridad información, galería de eventos, entre otros.
	CORREO ELECTRÓNICO	Servicio de mensajería electrónica para intercambio de información institucional por parte de los funcionarios de la Unidad, disponible en el portal WEB de la entidad.
Soporte tecnico	GESTIÓN DE CUENTAS DE USUARIOS	Autorización, administración y control del acceso de los usuarios a la red de datos y los servicios de TI de la USPEC.
	ASESORÍA TÉCNICA	Apoyo brindado en la definición de especificaciones técnicas para adquisición o contratación de hardware, software y servicios tecnológicos, por parte del INPEC y de las diferentes dependencias de la USPEC.
	PUBLICACIÓN DE DATOS ABIERTOS	Apoyo a las diferentes dependencias de la Entidad en la definición de sus conjuntos de datos, así como su publicación y actualización en la plataforma del gobierno nacional www.datos.gov.co
	MESA DE AYUDA	Soporte y asesoría a los funcionarios de la USPEC para solucionar los problemas básicos de funcionamiento de los equipos de cómputo de la Entidad (Hardware, software, conexiones).
	HERRAMIENTAS COLABORATIVAS	Apoyo técnico para realización de Foros, chats, encuestas y espacios comunes de almacenamiento digital.
	TELEFONÍA IP	Servicio de comunicación telefónica para funcionarios de la USPEC, a través de la red local de datos, para llamadas locales , nacionales e internacionales, según la autorización de cada usuario.
	IMPRESIÓN, ESCANEO Y FOTOCOPIADO	Apoyo a los funcionarios y contratistas de la USPEC para solucionar los problemas de funcionamiento del proceso de impresión, fotocopiado y escaneo.
	APOYO AL SISTEMA PQRD	Brindar soporte basico del aplicativo de PQRD, indicado por el Grupo de Atención al Ciudadano
Administración	RESPALDO DE INFORMACIÓN	Servicio a través del cual se resguarda la información institucional almacenada en las estaciones de trabajo de cada uno de los usuarios de la Entidad. (Funcionarios - Contratistas)
	REDES PRIVADAS VIRTUALES (VPN)	Autorización y configuración de conexiones con otras entidades, bien sea para acceder a un servicio o para autorizar el ingreso a un usuario especifico a la red de datos de la USPEC.
Desarrollo	DESARROLLO DE SOFTWARE	Desarrollo de herramientas tecnológicas de baja complejidad para solución de necesidades específicas de la Entidad.
	SOPORTE A APLICATIVOS	Soporte y asesoría a funcionarios de algunas dependencias de la USPEC para solución de problemas y mejoras de algunas aplicaciones de operación local en dichas dependencias.

Fuente: OTEC

- La entidad ha definido una política de TI y seguridad y privacidad de la información acorde con su contexto y misión, la cual ha sido aprobada por la alta dirección, la tiene implementada y las mantiene actualizada. Enlace Página web Política.: https://www.uspec.gov.co/?page_id=311 Todas las políticas Incluyendo la de seguridad de la información.
- La entidad aplica metodologías y criterios de evaluación para la selección de alternativas de solución tecnológicas, antes de realizar inversiones en Tecnologías de la Información (TI), buscando satisfacer las necesidades con la mejor relación costo/beneficio para la institución. Se analiza la necesidad del área en específico y real, se crea la ficha técnica, (Anexo en carpeta soportes OTEC)
- La entidad aplica siempre un proceso o procedimiento de control de cambios cuando se requiere realizar una nueva funcionalidad, ajuste o corrección en los sistemas de información que se encuentran en producción. Enlace: Página Web SGSI: https://www.uspec.gov.co/wp-content/uploads/2018/02/A3-PR-13_Control_de_Cambios_V01.pdf
- La Entidad tiene establecido y aplica un los mantenimientos preventivo y correctivo de los sistemas de información pero se recomienda crear el procedimiento. El mantenimiento correctivo se aplica con una frecuencia definida, según el plan de mantenimientos de la entidad. cumple con las funcionalidades de accesibilidad que indica la Política de gobierno Digital, en los sistemas de información que están disponibles para el acceso a la ciudadanía o aquellos que de acuerdo a la caracterización de usuarios lo requieren. Enlace transparencia a la Información: https://www.uspec.gov.co/?page_id=11079 Enlace Gobierno en Línea: https://www.uspec.gov.co/?page_id=314

Debilidades

- No se ha medido el nivel de satisfacción de las dependencias de la entidad que han recibido los beneficios de la implementación de políticas de seguridad.
- La entidad No posee documentada su estrategia en materia de Tecnologías de la Información en el Plan estratégico de Tecnologías de la Información y lo mantiene actualizado.
- No se ha actualizado el PETI en todos los niveles de la entidad, No se difunde y se trabaja en la apropiación.
- No se ha desarrollado la capacidad de Arquitectura empresarial a través de la realización de uno o más ejercicios de Arquitectura empresarial ya sea institucionales o de proceso.
- No se cuenta con un grupo de Arquitectura empresarial que gobierna y toma decisiones frente al impacto o evolución de la arquitectura empresarial al interior de la entidad. Este grupo depende del Comité de Gestión y Desempeño Institucional.
- No se tiene definidos, no se mide y no se hace seguimiento a indicadores de gestión de TI y seguimiento a la estrategia de TI a través de tableros de control automatizados.
- No se ha definido ni tiene implementado un esquema de Gobierno TI alineado con la estrategia misional y con el Modelo Integrado de Planeación y Gestión. Se han realizado las reuniones para la toma de decisiones respecto a la información. Pero no se han concretado.
- No se realizan proyectos de TI no realiza monitoreo y evaluación de desempeño de la gestión, proyectos y estrategia de TI a través de mediciones y monitoreo de indicadores.

- La entidad no posee documentada la arquitectura de información. (dentro de la arquitectura incluye los datos georreferenciados si posee)
- No posee servicios de información dispuestos para ser consumidos por otras entidades públicas, los cuales incorporan y aplican el lenguaje común de intercambio definido por el Estado.
- No se han definido fuentes únicas de información, para un acceso oportuno, confiable, completo y veraz de los datos e información que almacena y procesa.
- No todas las aplicaciones de software de la entidad poseen funcionalidades de trazabilidad y auditoría de transacciones o acciones de creación, actualización, modificación o borrado de información. Las que se tramitan se realizan seguimientos mediantes actas (Anexo en carpeta soportes OTEC)
- No se aplica en el desarrollo software para la entidad metodologías de software ágiles.
- No se encuentran actualizados en la entidad los sistemas de información cuenten con la documentación técnica y funcional debidamente actualizada.
- No se tiene integrados sus sistemas internos de información estratégica, misional y de apoyo con el sistema de gestión documental electrónica de archivo para la toma de decisiones.
- No se ha implementado sistemas de información que generan datos abiertos, poseen funcionalidades que permiten la generación de datos abiertos de forma automática en el portal de datos.gov.co
- No se ha definido e implementado un programa de correcta disposición final de los residuos tecnológicos de acuerdo con la normatividad del gobierno nacional.
- La entidad no ha implementado capacidades de alta disponibilidad para las infraestructuras críticas que posee y los Servicios Tecnológicos que afecten la continuidad de los servicios de la institución, las cuales deben son puestos a prueba periódicamente.
- No se ha definido y ejecutado un plan de formación que incorpore el desarrollo de competencias requeridas por los profesionales de TI y de los funcionarios de la entidad para hacer un uso adecuado de los servicios de TI.

2.2.4 **Gobierno en Línea** segmentación Elementos Habilitantes: Seguridad de la Información

- La Unidad desarrolla una autoevaluación de estado actual de seguridad de la información al interior de la entidad (diagnóstico) todo se rige por la herramienta que define MINITIC Diagnostico de seguridad.

- Las entidades de este nivel deben desarrollar y apropiar una de la política de seguridad de la información para el caso de la USPEC se encuentra en la página publicada y se va a socializar y sensibilizar: https://www.uspec.gov.co/?page_id=311

- Se requiere desarrollar y apropiar un gobierno de seguridad de la información que incluya Roles y Responsabilidades, inclusión de la seguridad de la información en los Comités Directivos, procedimientos de gestión de seguridad de la información, políticas de seguridad de la información y se encuentra Inmerso en la política y en SGSI y evaluando las nuevas versiones.

- La USPEC desarrolla y apropia un gobierno de seguridad de la información que incluya Roles y Responsabilidades, inclusión de la seguridad de la información en los comités directivos, procedimientos de gestión de seguridad de la información, políticas de seguridad de la información y se encuentra inmerso en la política de SGSI.

- La USPEC desarrolla y apropia una metodología de gestión de activos, y cuenta con un inventario de activos de todos los procesos o áreas de la entidad

- Se desarrolla un plan de mejoramiento continuo que determine las causas de las no conformidades potenciales, las cuales permitan identificar acciones necesarias mejora, y posteriormente revisar la oportunidad de la acción tomada donde se definió un plan general para solucionar las no conformidades producto de la auditoría realizada en 2017. Se encuentra pendiente realizar seguimiento para verificar el cierre de las mismas.

- La USPEC debe desarrollar e integrar un plan de Auditorias de seguridad de la información en el cual se tiene previsto realizar auditoria al SGSI en el mes de enero de 2019. La última se realizó en febrero de 2017.

- No se posee Plan de control y operación de la seguridad de la información

- No se tiene Plan de Seguimiento y evaluación a la implementación del plan de tratamiento de riesgos que permita verificar la efectividad de los controles establecidos en todos los procesos de la entidad

- La re-evaluación de los riesgos desarrollada en la entidad, donde a su vez se validen los niveles aceptables de riesgo y el riesgo residual después de la aplicación de controles técnicos y medidas administrativas. Se realizó la reevaluación de riesgos de seguridad pero a partir de los controles existentes, los nuevos controles para mitigar riesgos se definieron después de identificar el riesgo residual.

3. OBSERVACIONES

Aspectos a fortalecer en la gestión tecnológica.

Plan de Pruebas para Desarrollos, Actualizaciones, Configuraciones, y Tratamiento de vulnerabilidades. Plan De Contingencia Desastres. Falta de supervisión en los formatos de control de dispositivos, habilitación de puertos USB y control de usuarios (establecer necesidades y priorizaciones reales de usuarios), actualizar el Normograma con las últimas normas que rigen al área de Tecnología. Establecer un formato para la creación de las fichas técnicas.

4. RECOMENDACIONES

Es necesario establecer en la entidad, las responsabilidades de los diferentes procesos que tiene la Oficina de Tecnología. Los responsables de cada actividad, deben generar informes donde se puedan mediar las estadísticas y avances en el apoyo a los procedimientos OTEC.

5. HALLAZGOS ENCONTRADOS

No. Hallazgo	Causa	Descripción del hallazgo
Debilidades e incumplimiento en el Procedimiento Gestión de Solicitudes de Soporte Técnico y Configuración de Redes	Por establecer por la dependencia responsable del proceso	▪ No se ha medido el nivel de satisfacción de las dependencias de la entidad que han recibido los beneficios de la implementación de políticas de seguridad. ▪ No se ha actualizado el PETI en todos los niveles de la entidad, No se difunde y se trabaja en la apropiación. ▪ No se ha desarrollado la capacidad de Arquitectura empresarial a través de la realización de uno o más ejercicios de Arquitectura Empresarial ya sea institucionales o de proceso. ▪ No se tiene definidos, no se mide y no se hace seguimiento a indicadores de gestión de TI y seguimiento a la estrategia de TI a través de tableros de control automatizados. ▪ No se ha definido ni tiene implementado un esquema de Gobierno TI alineado con la estrategia misional y con el Modelo Integrado de Planeación y Gestión. ▪ La entidad no posee documentada la arquitectura de información. ▪ No se ha definido fuentes únicas de información, para un acceso oportuno, confiable, completo y veraz de los datos e información que almacena y procesa. ▪ No todas las aplicaciones de software de la entidad poseen funcionalidades de trazabilidad y auditoria de transacciones o acciones de creación, actualización, modificación o borrado de información. Las que se tramitan se realizan seguimientos mediantes actas (Anexo en carpeta soportes OTEC) ▪ No se tiene integrados sus sistemas internos de información estratégica, misional y de apoyo con el sistema de gestión documental electrónica de archivo para la toma de decisiones. ▪ No se ha implementado sistemas de información que generen datos abiertos

		▪ No se ha definido e implementado un programa de correcta disposición final de los residuos tecnológicos de acuerdo con la normatividad del gobierno nacional. ▪ No se ha definido y ejecutado un plan de formación que incorpora el desarrollo de competencias requeridas por los profesionales de TI y de los funcionarios de la entidad para hacer un uso adecuado de los servicios de TI.
Incumplimiento parcial del Programa Estrategia de Gobierno en Línea	Por establecer por la dependencia responsable del proceso	▪ No se posee Plan de control y operación de la seguridad de la información ▪ No se tiene Plan de Seguimiento y evaluación a la implementación del plan de tratamiento de riesgos que permita verificar la efectividad de los controles establecidos en todos los procesos de la entidad ▪ La re-evaluación de los riesgos desarrollada en la entidad, donde a su vez se validen los niveles aceptables de riesgo y el riesgo residual después de la aplicación de controles técnicos y medidas administrativas. Se realizó la reevaluación de riesgos de seguridad pero a partir de los controles existentes, los nuevos controles para mitigar riesgos se definieron después de identificar el riesgo residual.

Jhonnier Yesid Zúñiga Mosquera
Auditor Interno

Vo. Bo. Jose Jorge Roca M.
Jefe Oficina de Control interno