Comisión Nacional del Servicio Civil CNSC IGUALDAD, MÉRITO Y OPORTUNIDAD	INFORME DE AUDITORIA	**Código:** F-ES-005
		Versión: 4.0
		Fecha: 25/06/2018
		Página: 1 de 1

	Preliminar		Definitivo	X	**Fecha de Emisión del Informe**	09	23	2019

1. INFORMACIÓN GENERAL	
Proceso (s) Auditado (s):	Gestión de las tecnologías de la Información, gestión de los recursos tecnológicos y normas aplicables de la CNSC
Actividad (es) auditada (s):	-Gestión y operación de la infraestructura tecnológica P-RT-001 -Caracterización Proceso Gestión de Tecnologías de la Información Código C-TI-001 Versión 2 del 7 de sep. de 2016. -Mantenimiento de soluciones informáticas P-RT-002 -Procedimiento ANS universidades - P-TI-002 -Mesa de servicios P-RT-003 -Procedimiento Adquisición y Crecimiento de Infraestructura - P-IT-003 -Procedimiento recibo de discos duros universidades - P-TI-004 - Matriz_Consolidada_Riesgos_OAI. -Plan de mejoramiento sobre el informe de auditoría *Desarrollo de Software y Gestión de Cambios* -Diagnóstico del estado de la implementación del SGSI -Evaluación Sistema de Información SIMO
Dependencia:	Oficina Asesora de informática
Líder del Proceso / Jefe(s) Dependencia(s):	Gustavo Adolfo Vélez Achury
Objetivo de la Auditoría:	Evaluar la administración del riesgo, el diseño y efectiva operatividad en la aplicación de controles y el cumplimiento de la normativa externa e interna aplicable a los procesos de Gestión de tecnologías de la información y Gestión de Recursos Tecnológicos, incluso a las actividades de aprovisionamiento, instalación, configuración, diagnóstico, mantenimiento y aseguramiento de recursos tecnológicos como apoyo a la gestión de las operaciones y procesos de la CNSC.
Objetivos Específicos:	-Evaluar el diseño y la eficacia operacional de los controles internos de los procesos auditados. -Identificar oportunidades de mejoramiento que permitan agregar valor a los procesos. -Verificar que se cumplan las normas y políticas de los procedimientos - Presentar un diagnóstico del estado actual del Modelo de Seguridad de la Información

	-Seguimiento a las acciones derivadas del último informe F-ES-005 realizado el pasado 25/06/2018 - Evaluar las fortalezas y debilidades del Sistema de Información SIMO.
Marco Normativo:	Ley 23 de 1982 Ley 962 de 2005 Ley 1273 de 2009 Ley 1581 de 2012 Ley 1266 de 2008 Ley 1712 de 2014 Resolución 305 de 2008 Decreto 1499 de 2017 NTC 5854 Accesibilidad Decreto 1078 de 2015 NTC-5854 Accesibilidad NTC ISO/27001:2013 Mapas de riesgos Las demás normas concordantes y aplicables
Alcance:	El alcance previsto para este trabajo de auditoría comprende la evaluación de los controles internos, la identificación de oportunidades de mejora y la evaluación del grado de conformidad con el Sistema Integrado de Gestión; Sistema de la seguridad de la Información bajo los requisitos de la NTC-IEC- ISO 27001:2013 de Oficina Asesora de Informática, para los Procesos: Gestión de Tecnologías de Información y Gestión de Recursos Tecnológicos.

Fecha Reunión de Apertura			**Vigencia Auditada**	1 de junio de 2018 al 30 de junio de 2019
17	**07**	**2019**		

Auditor Líder	**Auditor (es) de Apoyo**
Luz Marlenny Cano Romero	N/A

2. SITUACIONES DETECTADAS DURANTE EL PROCESO DE AUDITORÍA

2.1 Resumen de la auditoría

En cumplimiento del Programa Anual de Auditoría para el año 2019, aprobado por la Secretaria General, la Oficina de Control Interno da inicio a la auditoria de informática mediante el contrato No. 319 de 2019 cuyo objeto: "*Prestar servicios profesionales .... Para adelantar auditoria a los procesos de gestión de las tecnologías de la información y gestión de recursos tecnológicos de la comisión Nacional del Servicio civil de acuerdo a las metodologías establecidas para tal fin*".

El desarrollo de la auditoria se realizó en tres fases de la siguiente manera:

- **Planificación:**

Dentro de esta etapa, se desarrollaron varias actividades relacionadas a continuación:

Entendimiento:

Se llevó a cabo el entendimiento general de la Oficina Asesora de Informática y de los procesos objeto de la auditoría, para identificar entre otros:

- Los documentos aplicables (Caracterizaciones, procedimientos, formatos, responsabilidades y estructura organizacional de la Oficina).
- Controles generales de tecnologías en las aplicaciones y las plataformas tecnológicas donde operan.
- Los Principales módulos que conforman las aplicaciones y actividades que soportan los procesos.
- Esquema de seguridad de las aplicaciones y sus plataformas tecnológicas.
- Aplicabilidad del Sistema de Gestión de Seguridad de la Información (SGSI)
- Definición Plan de Auditoría y Plan de pruebas:

De acuerdo con el entendimiento obtenido en la fase anterior y las expectativas de la entidad, se diseñó el plan de trabajo cuyo contenido correspondió a diferentes pruebas de recorrido, de modo que a través de su ejecución permitieran determinar la existencia, funcionalidad y aplicación de controles y requisitos identificados para el proceso logrando así el cumplimiento de los objetivos y el alcance definido.

Las pruebas definidas para la evaluación de los controles generales de tecnología para la infraestructura tecnológica y desarrollo y mantenimiento de aplicaciones de la CNSC se realizaron con base en la metodología definida por la Entidad para la realización de auditorías, bajo el enfoque ISO:27001:2013 y bases de datos de buenas prácticas de seguridad.

- **Ejecución**

La ejecución del plan incluyó la realización de pruebas de diseño e implementación, documentación y análisis de los resultados; dependiendo de la actividad de control a probar en cada caso, se utilizaron procedimientos de revisión que a juicio fuera el más efectivo, como revisión directa de los sistemas, muestreos, pruebas sobre datos, evaluación y verificación de documentación entre otros.

Fue solicitada la información objeto de la auditoría para seleccionar muestras con el fin de validar los controles claves y requisitos establecidos en el proceso. Lo anterior mediante la aplicación de pruebas de observación, indagación, y comparación dado el alcance de la auditoría.

Adicionalmente, se ejecutaron las listas de chequeo diseñadas para probar los controles y constatar las actividades adelantadas en materia de implementación del Sistema de Seguridad de la información.

Como parte del proceso de comparación entre el criterio (estado correcto del requisito) y la condición (estado actual) se evidenció que se presentaron diferencias que se tomaron como base para elaborar el informe.

- **Finalización**

En esta etapa se realizaron las siguientes actividades:

➢ Presentación de Resultados y radicación del Informe

El 13 de septiembre de 2019 será socializado el informe con el líder del proceso con el objetivo de validar cada uno de los hallazgos, /oportunidades de mejora evidenciadas, de igual manera, fueron socializadas las recomendaciones que permitan definir y ejecutar planes de mejora necesarios para mitigar y administrar los riesgos identificados.

➢ Plan de mejoramiento

Se reiteró durante la reunión de cierre que, para la implementación de las acciones correctivas, preventivas y/o de mejora derivadas del presente informe, los responsables del proceso, como parte del mejoramiento continuo, deben elaborar y presentar a la Oficina de Control Interno, el plan de mejoramiento de acuerdo con los lineamientos definidos por la Entidad y descritos en la última parte del presente informe.

2.2. Desarrollo de la Auditoria

2.2.1. Riesgos Identificados del proceso Evaluado

Durante el entendimiento de los procesos y la revisión documental, así como al análisis del mapa de riesgos, la Oficina de Control Interno, identificó los riesgos registrados a continuación:

- ✓ Insatisfacción de los usuarios de la entidad.
- ✓ Fallo o no disponibilidad de la plataforma misional
- ✓ Fallo o no disponibilidad de la red de datos interna e Internet.
- ✓ Adoptar un enfoque tecnológico incompatible con las necesidades y misión de la entidad.
- ✓ Fallo o no disponibilidad de los ambientes web de la entidad.
- ✓ Fallo o no disponibilidad de la aplicación SIMO de la CNSC para celulares.
- ✓ No disponibilidad de los sistemas de información de la entidad por fallos o insuficiencia eléctrica.
- ✓ Fallo o no disponibilidad de la plataforma de gestión.

2.2.2 Actividades específicas realizadas

Durante el desarrollo de la auditoria se realizó las siguientes acciones cumpliendo con el cronograma del proyecto.

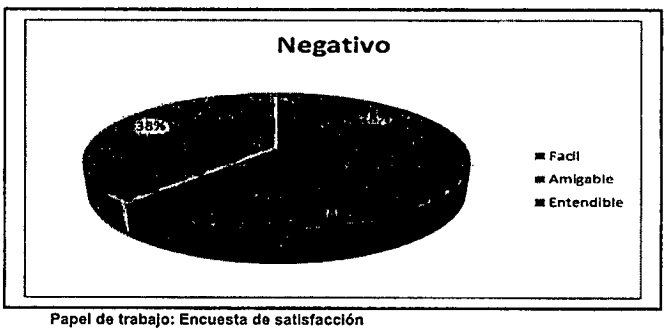
a) **Procedimientos: Gestión de tecnologías de la información y gestión de recursos tecnológicos:**
Se verificó el cumplimiento frente a los objetivos, alcance, normatividad, políticas de operación y desarrollo de procedimiento de los procesos; evidenciando debilidades tanto en el diseño, como en actualización y aplicación de los mismos, los cuales serán presentados en el numeral 2.2 ***Hallazgos y/o No Conformidades*** de este informe.

Encuesta de satisfacción : Se realizó por la intranet de la CNSC, los días 5,6 y 8 de agosto de 2019, una encuesta de satisfacción del usuario, con el fin de evaluar el servicio que presta la Oficina Asesora de Informática a través del aplicativo GLPI. Con lo anterior, se obtuvieron los siguientes resultados para 63 cuestionarios diligenciados:

1. Para el registro de un servicio (incidente y/o requerimiento) el acceso y el diligenciamiento para la solicitud es: [Fácil, amigable, entendible]

Calificativo	No
Fácil	32
Amigable	38
Entendible	43

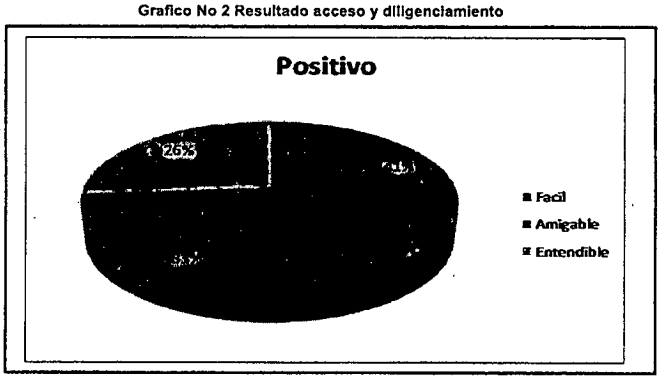
Grafico No 1Resultado acceso y diligenciamiento



Papel de trabajo: Encuesta de satisfacción

Calificativo	Si
Fácil	31
Amigable	25
Entendible	20

Grafico No 2 Resultado acceso y diligenciamiento



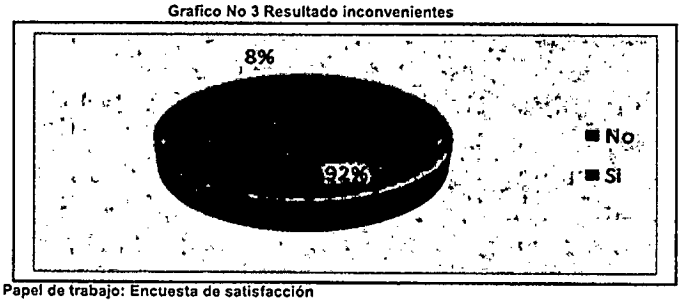
Papel de trabajo: Encuesta de satisfacción

2. Presenta inconvenientes para el registro de un servicio (incidente y/o requerimiento), el

acceso y el diligenciamiento de una solicitud?

No	58
Si	5
Total realizó	63

Grafico No 3 Resultado inconvenientes



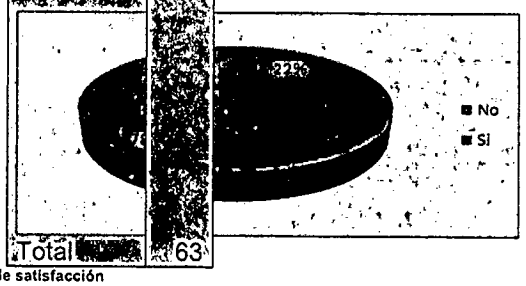
Papel de trabajo: Encuesta de satisfacción

"En algunas ocasiones es difícil determinar cuál es la categoría adecuada para el servicio que se requiere".

3. ¿Al momento de crear la solicitud, usted tiene claro al seleccionar, si es un incidente o requerimiento?

Grafico No 4 Resultado seleccionar

No	14
Si	49
Total	63



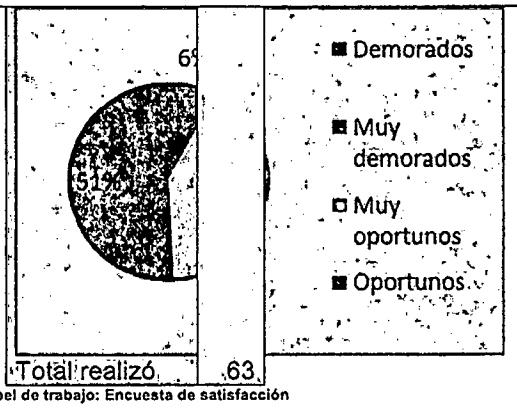
Papel de trabajo: Encuesta de satisfacción

Porque: *El aplicativo no describe los casos que se consideran requerimiento o incidente*
Nunca se me ha informado cuando es un requerimiento y cuando es un incidente
No está la definición de esta clasificación publicada.

4. ¿Cómo califica los tiempos de respuesta de la atención de los servicios que ha solicitado a través de GLPI en los últimos seis meses?

Grafico No 5 Resultado tiempos de respuesta

Demorados	4
Muy demorados	1
Muy oportunos	26
Oportunos	32

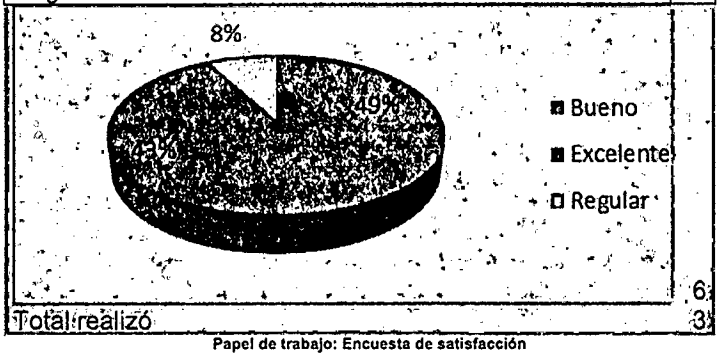


Papel de trabajo: Encuesta de satisfacción

5. ¿Cómo califica los tiempos de respuesta de la solución de los servicios que ha solicitado a través de GLPI, los últimos seis meses?

Grafico No 6 Resultado solución de servicios.

Bueno	31
Excelente	27
Regular	5

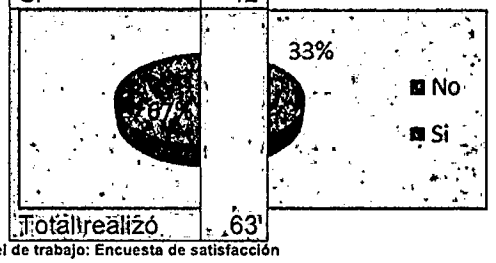


Papel de trabajo: Encuesta de satisfacción

6. ¿Ha recibido atención de requerimientos sin necesidad de ser reportados a través del acceso GLPI, para casos de extrema urgencia?

Grafico No 7 Resultado requerimientos

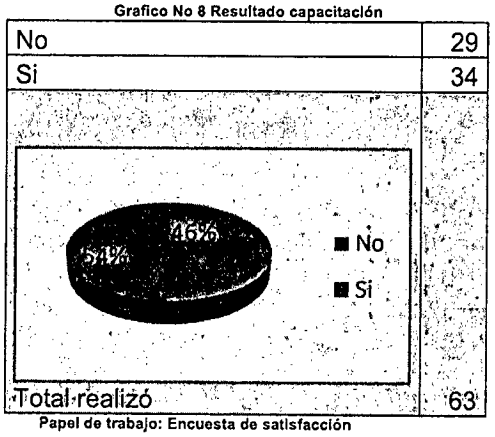
No	21
Si	42



Papel de trabajo: Encuesta de satisfacción

7. Cuando ingresó a la CNSC, ¿Le compartieron capacitación para el reporte de un servicio?

Grafico No 8 Resultado capacitación



Papel de trabajo: Encuesta de satisfacción

8. ¿Qué aspectos usted considera que se deban mejorar para prestación de un servicio por GLPI?

- ✓ *Una capacitación para las personas que ingresan a la entidad, con el ánimo de tener conocimiento y manejo del aplicativo.*
- ✓ *Que se realice un mejor seguimiento a las soluciones.*
- ✓ *facilitar el lenguaje de las categorías para tipificar la clase de requerimiento o incidencia, de la lectura de las categorías es fácil entender, pero no es fácil elegir cual es la adecuada.*
- ✓ *La distribución de casos entre los ingenieros.*
- ✓ *Considero que las tipologías disponibles deben revisarse para que sea de fácil comprensión para los usuarios a que hace referencia cada una de ellas.*
- ✓ *Mejorar la interacción de los documentos compartidos, es decir que sea más fácil el acceso de los documentos que cuelgan como respuesta.*
- ✓ *respuesta, indicando el tiempo aproximado que se tardará el equipo en brindar solución al requerimiento, así no se tiene incertidumbre sobre la misma.*

b) Evaluación del Sistema de información SIMO a los tres (3) módulos:

SIMO CUIDADANO SIMO IES SIMO OPEC

Lo anterior frente a las siguientes definiciones:

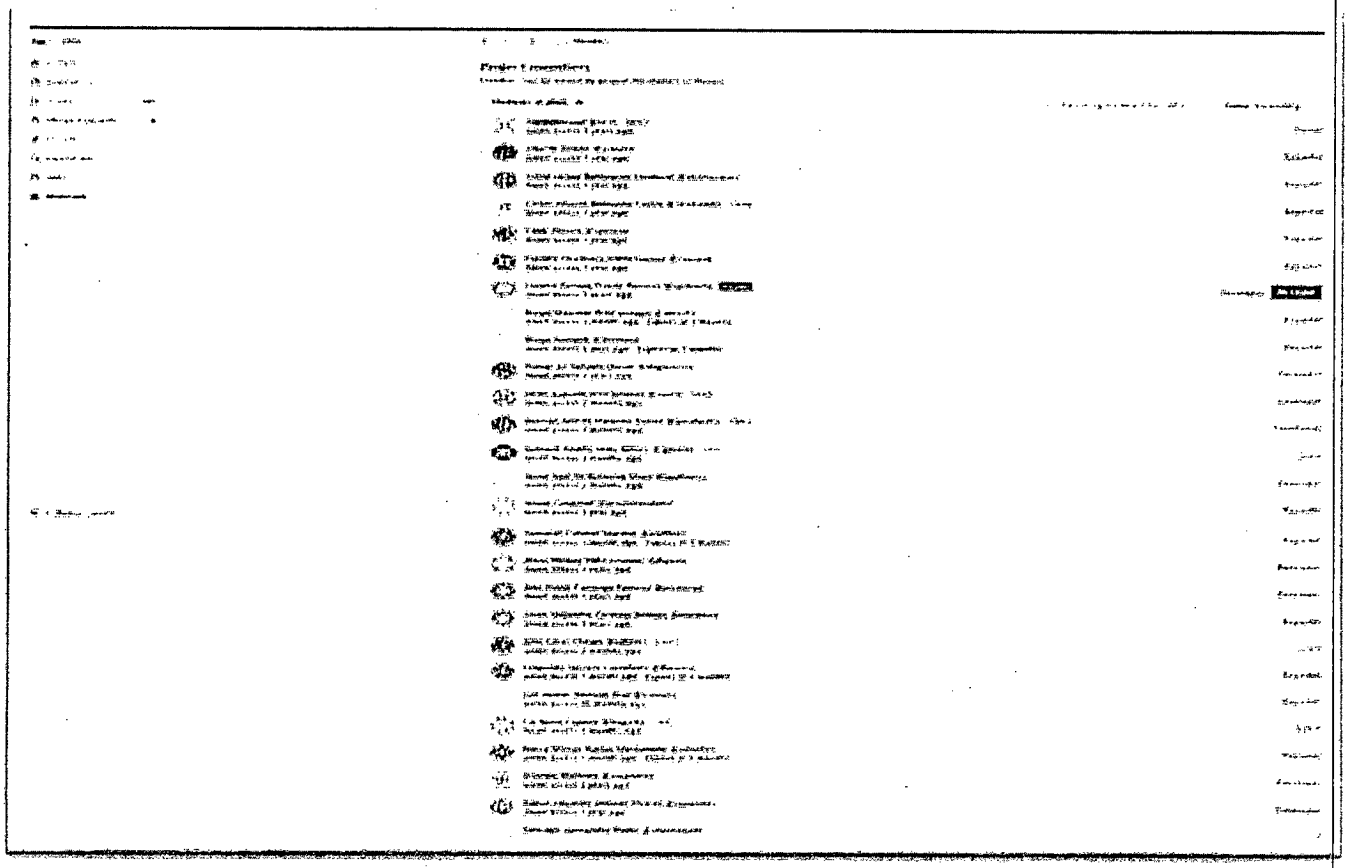
Confidencialidad de la Información:

Para el aplicativo SIMO, la confidencialidad de la información, está basada en la adecuada segregación de funciones establecidas a nivel de roles y perfiles, por los diferentes administradores de la herramienta, permitiendo así, que cada usuario determine sus propios procesos y/o actividades.
Lo anterior se pudo observar mediante la herramienta GITLAB que es la utilizada por el equipo

del proyecto SIMO para el desarrollo de los requerimientos y/o funcionalidades requeridas frente a cada módulo, dado que es un servicio web de control de versiones y desarrollo de software colaborativo.

Así mismo, se encontró que son administrados adecuadamente los permisos de los usuarios y se les da acceso sólo al/los proyectos a los que se encuentran designados, se les asigna un nivel de acceso: invitado (guest), reporter, developer o maintainer, así como el tipo de permisos a otorgar a cada uno de estos niveles de acceso, de la siguiente manera: desde el acceso más básico, que es solo de lectura, hasta el que se pueden cargar incidencias, escribir códigos, entre otros, hasta el nivel de maintainer que es el superusuario (que significa super usuario). Incluso se pueden restringir los permisos a un usuario para que tengan una fecha límite como se presenta a continuación en la siguiente grafica tomada de la herramienta:

Grafica N.8 Roles Administrador SIMO



Fuente: Herramienta GITLAB, capturada el xx de 2019

Adicionalmente, la Base de datos del SIMO se encuentra encriptada, por lo tanto los usuarios de la aplicación tienen encriptada sus contraseñas de acceso en la Base de Datos (BD), impidiendo que sean modificadas o copiadas fácilmente, evitando posibles vulnerabilidades al respecto.

Los archivos que se cargan al sistema tienen un método de seguridad el cual opera asignando un código HASH (encriptado) que es único para cada archivo haciéndolo inmodificable.

Integridad de la Información.

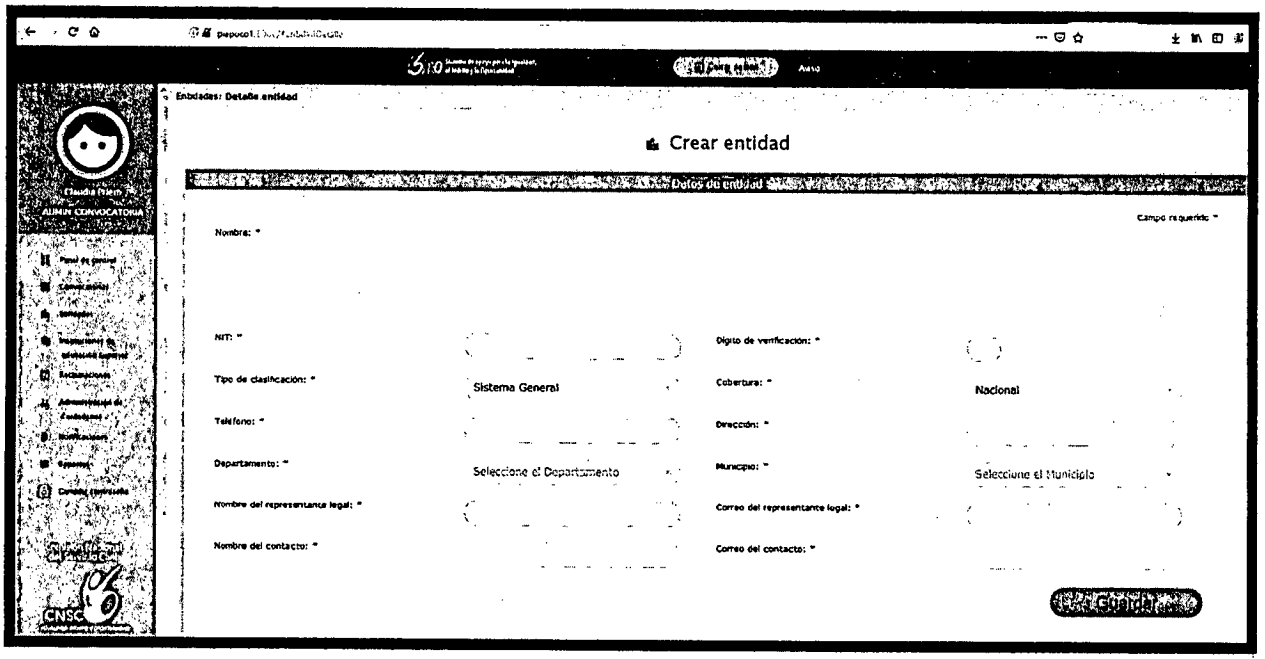
- El registro de los datos, se realiza por los ciudadanos a través del módulo SIMO-Ciudadano, la modificación de los datos básicos, de experiencia, formación o la requerida (Información personal), se realiza directamente por cada usuario registrado. Así mismo al presentarse algún tipo de aclaración dicho usuario podrá acceder a las ayudas visuales y auditivas con las que cuenta la herramienta, tal como se muestra a continuación:

- Se cuenta con un registro de auditoria por Base de Datos, permitiendo tener trazabilidad de las acciones realizadas sobre los objetos en la base de datos.

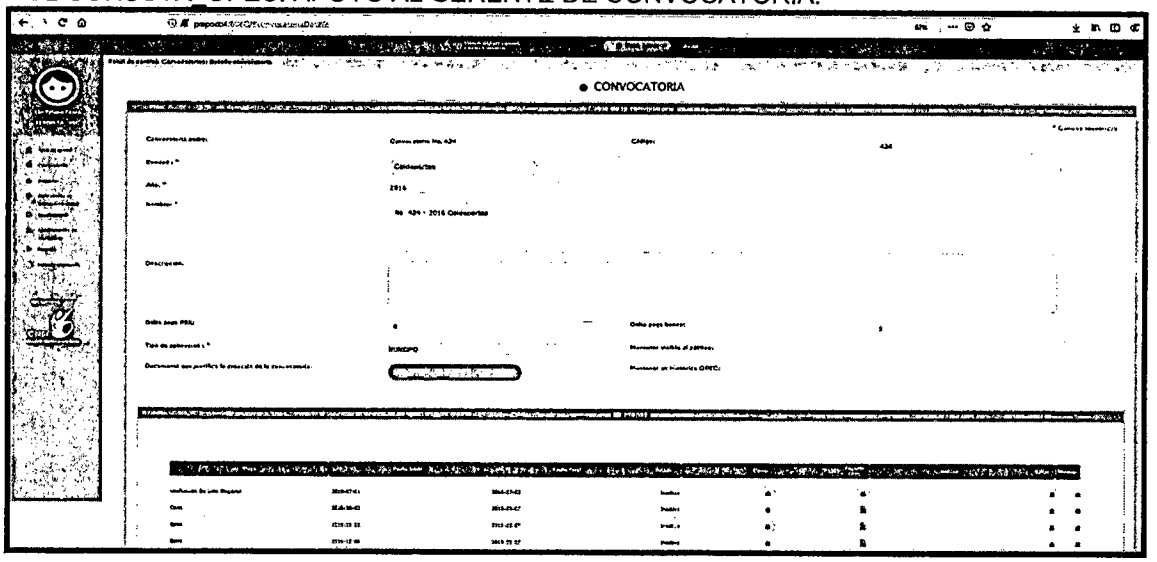
- Se evidenció adecuada gestión frente a la integridad de la información, sobre los roles establecidos, en la herramienta para los de más módulos (OPEC y IES (INSTITUCIONES DE EDUCACIÓN SUPERIOR), de acuerdo con lo presentado en las siguientes ilustraciones que son determinadas por color en la herramienta SIMO :

MODULO OPEC: USUARIOS INTERNOS MODULO OPEC

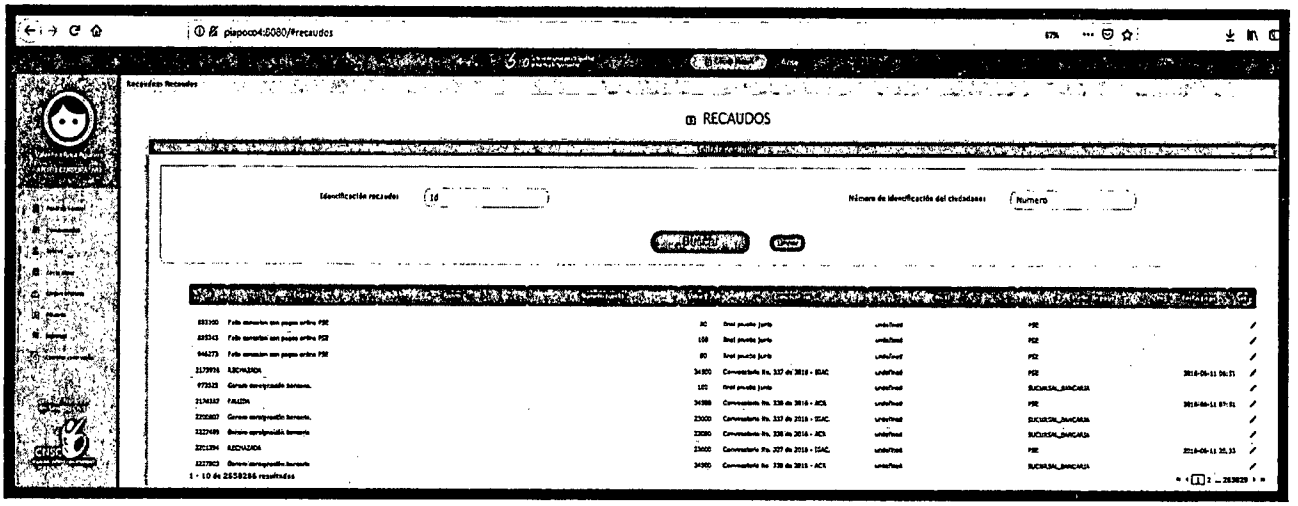
MENU ROL ADMIN_CONVOCATORIA: GERENTE DE CONVOCATORIAS CNSC



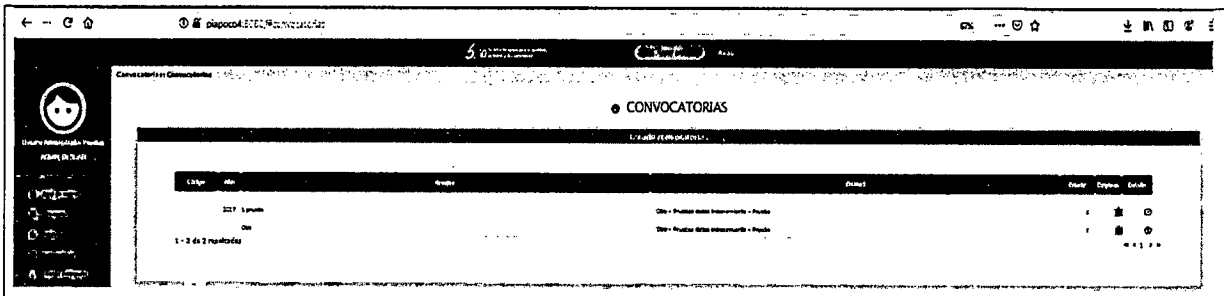
ROL CONSUTA_OPEC: APOYO AL GERENTE DE CONVOCATORIA:



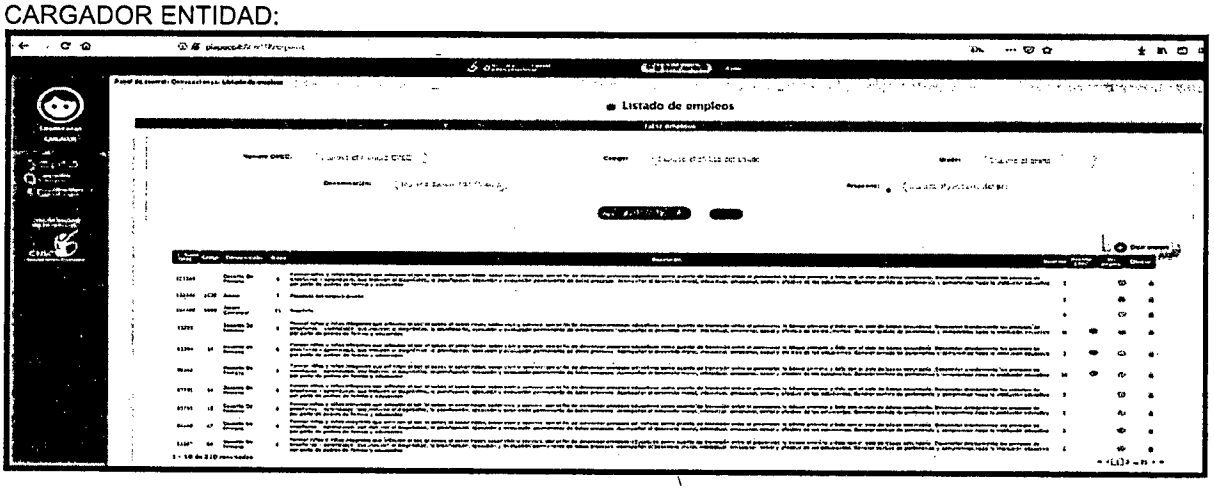
ROL APOYO CORPORATIVO:



<u>USUARIOS EXTERNOS MODULO OPEC</u>
ROL ADMINISTRADOR ENTIDAD

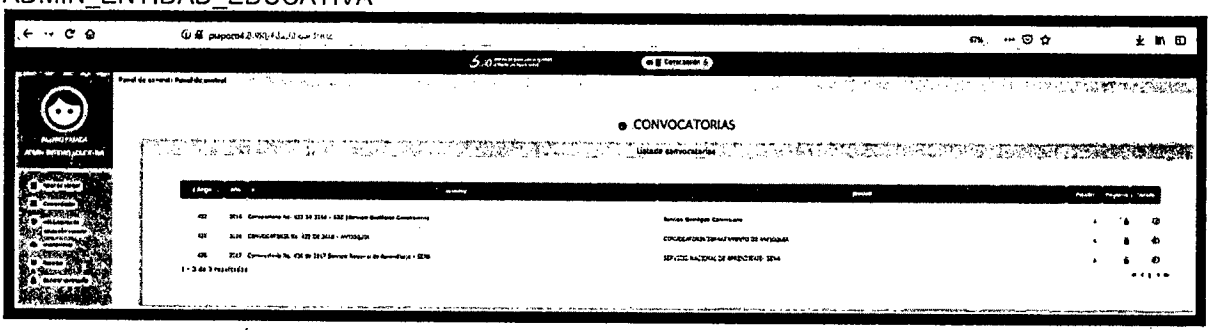


ROL CARGADOR ENTIDAD:

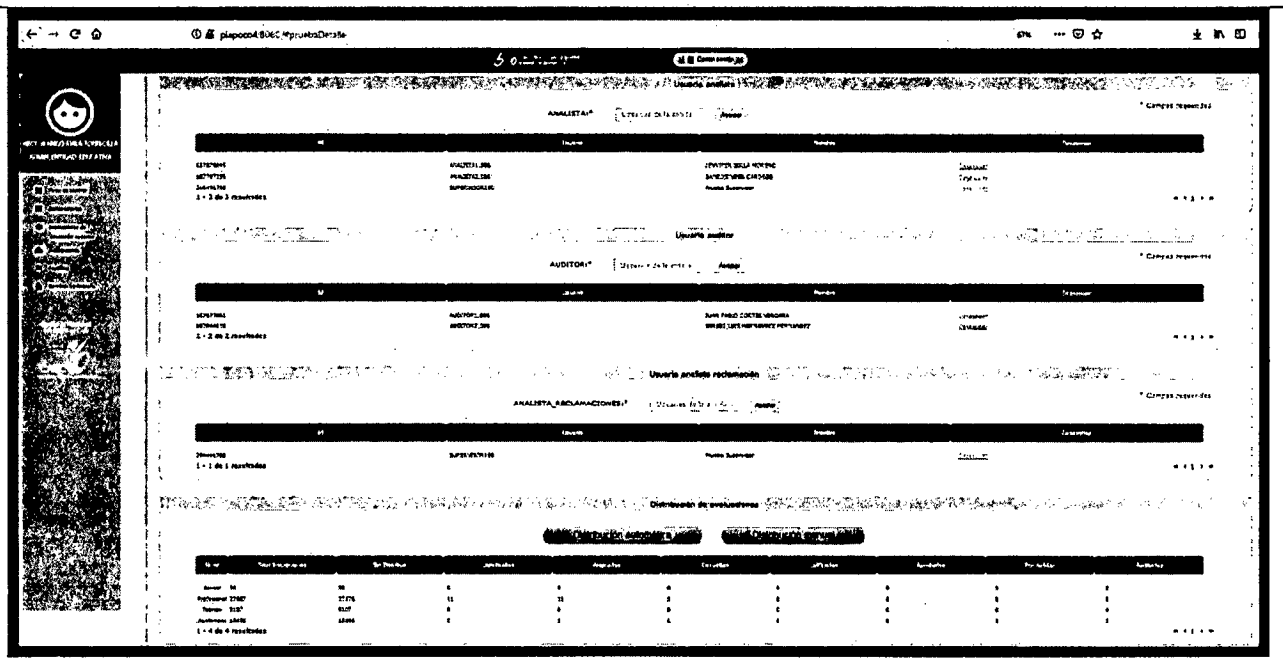


MODULO IES (INSTITUCIONES DE EDUCACIÓN SUPERIOR)

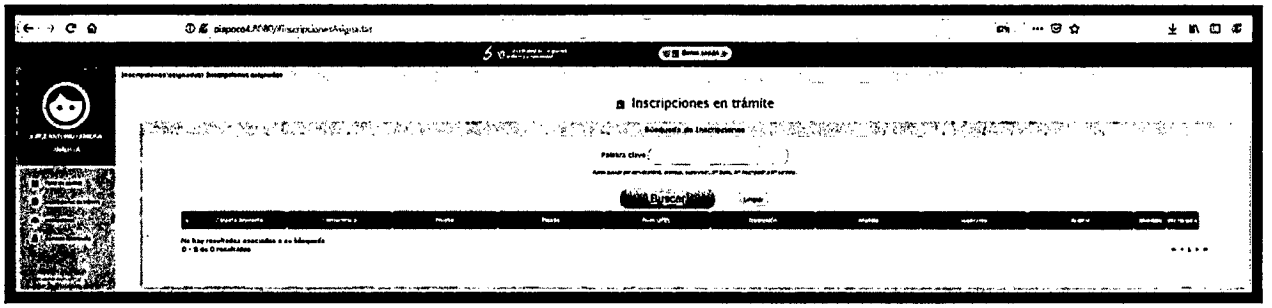
ROL ADMIN_ENTIDAD_EDUCATIVA



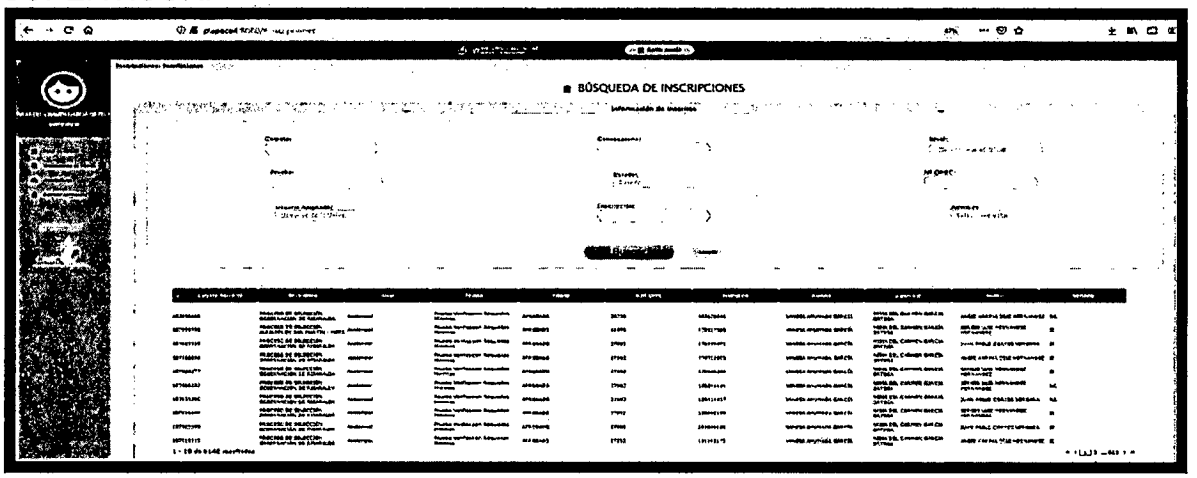
En la siguiente pantalla se muestra como se hace la distribución de las carpetas para evaluar, que es a través de los botones de distribución automática o manual:



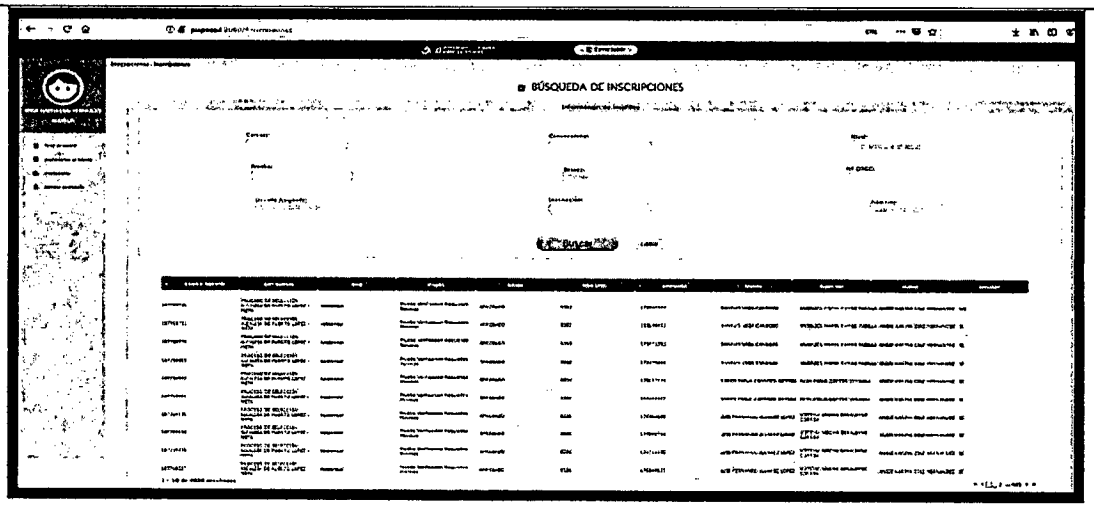
ROL ANALISTA:



ROL SUPERVISOR:



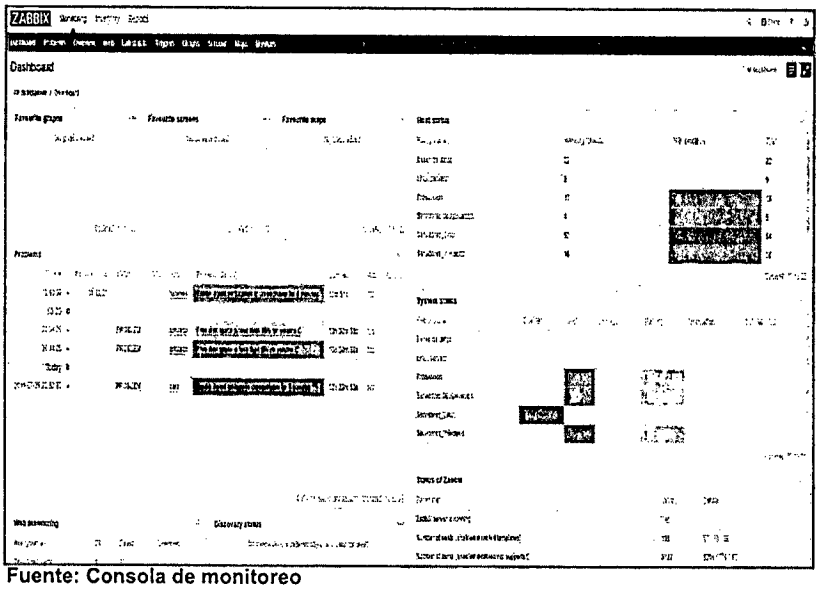
ROL AUDITOR



Disponibilidad de la Información:

- En el aplicativo SIMO, modulo ciudadano, la disponibilidad está dada 365 días de año, debido a la necesidad de los ciudadanos y a la finalidad de servicio de la CNSC.
- La información se clasifica en privada, de acuerdo al registro de cada ciudadano que ingrese al sistema y pública las posibles convocatorias de su ejecución.
- Se cuenta con una consola de monitoreo ZABBIX, del cual se revisa periódicamente el estado actual de los equipos para detectar fallas e inconsistencias en los mismos.

Pantallazo Consola monitoreo



Fuente: Consola de monitoreo

Backup de la información de la Base de Datos del aplicativo SIMO

- El backup de la información asociada a la base de datos del sistema de información SIMO, se realiza diariamente a través de tareas programadas, por el servidor.
  La infraestructura de Base de Datos está conformada por nueve (9) servidores (8 servidores de consulta y uno de escritura). Se realiza el Backups a dos (2) Servidores (Chami 1 y Chami2) cada hora y uno general al final del día, éstos se guardan con base en políticas de seguridad de la información generalmente aceptadas de backups, incrementales y en la semana se realiza un backups Full de toda la información. No obstante, pese a que en las herramientas de gestión de backups se evidencia están implícitas las políticas que se aplican para la toma de las copias de seguridad, la Entidad no cuenta con documentación formal y controlada desde el Sistema Integrado de Gestión, que describa las políticas de seguridad de la información documentada y formalizada

- Adicionalmente se cuenta con un sistema de backups denominado Data protector. No obstante, al momento de realizar la auditoría se evidenció que la Entidad se encuentra en proyecto de implementación de un segundo sistema de backups denominado Veam y permitirá almacenar la información de tipo incremental y full en las cintas, de la siguiente manera:

1. Se analizó y validó la información de un equipo de ejemplo, para el caso chami1, servidor maestro de base de datos de SIMO.

La primera imagen permite ver la información de máquina del host virtual:

Host	EQUIPO	HD	CPU Model	Speed	HT Available	# CPU	# Memory	# NICs	Domain
192.168.50.12	chimila2	204 GB	Intel Xeon E312xx (Sandy Bridge)	2.000	lenta para la gestión colaborativa de proyectos de Oper	2 (2:1:1)	16384	c1 DMZ - nic2 Replicatic	cnsc.net
192.168.50.24 / 192.168.50.26 / 192.168.54.6	chami1	655 GB	Intel Xeon E312xx (Sandy Bridge)	2.000	Base de datos de SIMO 1 - Servidor maestro	16 (16:1:1)	65536	c1 DMZ - nic3 Replicatic	cnsc.net
192.168.50.25	chami2	1.03 TB	Intel Xeon E312xx (Sandy Bridge)	2.000	Servidores de base de datos de SIMO 2	16 (16:1:1)	56320	c1 DMZ - nic3 Replicatic	cnsc.net
192.168.0.4	kanza	472 GB	Intel(R) Xeon(R) CPU E5-2640 0 @ 2.50GHz	2.500	Servidor SQL Server - Producción	4	32768	Producción	cnsc.net
192.168.50.31	kurripakodwh	10 GB	Intel Xeon E312xx (Sandy Bridge)	2.000	Bodega de datos Pentaho	4 (4:1:1)	16384	nic1 DMZ	cnsc.net

2. La segunda imagen permite ver información de especifica del host virtual (para su mejor visualización se ha dividido en dos imágenes)

VM	Powerstate	Template	Config status	DNS Name	Connection state	Guest state	Heartbeat	CPUs	Memory	NICs
Chimila2	Powered On	False	green	chimila2.cnsc.net	connected	running	green	2	16384	2
chami1	Powered On	False	green	chami1.cnsc.net	connected	running	green	16	65807	2
chami2	Powered On	False	green	chami2.cnsc.net	connected	running	green	16	56518	2
kanza	Powered On	False	green	kanza.cnsc.net	connected	running	green	4	32768	1

Memory	NICs	Disks	Video Ram KB	Provisioned MB	In Use MB	Datacenter	Cluster	Host	OS according to the configuration file	OS according to the VMware Tools
16384	2	5	N/A	190000	175000	CNSC	oVirt	i8.50.12 - 192.168	CentOS Linux release 7.5.1804 (Core)	CentOS Linux release 7.5.1804 (Core)
65807	2	5	N/A	610000	605000	CNSC	oVirt	/ 192.168.50.26 /	CentOS Linux release 7.5.1804 (Core)	CentOS Linux release 7.5.1804 (Core)
56518	2	8	N/A	960000	954970	CNSC	oVirt	192.168.50.25	CentOS Linux release 7.4.1708 (Core)	CentOS Linux release 7.4.1708 (Core)
32768	1	3	N/A	470000	351000	CNSC	VMware	192.168.0.4	Microsoft Windows Server 2008 R2 (64-bit)	Microsoft Windows Server 2008 R2 (64-bit)

3. La tercera imagen contiene la información del disco duro y sus discos virtuales respectivos

chami1	backupsvg	Powered On	True	/dev/vde	50000	plantillacentos7_Disk1: (70 GB) existente (boot)
	backupsvg	Powered On	False	/dev/vdb	140000	Chami1_Produccion_Backup: (140 GB) existente
	pgarchivesvg	Powered On	False	/dev/vdd	50000	Chami1_Produccion_Pgarchives: (50 GB) existente
	pgdatavg	Powered On	False	/dev/vdc	300000	Chami1_Produccion_Data: (300 GB) existente
	pgsqlvg	Powered On	False	/dev/vdf	50000	Chami1_Produccion_Pgsql: (50 GB) existente
	rootvg	Powered On	False	/dev/vda	70000	Chami1_Produccion_OS: (70 GB) existente (boot)

4. Información de cada partición del disco duro.

chami1	Powered On	False	/dev/vdb	140000	139980	20	0,01	/pg_bck	140.000	24.000	116.000	/pg_bck
	Powered On	False	/dev/vdd	50000	49990	10	0,02		0	0	0	/pg_archives
	Powered On	False	/dev/vdc	300000	299990	10	0,00	/pg_data	300.000	132.000	168.000	/pg_data
	Powered On	False	/dev/vde	50000	49990	10	0,02	/var/lib/pgsql	50000	5.200	44.800	/var/lib/pgsql
	Powered On	False	/dev/vda	70000	65000	5000	7,14	/usr	10.000	1.700	8.300	/rootvg
	Powered On	False	/dev/vda	70000	65000	5000	7,14	/var	10.000	4.100	5.900	/rootvg

5. Información de la tarjeta de red.

chami1	Powered On	E1000	fe80::21a:4aff:fe16:169	192.168.50.255	oVirt
	Powered On	E1000	fe80::21a:4aff:fe16:173	192.168.54.255	oVirt

Por último, se envía la programación de backups

F-FULL_BD_KANZA	Lunes -- 2 am	5 horas	Permanente	chami1	/pg_bck		34 / 192.168.50.26 / 1[illegible]	CentOS 7.5.180[illegible]
		5 horas	Permanente	chami2	/pg_bck		192.168.50.25	CentOS 7.4.170[illegible]
		5 horas	Permanente	kanza	BCK_ACCNSBOR1		192.168.0.4	Microsoft Windows Server 200[illegible]
		5 horas	Permanente	kanza	BCK_DEFAULT		192.168.0.4	Microsoft Windows Server 200[illegible]
		5 horas	Permanente	kumipdrotarh	/pg_bck		192.168.50.31	CentOS Linux release 7.5.[illegible]
		5 horas	Permanente	[illegible]	/backupsmariadb		192.154.50.30	
		5 horas	Permanente	openproject	/var		192.168.100.64	CentOS Linux release 7.5.[illegible]
		5 horas	5 semanas	Lanamedra-bd	/pg_bck		192.168.50.40	CentOS 7.5.180[illegible]
		5 horas	Permanente	tororo1	/pg_bck		192.168.50.21	CentOS Linux release 7.5.[illegible]
		5 horas	Permanente	tororo2	/pg_bck		192.168.50.22	CentOS Linux release 7.5.[illegible]
		5 horas	Permanente	remu1	/pg_bck		192.168.52.45	CentOS Linux release 7.5.[illegible]

Seguridad del aplicativo SIMO

Se cuenta con niveles de seguridad informática en cuanto a:

- ✓ Firewall: Protegidos a nivel de red y centro de datos de la CNSC
- ✓ Zona desmilitarizada: Pero la DMZ no se pude conectar a nivel interno y externo, protegiendo los equipos de la red de cualquier ataque.
- ✓ Se cuenta con reglas seguras dentro de los Firewall que impide al acceso directo a los equipos protegidos.
- ✓ La aplicación SIMO cuenta con un certificado de seguridad (https://simo.cnsc.gov.co), para el acceso desde internet, que cifra la información entre el usuario y la página web.

Con lo anterior, la Oficina de Control Interno diseñó y aplicó una lista de chequeo para validar la adecuada gestión e implementación del sistema de Información SIMO, encontrando lo siguiente:

Actividad validada	Grado de cumplimiento en porcentaje (%)
I. Origen y preparación de los datos	92%
II. Acceso y seguridad al Sistema	88%
III. Salida de datos	76%
IV. Integridad de los datos	92%
V. Documentación Técnica y de Usuario	68%
VI. Respaldo y recuperación de desastres	28%
VII. Seguridad física	89%
VIII. Recurso Humano	87%
Total	**70%**

Fuente. Lista de chequeo aplicada por la Oficina de Control Interno para el periodo auditado.

La tabla muestra que fueron evaluados ocho (8) aspectos, de los cuales tres (3) se encuentran en un grado de cumplimiento relativamente alto, tales son: Integridad de los datos (92%), Origen y preparación de los datos (92%) y seguridad física (89%). En un grado de cumplimiento relativamente bueno, se encontraron tres (3) aspectos que son: Salida de datos (76%),

documentación técnica y de usuario (68%) y Acceso y seguridad al sistema (88%).

Lo anterior indica que, si bien se han adelantado parte de las acciones previstas, y se cuenta con un plan de trabajo falta culminar con el grado de implementación al 100%.

c) Verificación del grado de implementación del sistema de seguridad de la información (SGSI) de la CNSC en el marco de los requisitos definidos en la NTC-ISO 27001:2013

Se realizó un análisis permitiendo evaluar el estado de los avances en la implementación del SGSI, enmarcado en la Norma NTC-ISO-IEC 27001: 2013 SGSI, de la CNSC.

Dicho análisis fue realizado, utilizando y aplicando la herramienta "Análisis GAP Norma NTC ISO-IEC 27001:2013, diligenciando el Anexo A, el cual presenta los controles de cada uno de los dominios y subdominios definidos en la norma mencionada. Una vez diligenciado el Anexo, se obtuvieron los resultados en porcentaje de avance del cumplimiento tanto de los subdominios, como de los dominios, representados en la escala de cumplimiento y en los resultados del nivel de implementación de controles.

Escala de cumplimiento Norma ISO 27001:2013

Este cuadro colorimétrico, recoge los resultados generales y se determina el nivel de implementación del Sistema en la Entidad, tal como se muestra a continuación:

Nivel de Implementación	% de Cumplimiento	Descripción
Gestionado	100%	Los procesos han sido llevados al nivel de mejores prácticas, con base en los resultados de la mejora continua.
		Es posible hacer seguimiento y medir el cumplimiento de los procedimientos, así como tomar acciones correctivas o preventivas cuando se detectan fallas y hacer seguimiento dichas acciones.
Medible	80%	Es posible hacer seguimiento y medir el cumplimiento de los procedimientos, aunque no es constante que se tomen acciones correctivas o preventivas.
Definido	60%	Los procesos se encuentran totalmente documentados pero la responsabilidad del cumplimiento recae en cada individuo y es poco probable que se detecten desviaciones a los estándares establecidos.
Repetible	40%	Los procesos se han desarrollado hasta un punto en el cual procedimientos similares son utilizados por personas diferentes para llevar a cabo la misma tarea, aun cuando estos no se encuentran totalmente documentados.
Inicial	20%	Se ha identificado una situación que debe ser tratada y se han implementado acciones aun cuando no hay directivas o procesos documentados relacionados con dichas acciones.
Inexistente	0	Carencia total de procesos relacionados con el SGSI.
		La organización no ha identificado una situación que debe ser tratada.

Resultados nivel de implementación de controles Norma ISO 27001:2013

Con esta tabla, se califican la totalidad de los controles definidos en la norma y recoge el porcentaje de avance que se registró en el Anexo A, tal y como se muestra a continuación:

Item	Controles	NM (%)
A.5	POLITICA DE SEGURIDAD	90%
A.5.1	Política de Seguridad de la Información	80%
A.5.1.1	Políticas para la seguridad de la información	100%
A.5.1.2	Revisión de la política de seguridad de la información	60%
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	46%
A.6.1	Organización interna	32%
A.6.1.1	Seguridad de la información Roles y responsabilidades	100%
A.6.1.2	Separación de deberes	0%
A.6.1.3	Contacto con las autoridades	20%
A.6.1.4	Contacto con grupos de interés especial	20%
A.6.1.5	Seguridad de la información en gestión de proyectos	20%
A.6.2	Dispositivos móviles y teletrabajo	60%
A.6.2.1	Política para dispositivos móviles	60%
A.6.2.2	Teletrabajo	60%
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	100%
A.7.1	Antes de asumir el empleo	100%
A.7.1.1	Selección	100%
A.7.1.2	Términos y condiciones del empleo	100%
A.7.2	Durante la ejecución del empleo	100%
A.7.2.1	Responsabilidades de la dirección	100%
A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	100%
A.7.2.3	Proceso disciplinario	100%
A.7.3	Terminación y cambio de empleo	100%
A.7.3.1	Terminación o cambio de responsabilidades de empleo	100%
A.8	GESTIÓN DE ACTIVOS	44%
A.8.1	Responsabilidad por los activos	45%
A.8.1.1	Inventario de activos	20%
A.8.1.2	Propiedad de los activos	40%
A.8.1.3	Uso aceptable de los activos	80%
A.8.1.4	Devolución de activos	40%
A.8.2	Clasificación de la información	40%
A.8.2.1	Clasificación de la información	40%
A.8.2.2	Etiquetado de la información	40%
A.8.2.3	Manejo de activos	40%
A.8.3	Manejo de medios de soporte	47%
A.8.3.1	Gestión de medios de soporte removibles	40%
A.8.3.2	Disposición de los medios de soporte	40%
A.8.3.3	Transferencia de medios de soporte físicos	60%
A.9	CONTROL DE ACCESO	45%
A.9.1.1	Requisitos del negocio para control de acceso	70%
A.9.1.2	Política de control de acceso	100%
A.9.1.3	Acceso a redes y a servicios en red	40%
A.9.2	Gestión de acceso de usuarios	40%

A.9.2.1	Registro y cancelación del registro de usuarios	60%
A.9.2.2	Suministro de acceso de usuarios	40%
A.9.2.3	Gestión de derechos de acceso privilegiado	40%
A.9.2.4	Gestión de información de autenticación secreta de usuarios	40%
A.9.2.5	Revisión de los derechos de acceso de usuarios	20%
A.9.2.6	Retiro o ajuste de los derechos de acceso	40%
A.9.3.	Responsabilidades de los usuarios	20%
A.9.3.1	Uso de información de autenticación secreta	20%
A.9.4.	Control de acceso a sistemas y aplicaciones	48%
A.9.4.1	Restricción de acceso a información	40%
A.9.4.2	Procedimiento de ingreso seguro	40%
A.9.4.3	Sistema de gestión de contraseñas	40%
A.9.4.4	Uso de programas utilitarios privilegiados	60%
A.9.4.5	Control de acceso a códigos fuente de programas	60%
A.10.	CRIPTOGRAFÍA	100%
A.10.1.	Controles criptográficos	100%
A.10.1.1	Política sobre el uso de controles criptográficos	100%
A.10.1.2	Gestión de claves	100%
A.11.	SEGURIDAD FÍSICA Y DEL ENTORNO	34%
A.11.1.	Áreas Seguras	20%
A.11.1.1	Perímetro de seguridad física	20%
A.11.1.2	Controles de acceso físico	20%
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	20%
A.11.1.4	Protección contra amenazas externas y ambientales	20%
A.11.1.5	Trabajo en áreas seguras	20%
A.11.1.6	Áreas de carga, despacho y acceso público	20%
A.11.2.	Equipos	49%
A.11.2.1	Ubicación y protección de los equipos	80%
A.11.2.2	Servicios públicos de soporte	20%
A.11.2.3	Seguridad del cableado	40%
A.11.2.4	Mantenimiento de los equipos	20%
A.11.2.5	Retiro de activos	40%
A.11.2.6	Seguridad de los equipos y activos fuera de las instalaciones	40%
A.11.2.7	Disposición segura o reutilización de equipos	40%
A.11.2.8	Equipos de usuario desatendido	60%
A.11.2.9	Política de escritorio limpio y pantalla limpia	100%
A.12.	SEGURIDAD DE LAS OPERACIONES	49%
A.12.1.	Procedimientos Operacionales y Responsabilidades	55%
A.12.1.1	Documentación de los procedimientos de operación	40%
A.12.1.2	Gestión del cambios	100%
A.12.1.3	Gestón de la capacidad	60%
A.12.1.4	Separación de las instalaciones de desarrollo, pruebas y operación	20%
A.12.2.	Protección contra códigos maliciosos	60%
A.12.2.1	Controles contra códigos maliciosos.	60%
A.12.3.	Copias de respaldo	60%
A.12.3.1	Copias de respaldo de la información	60%
A.12.4.	Registro y seguimiento	40%

A.12.4.1	Registro de eventos	20%
A.12.4.2	Protección de la información de registro	20%
A.12.4.3	Registros del administrador y del operador	20%
A.12.4.4	Sincronización de relojes	100%
A.12.5.	Control de software operational	60%
A.12.5.1	Instalación de software en sistemas operativos	60%
A.12.6.	Gestión de la vulnerabilidad técnica	50%
A.12.6.1	Gestión de las vulnerabilidades técnicas	60%
A.12.6.2	Restricciones sobre la instalación de software.	40%
A.12.7.	Consideraciones sobre auditorías de sistemas de información	20%
A.12.7.1	Controles de auditorías de sistemas de información.	20%
A.13.	SEGURIDAD DE LAS COMUNICACIONES	37%
A.13.1.	Gestión de la seguridad de redes	20%
A.13.1.1	Controles de redes	20%
A.13.1.2	Seguridad de los servicios de red.	20%
A.13.1.3	Separación en las redes	20%
A.13.2.	Transferencia de información	90%
A.13.2.1	Políticas y procedimientos de transferencia de información	100%
A.13.2.2	Acuerdos sobre transferencia de información	80%
A.13.2.3	Mensajes electrónicos	100%
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	80%
A.14.	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	51%
A.14.1.	Requisitos de seguridad de los sistemas de información	33%
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	60%
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	20%
A.14.1.3	Protección de transacciones de servicios de aplicaciones	20%
A.14.2.	Seguridad en los procesos de desarrollo y de soporte	60%
A.14.2.1	Política de desarrollo seguro	60%
A.14.2.2	Procedimientos de control de cambios en sistemas	60%
A.14.2.3	Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones	60%
A.14.2.4	Restricciones en los cambios a los paquetes de software	60%
A.14.2.5	Principios de construcción de los sistemas seguros	60%
A.14.2.6	Ambiente de desarrollo seguro	60%
A.14.2.7	Desarrollo contratado externamente	60%
A.14.2.8	Pruebas de seguridad de sistemas	60%
A.14.2.9	Prueba de aceptación de sistemas	60%
A.14.3.	Datos de prueba	60%
A.14.3.1	Protección de datos de prueba	60%
A.15.	RELACIONES CON LOS PROVEEDORES	53%
A.15.1.	Seguridad de la información en las relaciones con los proveedores	47%
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	100%
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	20%
A.15.1.3	Cadena de suministro de tecnología de información y	20%

	comunicación	
A.15.2.	Gestión de la prestación de servicios de proveedores	60%
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	60%
A.15.2.2	Gestión de cambios a los servicios de los proveedores	60%
A.16.	GESTIÓN DE INCIDENTES DE SEGURIDAD	74%
A.16.1.	Gestión de incidentes y mejoras en la seguridad de la información	74%
A.16.1.1	Responsabilidades y procedimientos	100%
A.16.1.2	Reporte de eventos de seguridad de la información	100%
A.16.1.3	Reporte de debilidades de seguridad de la información	60%
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos.	100%
A.16.1.5	Respuesta a incidentes de seguridad de la información	80%
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	40%
A.16.1.7	Recolección de evidencia	40%
A.17.	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO	0%
A.17.1.	Continuidad de seguridad de la información	0%
A.17.1.1	Planificación de la continuidad de la seguridad de la información	0%
A.17.1.2	Implementación de la continuidad de la seguridad de la información	0%
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	0%
A.17.2.	Redundancias	0%
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información	0%
A.18.	CUMPLIMIENTO	71%
A.18.1.	Cumplimiento de requisitos legales y contractuales	68%
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	100%
A.18.1.2	Derechos de propiedad intelectual	100%
A.18.1.3	Protección de registros	20%
A.18.1.4	Privacidad y protección de información de datos personales	40%
A.18.1.5	Reglamentación de controles criptográficos	80%
A.18.2.	Revisiones de seguridad de la información	73%
A.18.2.1	Revisión independiente de la seguridad de la información	100%
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	60%
A.18.2.3	Revisión del cumplimiento técnico	60%
	TOTAL	57%

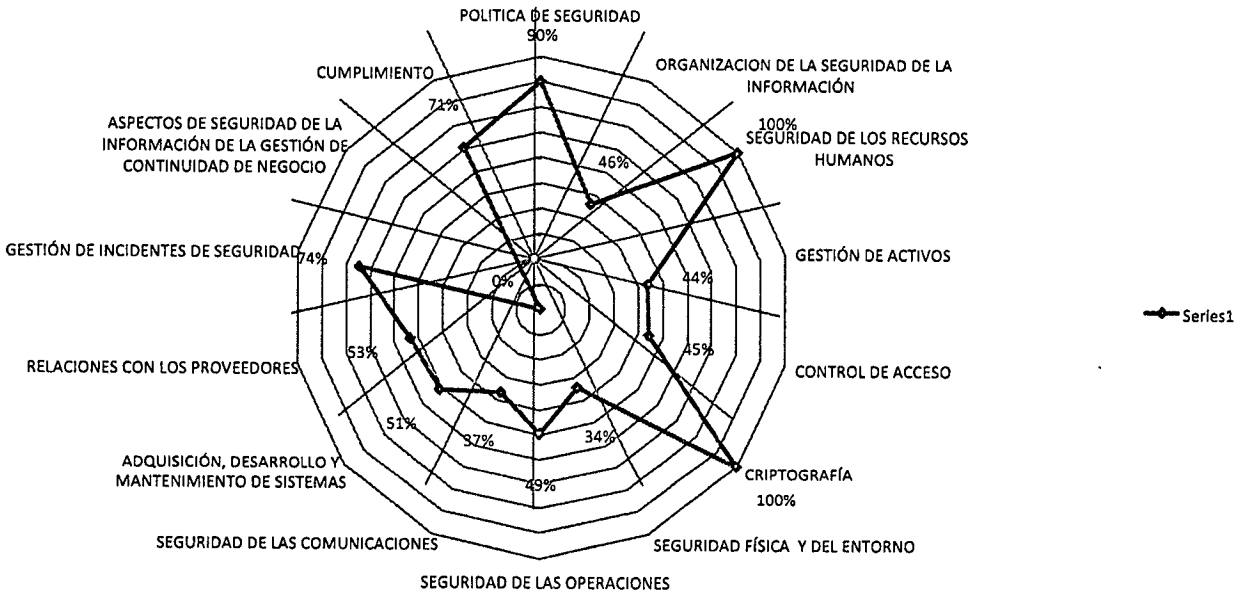
Tabla de resultados por dominio:

Esta tabla, recoge y resume los porcentajes de avance arrojados por la tabla anterior "Resultados Nivel de Implementación de Controles", y muestra el grado de cumplimiento para el total de dominios, tal y como se muestra a continuación:

Item	Dominios	Cumplimiento
5	POLITICA DE SEGURIDAD	90%
6	ORGANIZACION DE LA SEGURIDAD DE LA INFORMACIÓN	46%
7	SEGURIDAD DE LOS RECURSOS HUMANOS	100%
8	GESTIÓN DE ACTIVOS	44%
9	CONTROL DE ACCESO	45%
10	CRIPTOGRAFÍA	100%
11	SEGURIDAD FÍSICA Y DEL ENTORNO	34%
12	SEGURIDAD DE LAS OPERACIONES	49%
13	SEGURIDAD DE LAS COMUNICACIONES	37%
14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	51%
15	RELACIONES CON LOS PROVEEDORES	53%
16	GESTIÓN DE INCIDENTES DE SEGURIDAD	74%
17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO	0%
18	CUMPLIMIENTO	71%
TOTAL		57%

Los porcentajes de avances para cada uno de los dominios y subdominios, fueron reportados por la Oficina Asesora de Informática de acuerdo al nivel de avance en el plan de implementación que adelanta la entidad y remitidos a esta oficina mediante CD y correo electrónico del 20 de julio de 2019, la Oficina de Control Interno, realizo la verificación, registró las observaciones y recomendaciones, de acuerdo con las evidencias aportadas por la Oficina Asesora de Informática (OAI) y por la documentación existente en la intranet de la Entidad en el micrositio designado para los (Manuales, Formatos, Procedimientos, instructivos, protocolos etc.

Análisis por Dominio



De acuerdo con la gráfica, se observa que los dominios con mayor nivel de madurez son criptografía (100%), seguridad de los recursos humanos (100%), política de seguridad de la información (90%) y gestión de incidentes de seguridad (74%), lo cual resulta del respaldo de la Alta Dirección y de la gestión adelantada por la OAI y demás dependencias comprometidas para la implementación del Sistema de Seguridad de la Información.

Sin embargo y aunque se muestra un avance significativo en los aspectos mencionados, el nivel de madurez al corte de julio 31 de 2019 del SGSI fue del 57% que significa de acuerdo a la escala de cumplimiento definida en el análisis GAP, que la Entidad está levemente por debajo del nivel "Definido" (60%) y por encima del nivel "repetible (40%) es decir, que los procesos se encuentran documentados pero la responsabilidad del cumplimiento recae en cada individuo de la entidad y es poco probable que se detecten desviaciones a los estándares establecidos.

Dichos avances no se han desarrollado en similares porcentajes en todos los frentes, prueba de ello son los relativos bajos avances en lo que tiene que ver con: seguridad física del entorno (34%), seguridad de las comunicaciones (37%), gestión de activos (43,9%), control de accesos (45%), organización de la seguridad de la información (46%), seguridad de las operaciones (49%), adquisición, desarrollo y mantenimiento de los sistemas (51%) y relación con los proveedores (53%) los cuales muestran muy bajos avances comparados con los otros dominios de la Norma. No obstante, se considera importante precisar que, dado que la Entidad no cuenta con un plan de continuidad del negocio, se incrementan los riesgos de interrupciones no planificadas en TI y telecomunicaciones, ciberataques, brechas de datos, interrupciones del suministro de red, incidentes de seguridad. Riesgos que no fueron identificados, analizados, valorados en el mapa de riesgos de los procesos: Gestión de Recursos tecnológicos y Gestión de Tecnologías de la Información, publicados en la intranet al corte de la presente evaluación. Sin embargo, la Oficina Asesora de Informática dentro de su plan estratégico de tecnologías de la información PETI 2019 – 2022 plantea desarrollar proyectos tendientes a mitigar este riesgo que a la fecha se puede llegar a materializar.

d) **Seguimiento al Plan de Mejoramiento Interno suscrito por la Oficina Asesora de Informática (OAI)**

De acuerdo con el archivo en Excel que contiene el Plan de Mejoramiento Interno de la Oficina Asesora de Informática, que fue descargado de la intranet en agosto 02 de 2019, se evidenció lo siguiente:

Total hallazgos y recomendaciones	Total acciones propuestas por la OAI	El campo definido para registrar el seguimiento se encuentra diligenciado.	Estado acción
6	22	8 de 22 no están diligenciados	El 100% están cerradas

Se considera importante indicar que, para las 22 acciones propuestas por la OAI para dar respuesta a los 6 hallazgos identificados, las fechas de vencimiento no sobrepasan el mes de febrero de 2019 y 2 de 22 presentaron reprogramación de las fechas de cierre, ya que su fecha

inicial se encontraba para cumplirse en diciembre 13 de 2018 y su fecha de reprogramación se registró para mayo 21 de 2019. Al corte del presente documento, el 100% de las acciones propuestas se encuentran cerradas evidenciando acciones oportunas en el desarrollo del plan de mejoramiento.

2.3 Hallazgos y/o No Conformidades

Como resultados de la evaluación a los procedimientos de gestión de tecnologías de la información gestión de recursos tecnológicos y normas aplicables se encontró:

Hallazgo 1: Gestión de Recursos Tecnológicos

- Al procedimiento Mesa de servicio con código P-RT-003 versión 2.1 del 10 de octubre de 2016 se le evidenciaron debilidades e incumplimientos en el diseño y aplicación del mismo, así como desactualización, incumpliendo lo establecido en el procedimiento "Control de Documentos con código P-SG-005 versión 3 en el paso 1 del numeral 6.1 Elaboración, actualización y control de documentos y en la ISO- IEC- NTC 27001:2013 en los numerales: *A.12.1.1Documentación de los procedimientos de operación* ya que se encontraron las siguientes situaciones:

  - En el numeral "5 Normativa Aplicable" del procedimiento enunciado, se registra la NTCGP1000:2009 Norma Técnica Colombiana de la Gestión Pública, la cual fue Derogada mediante el Decreto 1499 de 2017 Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.

  - En numeral 6 "Desarrollo del Procedimiento", se describen en la actividad 5, actividades que no son concordantes con lo descrito en el flujograma del procedimiento. Ya que se define que si la incidencia es solucionada y si la misma registrada requiere acciones de proveedores de productos externos, se continúa al paso 8, de igual forma, se define si la incidencia no tiene solución en el nivel 2 ni en el nivel 3, se continúa en el paso 7. No obstante el flujograma se indica que si se requiere acción del proveedor se debe continuar al paso 7, de igual forma si no es solucionada la incidencia se debe continuar al paso 6 (aplicar procedimiento de contratación).

  - No se evidenciaron registros ni soportes que demuestren seguimiento a los resultados de la satisfacción al usuario, ni que sean utilizados para la toma de decisiones que encaminen el sistema hacia la mejora continua. De igual forma, el procedimiento no cuenta con la descripción de actividades que indiquen el seguimiento que se debe realizar a la satisfacción del usuario interno, una vez son gestionados los requerimientos que se realizan mediante el sistema de información GLPI destinado para tal fin. Por lo tanto, falta diseñar e implementar una metodología que dé respuesta a lo definido en el numeral *A16 Gestión de incidentes de la Norma* ISO – IEC-NTC 27001:2013 y que le permitan a la Oficina Asesora de Informática y a la Alta Dirección tomar decisiones encaminadas hacia la mejora continua.

- Del procedimiento Gestión y Operación de la Infraestructura Tecnológica con código P-RT-001 versión 1.0 del 29 de febrero de 2016, se evidenció debilidad en el diseño y aplicación del mismo, desactualización e incumplimiento al procedimiento "Control de Documentos con código P-SG-005 versión 3 en el paso 1 del numeral 6.1 Elaboración, actualización y control de documentos, ya que se encontraron las siguientes situaciones:

  - El procedimiento no se revisa periódicamente con el fin de identificar la necesidad de ajuste, ya que se encontró que el numeral 4 "Normativa Aplicable", no registra normativa aplicable a la actualidad de la Entidad y del proceso en materia de Sistemas de Información y Tecnologías de la Información, pues no registra las siguientes normas: Decreto 1499 de 2017, Ley 1712 de 2012, y la NTC-IEC-ISO 27001:2013.

  - La descripción de las actividades registradas en el procedimiento, no son concordantes con el objetivo y alcance y tampoco son concordantes con la realidad actual del proceso, en razón a que los pasos definidos en el numeral 6 *"Desarrollo del procedimiento"*, describen el que hacer frente a la gestión de una mesa de servicio, pero el procedimiento no describe el que hacer frente a aprovisionar, mantener, diagnosticar, asegurar y soportar la infraestructura tecnológica de la Entidad (hadware y software), para velar por el correcto funcionamiento de las aplicaciones y servicios informáticos de la entidad, actividades que corresponden al objetivo de dicho documento.

  - Por otra parte, en el numeral 5 "Políticas de Operación", se listan unos documentos que deben ser aplicados, tales como: documento acceso a las bases de datos ambiente de producción, Guía de Backups, instructivo de apagado y encendido seguro DATACENTER, controles de seguridad informática, instructivo para la recepción de información, instructivo de asignación de permisos de navegación, instructivo de segmentación y aseguramiento de equipos activos e instructivo de conexión VPN. No obstante tales documentos no son controlados desde el Sistema de Gestión de la Entidad pues no están en la intranet, ni están oficializados. Se considera importante mencionar que algunos de los documentos mencionados, existen en un repositorio de información denominado "WIKI", pero no es el oficial y los colaboradores de la Entidad, no tienen acceso a dicha información.

  - En numeral 6 "*Desarrollo del Procedimiento*", se describe en la actividad 8 aprobar caso en mesa de servicio, no obstante, en el flujograma del procedimiento para la actividad 8 se describe "fin de servicio". Lo anterior evidencia que lo descrito en los pasos del procedimiento no es concordante con lo registrado en el flujo grama.

- Del procedimiento de Mantenimiento de Soluciones Informáticas P-RT-002, Versión 2.0, se encontraron las siguientes debilidades:

  - La normativa aplicable debe ser verificada, lo anterior dado a que la norma: NTCGP1000: 2009 Norma Técnica Colombiana de la Gestión Pública, norma que fue Derogada mediante el Decreto 1499 de 2017 Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en

lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.

- En el desarrollo del procedimiento en el paso 4 se hace referencia a: aclarar *la solicitud*, con el responsable Oficina *Asesora de informática,* en el flujograma, el paso 4 *Se refiere a Levantar requerimientos y especificar los cambios que se van a realizar* Esten cargo de: *Gerente de convocatoria/líder de proceso/Jefe de dependencia;* frente al paso 7,8,9 y 10 tampoco hay concordancia con lo registrado en el flujograma.
- Por otro lado, durante la ejecución de la auditoria se mencionó por parte de Ingeniero de la Oficina Asesora de Informática que este procedimiento será reemplazado por el de Desarrollo de Software.

- Lo anterior demuestra un incumplimiento de seguimiento para los puntos señalados frente a las funciones de la oficina Asesora de informática, que se encuentran publicadas en la intranet de la Entidad, al corte de la presente evaluación. Las funciones incumplidas son las siguientes: numerales 4. *Preparar y realizar el seguimiento a todos los planes y programas para mantener actualizada la infraestructura tecnológica como soporte para la gestión administrativa y la gestión misional de la Comisión y gestionar los recursos que sean necesarios*

Hallazgo 2: Gestión de Tecnologías de la Información

- Del procedimiento verificación acuerdo de niveles de servicio del sistema de comunicaciones, de la capacidad computacional y de carácter procedimental, que use la universidad o IES - P-TI-002 se debe ajustar y aplicar adecuadamente, ya que se evidenció lo siguiente:

  - Debilidades e incumplimientos en el diseño y aplicación del procedimiento P-TI-002 versión 1.0., del 1 de marzo de 2016, así como desactualización del mismo, incumpliendo lo establecido en la ISO- IEC- NTC 27001:2013 en los numerales: *A.12.1.1Documentación de los procedimientos de operación* ya que se encontraron las siguientes situaciones:

  - En el numeral "4 Normativa Aplicable" del procedimiento enunciado, se registra la NTCGP1000:2009 Norma Técnica Colombiana de la Gestión Pública, norma que fue Derogada mediante el Decreto 1499 de 2017 Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.

  - El objetivo del procedimiento, no está actualizado a la operatividad dado a que revisa es el
    cumplimentó de las obligaciones contractuales del contrato de la Universidad con la CNSC

- Del procedimiento Proyección de Adquisición y Crecimiento de Infraestructura - P-IT-003, se evidenciaron las siguientes situaciones:

  - Debilidad en el diseño y aplicación del procedimiento Proyección de Adquisición y crecimiento de Infraestructura con código P-TI-003 versión 2 del 29 de febrero de 2016, así como desactualización e incumplimiento al procedimiento "Control de Documentos con código P-SG-005 versión 3 en el paso 1 del numeral 6.1 Elaboración, actualización y control de documentos, ya que se encontraron las siguientes situaciones:

    - En el numeral 5 Políticas de operación, se despliegan tres (3) actividades, las cuales quedaron derogadas luego de que la Entidad implementó el Sistema de Información SIMO.

    - En el numeral 6 Desarrollo del procedimiento, se describen pasos que no están ajustados a la actualidad del procedimiento y no son concordantes con el objetivo del mismo, por ejemplo: El paso 1 (recibir a través de mesa de servicio requerimiento de infraestructura tecnológica) aplica solo para software y no para hardware, lo anterior contraviene lo definido en el objetivo del procedimiento ya que corresponde a adquirir, renovar o contratar la infraestructura tecnológica hardware y software necesaria para soportar las aplicaciones y servicios informáticos de la Entidad.

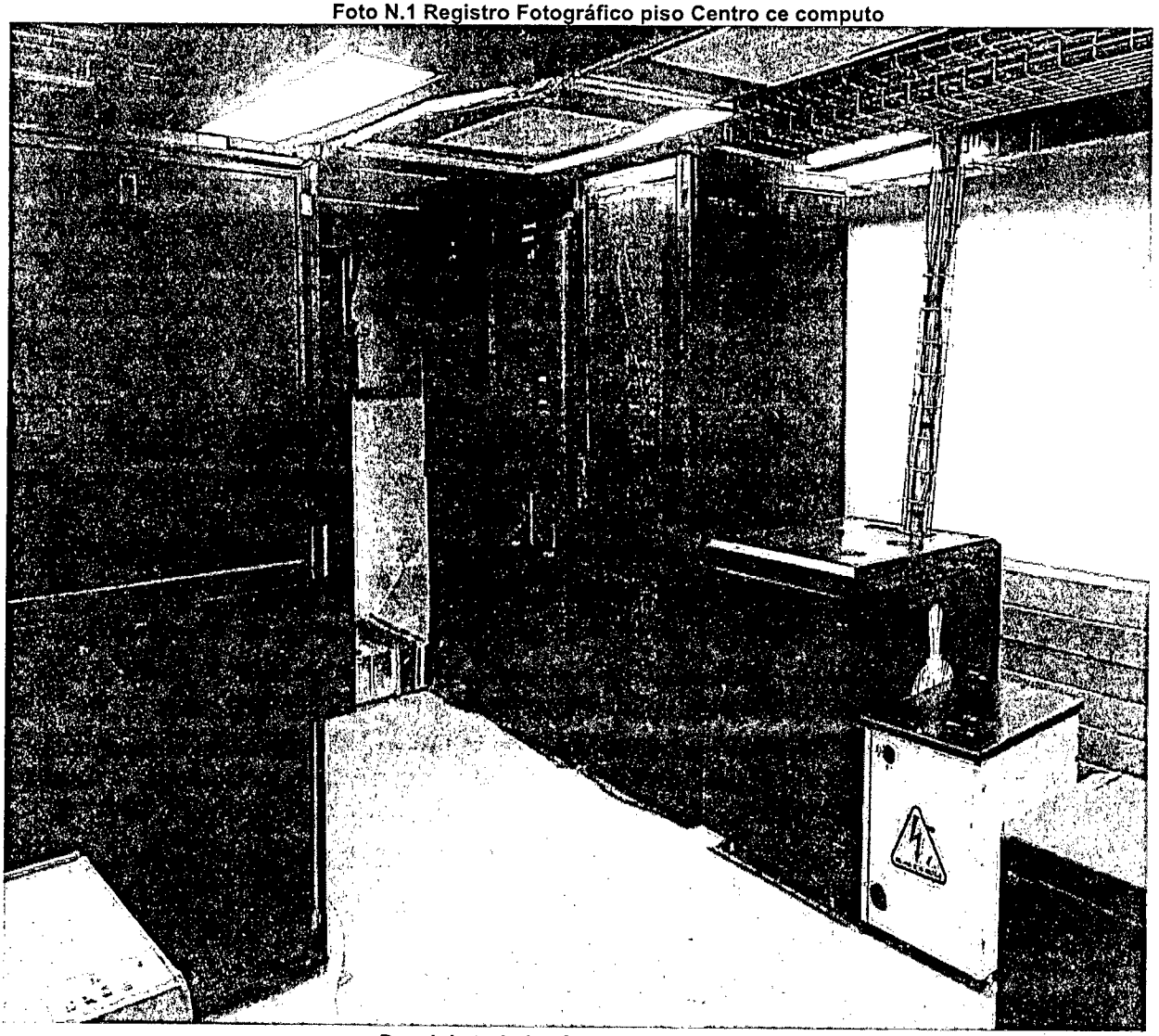
- Los procedimientos Proyección de Adquisición y crecimiento de Infraestructura con código P-TI-003 versión 2 del 29 de febrero de 2016 y Gestión y Operación de la Infraestructura Tecnológica con código P-RT-001 versión 1.0 del 29 de febrero de 2016 son similares, por tanto, no es posible identificar la diferencia entre los dos procedimientos.

  - De otra parte, durante la visita realizada al Centro de Computo, la cual se efectuó con el fin de, realizar observaciones y/o recomendaciones que contribuyan a la optimización del proceso, se encontró:

Observaciones:

- El techo del área no es uniforme ya que presenta sócalos, esto complica la administración de las redes eléctricas y de datos que alimentan los racks:

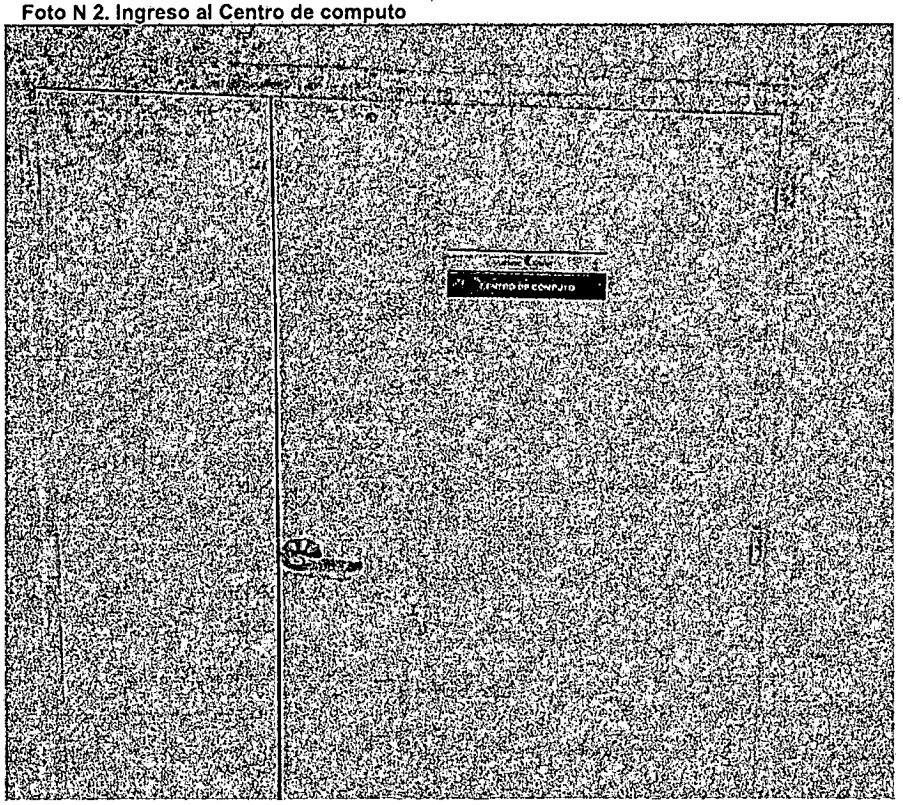
Foto N.1 Registro Fotográfico piso Centro ce computo

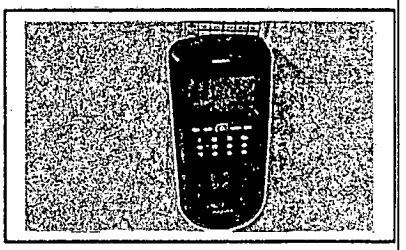


Papel de trabajo: Centro de Computo CNSC

- De otra parte, para el ingreso al Centro de computo, se cuenta con un sistema de identificación mediante huella digital y tarjeta para el control de accesos, el registro de acceso al centro de cómputo se realiza por medio de una Bitácora que actualmente está formalizado mediante el *"PROTOCOLO PARA EL CONTROL DE INGRESO AL CENTRO DE CÓMPUTO PR-TI-001"*, A continuación, se presenta el registro fotográfico de lo enunciado:

Foto N 2. Ingreso al Centro de computo



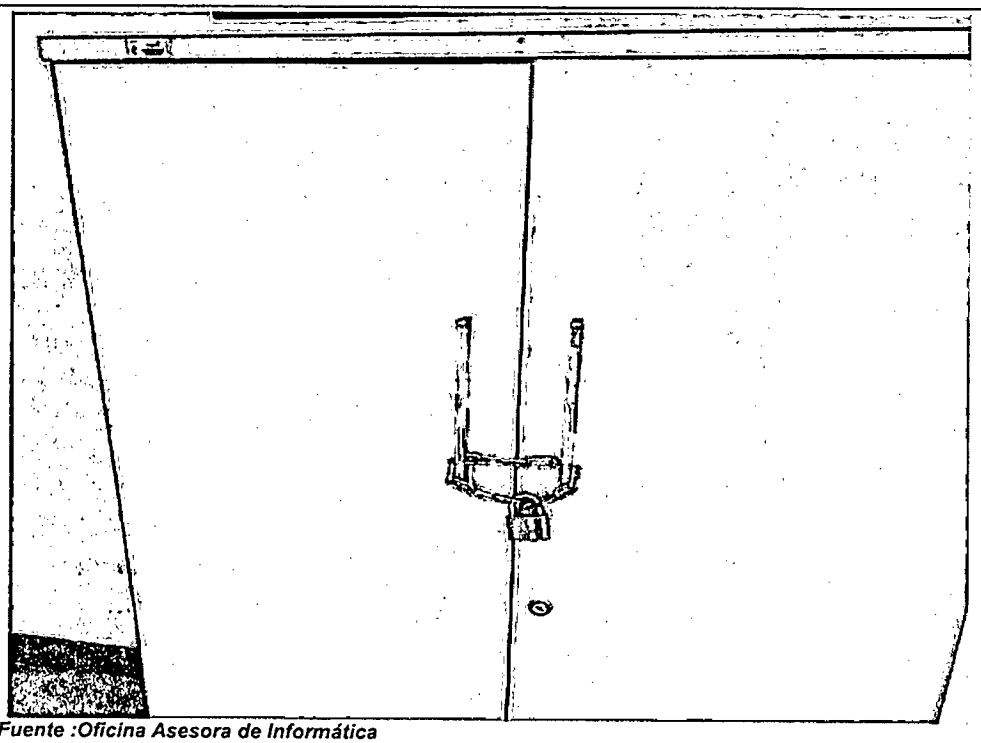


Papel de trabajo: Centro de Computo CNSC

- Adicionalmente, se evidenció incumplimiento a la norma NTC-ISO 27001: 2013 Numeral A.17 (Aspectos de Seguridad de la Información de la gestión de Continuidad del Negocio) ya que pese a que se tiene incluida en el plan estratégico de tecnologías de la información PETI 2019-2022 un proyecto tendiente a desarrollar actividades para atender este punto, hoy día no se cuenta con Plan de Continuidad del Negocio, pues no se tiene un sitio alterno del centro de cómputo en caso de presentarse situaciones no previstas y/o desastres naturales.

- Los Backups de la información se realizan mediante unidad robótica, estas copias (Cintas) se almacenan en un mueble, donde no cuenta con las condiciones físicas y ambientales (luz, humedad relativa, entre otros), necesarias para garantizar la adecuada custodia y recuperación de la información allí contenida, lo que deja descubierto el riesgo de pérdida de la información, pues no se cuenta con una cintoteca, lo que evidencia incumplimiento a la NTC-ISO– IEC 27001:2013, Numeral A.12 (Copias de respaldo).

Foto No 3. Mueble la seguridad es un candado con una cadena



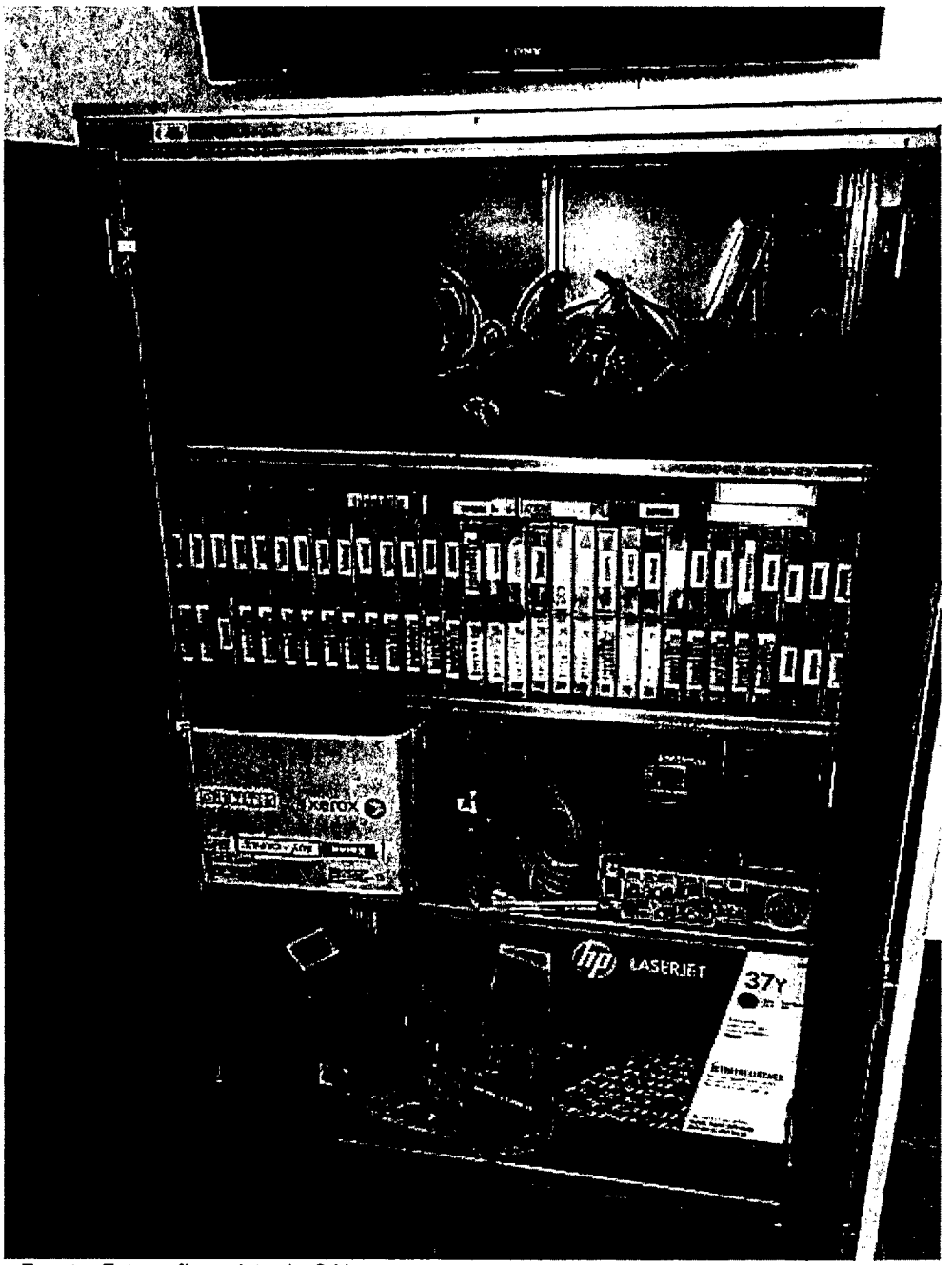
Fuente :Oficina Asesora de Informática

- No obstante, se cuenta con un documento interno de trabajo, el cual describe las actividades relacionadas con la programación y el detalle de la toma de los backups que realiza la Oficina Asesora de Informática, sin embargo el documento no está controlado de acuerdo con el procedimiento P-SG-005 versión 3 en el paso 1 del numeral 6.1 Elaboración, actualización y control de documentos, tampoco se evidenciaron políticas y procedimientos de respaldos, restauración, custodia, eliminación/baja de medios y retención, lo que evidencia incumplimiento a la NTC-SIO-IEC 27001:2013.

- De la misma manera en el PETI 2019 – 2022 se registró una actividad para contratar el servicio de custodia de medios magnéticos a hoy la gestión de los medios magnéticos se encuentra en el estado descrito.

- Adicionalmente, durante la realización de la visita en sitio se evidenció que no se cuenta con un rol especifico de custodia y/o un adecuado control del mismo pues los contratistas de mesa de ayuda y el administrador de las cintas de Backup de la Oficina Asesora de Informática, operan y abren el gabinete cuando lo requieren: lo anterior genera incumplimiento frente a las buenas prácticas de seguridad de la información definidas en la NTC-ISO-IEC 27001:2013.tal como se observa a continuación:

Foto N4 presentación mueble donde se almacena las cintas Backups



Fuente. Fotografía registrada OAI

- Del Procedimiento Recibo de Discos Duros Universidades P-TI-004, versión 2.1 del 12 de octubre de 2016 ya que se evidenció lo siguiente:

  ➢ Debilidades, e incumplimientos en el diseño y aplicación del procedimiento P-TI-004 versión 2.1., del 12 de octubre 2016, así como desactualización del mismo, incumpliendo

lo establecido en el procedimiento P-SG-005 versión 3 en el paso 1 del numeral 6.1 Elaboración, actualización y control de documentos el cual define que se debe revisar periódicamente los documentos del proceso con el fin de identificar la necesidad de diseño, ajuste o eliminación, adicional se incumplió lo definido en la ISO- IEC- NTC 27001:2013 en los numerales: *A.12.1.1Documentación de los procedimientos de operación* ya que se encontraron las siguientes situaciones:

- En el numeral "4 Normativa Aplicable" del procedimiento P-TI-004 versión 2.1, se registra la NTCGP1000:2009 Norma Técnica Colombiana de la Gestión Pública, norma que fue Derogada mediante el Decreto 1499 de 2017 Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.

- En el numeral 6 Desarrollo del procedimiento, se evidenció que en el paso 1. Se describe el instructivo denominado "protocolo de seguridad" el cual no es un documento oficial ya que no existe en la intranet de la Entidad. De igual manera se evidenció desactualización de los pasos 5,6,7,8,10 y 11 ya que difieren de la actualidad del procedimiento, dado que se ejecutan mediante el aplicativo SIMO.

- En lo referente al responsable en los pasos 3 y 5 se debe cambiar a la actualidad

- El flujograma del procedimiento para la actividad 5 se describe "***Entregar el disco duro al área de Informática***". Lo anterior evidencia que lo descrito en los pasos del procedimiento no es concordante con lo registrado en el flujo grama.

Hallazgo 3: Matriz Consolidada Riesgos OAI

- De los controles asociados a los riesgos identificados para los procesos Gestión de tecnologías de la Información y Gestión de Recursos Tecnológicos se evidenciaron debilidades relacionadas con la gestión y Administración de los riesgos, de acuerdo con lo expuesto a continuación:

  - Se evidenció debilidad en la descripción y definición en 18 de 18 (100%) controles asociados a los 18 riesgos identificados, analizados y valorados y registrados en la matriz consolidada de riesgos institucionales por proceso publicada en la intranet de la Entidad, para el proceso Gestión de Recursos Tecnológicos, y para 12 de 12 (100%) controles asociados a los 12 riesgos definidos para el proceso Gestión de tecnologías de la Información ya que no cuentan con 1 o más de los 6 componentes que debe contener un control, tales como: responsable, periodicidad, propósito del control, como realizar la actividad, indicar que pasa con las observaciones o desviaciones y la evidencia. Lo anterior deja descubiertos el 100% de los riesgos definidos para los dos (2) procesos, incumpliendo así lo definido en la "*Guía para la administración del riesgo y el diseño de controles en entidades públicas DAFP*" Versión 4 octubre 2018 y lo establecido en el Manual Operativo del Modelo integrado de gestión y Planeación, reglamentado mediante el Decreto 1499 de 2017, en el

numeral 4.2.1 Seguimiento y evaluación del desempeño institucional, en donde se establece en el ambiente de control lo siguiente: "*Cuando se detecten desviaciones en los avances de gestión e indicadores, o posibilidad de materialización de un riesgo, es indispensable que el responsable establezca las acciones de mejora de manera inmediata. La utilidad de este ejercicio es apoyar la toma de decisiones para lograr mejores resultados, gestionar con mayor eficacia y eficiencia los recursos y facilitar la rendición de cuentas a los ciudadanos e informes a los organismos de control" ... y en otro acápite de define que: "La Entidad debe establecer la planeación estratégica, responsables, metas, tiempos que faciliten el seguimiento y aplicación de controles que garanticen de forma razonable su cumplimiento. Así mismo a partir de la política de riesgo, establecer sistemas de gestión de riesgos y las responsabilidades para controlar riesgos específicos bajo la supervisión de la alta dirección".* Con base en esto, establecen los mapas de riesgos en los diferentes niveles. En este sentido, teniendo en cuenta que los controles son débiles y los riesgos están descubiertos, la gestión del riesgo no cumple con la normativa vigente.

- De otra parte, se evidenció que 4 de 18 es decir el 22% de los riesgos identificados, analizados, valorados y registrados en la matriz consolidada de riesgos institucionales por proceso publicada en la intranet de la Entidad, para el proceso Gestión de Recursos Tecnológicos, no son aplicables a dicho proceso sino al proceso encargado de la infraestructura de la Entidad. Los riesgos son los siguientes:

  - Conato o Incendio en el centro de cómputo.
  - Fallas eléctricas.
  - Inadecuado control de visitantes y/o contratistas.
  - Inadecuado control de personal de mantenimiento y limpieza.

- Se evidenció que 3 de 18 es decir el 16% de los riesgos asociados al proceso de Gestión de Recursos Tecnológicos, cuyo nivel de riesgo inherente (valoración del riesgo) que se encuentran en zona Alta, luego de aplicar controles, el nivel de riesgo residual continúa en zonal Alta, es decir que los controles no son efectivos o son débiles y a pesar de contar con plan de tratamiento de riesgos puede generarse desgaste administrativo, así como la materialización de los riesgos identificados. Lo anterior evidencia debilidad en la gestión y administración del riesgo, incumpliendo lo definido en la "Guía para la administración del riesgo y el diseño de controles en entidades públicas DAFP" Versión 4 octubre 2018 y en lo establecido en el Manual Operativo del Modelo integrado de gestión y Planeación, reglamentado mediante el Decreto 1499 de 2017. Los riesgos son los siguientes:

  - Inadecuado control de visitantes y/o contratistas riesgo aplicable a otro proceso).
  - Pérdida de información
  - Ataques informáticos

- Es importante precisar que resulta necesario solicitar a la Oficina Asesora de Planeación, acompañamiento y asesoría en la revisión y ajustes del mapa de riesgos del proceso, por ser dicha oficina la dependencia responsable del sistema de Gestión

de Riesgos en la Entidad.

Observación 1. Sistema de información SIMO

Se evidenció debilidad en la adecuada gestión, de cara a la atención y servicio a la Ciudadanía. Lo anterior de acuerdo con lo evidenciado en la información recolectada mediante las PQRS archivo reportado por la dependencia *Atención al Ciudadano* mediante correo electrónico del 12 de agosto de 2019, ya que de 35.417 PQRS presentadas en el periodo comprendido entre junio de 2018 y junio de 2019, 2.500, correspondieron al tipo de imposibilidad de acceder o realizar transacciones en el SIMO debido a fallas, y/o bloqueos del Sistema de Información.

Hallazgo 4: Sistema de Gestión de Seguridad de la Información: Análisis de los 18 Dominios y 114 controles definidos en el Anexo A ISO27001:2013.

Como resultado de la encuesta realizada al anexo A de la norma ISO 27001:2013 que contiene los 18 dominios y 114 controles, y verificando las evidencias presentadas por el profesional que atendió la auditoria, se describe dominio a dominio el aspecto a mejorar. Es importante tener en cuenta que la gestión de la seguridad de la información requiere de una estrategia alineada con la entidad y sus objetivos, adicionalmente, se requiere de recursos y de un conjunto de actividades dirigidas y coordinadas por la Alta Dirección, de modo que se despliegue hacia toda la Entidad y en todos los niveles jerárquico hacia los usuarios finales. Lo anterior teniendo en cuenta la Resolución 201712000582225 del 19/09/2019 que adopta y actualiza la política del Sistema de Gestión de Seguridad de la Información tal como lo manifestó la mesa de trabajo conformada por la Oficina Asesora de Planeación, Dirección de Apoyo Corporativo, Oficina Asesora Jurídica y Oficina Asesora de Informática en lo referente al compromiso institucional de implementar el subsistema como parte integral del sistema integrado de gestión. El análisis obtenido por dominio se presenta a continuación:

A5 Política de Seguridad de la información: Cumplimiento 90%

Si bien se cuenta con la política documentada y aprobada por la Alta Dirección, al corte de la evaluación no se evidenció revisión de la misma. Se recomienda dar celeridad a dicha revisión.

A6 Organización de la Seguridad de la Información: Cumplimiento 46%

Si bien se cuenta con el M-SG-SI-001 Manual de Responsabilidades, documento que contiene los diversos niveles de responsabilidad de los colaboradores de la Comisión frente al SGSI, no se evidencia adecuada distribución o segregación, entre las funciones y las áreas de responsabilidad para reducir las oportunidades de la modificación no autorizada o uso inadecuado de los activos de información. De igual manera no se ha oficializado el documento relacionado con contacto con autoridades (Guía para la gestión de los grupos de interés y las autoridades en la CNSC.) y en cuanto a gestión de proyectos, no se ha presentado a la Comisión los conceptos de Seguridad de la Información para emprender actividades institucionales que se puedan gestionar como proyectos. A la fecha no se manejan formalmente los proyectos en el marco de la Administración de proyectos. Se propone elaborar un documento de recomendaciones para incluir elementos de Seguridad de la Información en Proyectos Institucionales. En materia de teletrabajo, si bien se cuenta con el Manual M-SG-SI-002 Políticas de Direccionamiento Estratégico que describe lo relacionado, no fue posible

verificar la implementación correcta del tema.

A7 Seguridad de los recursos humanos: Cumplimiento 100%

Se cuenta con el diseño y aplicación de los procesos de selección, así como de términos y condiciones del empleo debidamente diseñado e implementado.

A8 Gestión de Activos: Cumplimiento 43,9%

Si bien se cuenta con un inventario de información, el mismo se encuentra obsoleto, ya que fue realizado en diciembre de 2017, no ha sido oficializada la política de activos de la información, ni el procedimiento de gestión de activos de la información.
De igual manera se cuenta con el instructivo I-RT-002 para el uso adecuado de los recursos tecnológicos, pero no se han oficializado: la Política de Gestión de Activos de Información (Archivo: 2019_Gestión-activos-información_Documento-implementación.docx) ni el Procedimiento de Gestión de Activos de Información (Archivo: Procedimiento_GestionActivosInformacion_v01.bpm (y docx). De igual forma no se han oficializado los documentos para la clasificación, etiquetado y manejo de la información, así como para el manejo de activos.
No se han oficializado ni implementado documentos ni controles respecto de gestión de medios removibles, disposición de los medios de soporte y transferencia de medios de soporte físico y no se cuenta con controles adecuados para la correcta restricción y acceso a internet.

A9 Control de Acceso. Cumplimiento 44,5%

Es de gran importancia limitar el acceso a información y a instalaciones de procesamiento de información asegurando el acceso de los usuarios autorizados y evitando el acceso no autorizado a sistemas y servicios. Se observa que en la Entidad hace uso de contraseñas como medida para restringir el acceso a sus sistemas y se tiene conocimiento de la necesidad de desarrollar políticas de control de accesos, gestión de contraseñas y gestionar correctamente escenarios como el teletrabajo, por lo cual han tomado medidas basadas en las buenas prácticas. Sin embargo, existe documentación parcial y se encuentran en construcción nuevos documentos.

Se cuenta con el Manual M-SG-SI-002 Políticas de Direccionamiento Estratégico, Sistema de control de acceso al centro de cómputo, Control de acceso a la propiedad horizontal, Control de acceso a la sede principal de la Comisión en el piso 7, documento que contempla una política de control de acceso con base en los requisitos del negocio en cuanto a seguridad, pero está desactualizada y no ha sido revisada.

En cuanto a gestión de usuarios, si bien se cuenta con el procedimiento para la gestión de recursos tecnológicos, que describe algunas actividades asociadas, el mismo se encuentra desactualizado, obsoleto y no da respuesta completa al subdominio mencionado.

A10 Criptografía: Cumplimiento 100%

Con la criptografía se busca asegurar el uso apropiado y eficaz de ésta, para proteger entre otras la confidencialidad, integridad y no repudiación de la información. Se evidenció la mención de forma general a las políticas de controles criptográficos en el documento Políticas de Direccionamiento Estratégico, pero no existen procedimientos escritos sobre el uso protección y tiempo de vida de las llaves criptográficas.
Se evidenció el uso de controles criptográficos, como por ejemplo el uso de conexiones VPN a través de los firewalls de la Entidad, sin embargo, como ya no se han determinado de forma oficial criterios para establecer tiempos de vida o políticas de gestión de las llaves criptográficas.

Mediante el documento: M-SG-SI-002 Políticas de Direccionamiento Estratégico se cuenta con la implementación de la política sobre uso de controles criptográficos y adecuado uso en la organización de llaves públicas y privadas. No obstante, no fue posible validar que lo enunciado en el Manual se encuentre debidamente implementado.

A11 Seguridad física y del entorno: Cumplimiento 34,4%

No se cuenta con la correcta implementación y controles diseñados que validen la adecuada seguridad respecto de: perímetro de seguridad física, controles de acceso físico, seguridad de oficinas, recintos e instalaciones, protección contra amenazas externas y ambientales, trabajo en áreas seguras y áreas de carga, despacho y acceso público y equipos, servicios públicos de soporte, seguridad en el cableado, mantenimiento de los equipos, retiro de activos, seguridad de los equipos fuera de las instalaciones, disposición segura o reutilización de los equipos, equipos de usuarios desatendidos. Si bien se cuenta con el instructivo, para uso adecuado de los recursos tecnológicos I-RT-002, y la política de direccionamiento estratégico M-SG-SI-002 formalizados, no se evidenció aplicación de la política de escritorio y pantalla limpia, así como la adecuada ubicación y protección de equipos.

A 12 Seguridad de las Operaciones: Cumplimiento 49,3%

Se cuenta con el procedimiento gestión de cambios, que describe los cambios de los servicios y los sistemas de procesamiento de información y se realizan actividades de control haciendo uso de las Herramientas de monitoreo Zabbix, Foglight, no obstante, no se han oficializado el total, de documentos asociados a la operación.

De igual forma se cuenta con una consola de antivirus y con equipos de seguridad perimetral (firewalls), sin embargo, no existe evidencia objetiva de la adecuada y completa aplicación de medidas preventivas de detección, prevención y recuperación de protección contra códigos maliciosos y procedimientos de concientización a usuarios. En materia de copias de respaldo de la información, se cuenta con dos (2) consolas de gestión de copias para las diferentes plataformas de equipos de la comisión, no obstante, las Políticas de backups se encuentran en revisión y ajustes.

No se cuenta con documento formal que defina lineamientos para la correcta aplicación de controles y verificaciones en sistemas de operaciones para minimizar el riesgo de interrupciones

a los procesos del negocio.

A 13 Seguridad de las Comunicaciones: Cumplimiento 55%

El objetivo de la Entidad de asegurar la protección de la información en las redes y la transferencia de información, se ha enfocado en la implementación de controles para proteger la confidencialidad, integridad y disponibilidad de la información publicada y transferida en los escenarios LAN y WAN de la Entidad. Se hace necesario contar con documentación formalizada que defina lineamientos sobre la correcta aplicación de controles para el acceso a los datos y a las funciones del sistema de aplicaciones y su respectiva restricción, en la seguridad de servicios de red, en la separación de las redes. Los documentos asociados se encuentran en construcción.

Se cuenta con políticas definidas en materia de transferencia de información (M-SG-SI-002 Políticas de Direccionamiento Estratégico y el instructivo I-RT-001 Protección de la información digital - Herramienta de cifrado). Se cuenta con controles para la adecuada gestión sobre acuerdos sobre transferencia de información, mensajes electrónicos y acuerdos de confidencialidad.

A 14 Adquisición, desarrollo y mantenimiento de Sistemas: Cumplimiento 46,7%

Se está efectuando el despliegue de una nueva versión del procedimiento de desarrollo de software que contenga la situación actual del proceso y elaboración de un documente que explique la forma en que se controla el código fuente. No obstante, no se cuenta con documentos formalizados que contengan la descripción de controles en materia de Seguridad de servicios de las aplicaciones en redes públicas y de Protección de transacciones de servicios de aplicaciones.

Sobre seguridad en los procesos de desarrollo y de soporte, se está efectuando el despliegue de una nueva versión de los procedimientos de: desarrollo de software que contenga la situación actual del proceso y elaboración de un documente que explique la forma en que se controla el código fuente y revisión técnica de aplicaciones después de cambios en la plataforma de operaciones. Se evidencian debilidades en la aplicación del procedimiento gestión de cambios, P-TI-005, instructivo de actualización de la plataforma de equipos tecnológicos e Instructivo de control de código fuente de proyectos de software. Se evidencian debilidades en la gestión de ambiente de desarrollo seguro, en la aplicación y actualización oportuna de los documentos asociados a desarrollo de software contratado, Gestión Ambientes de Pruebas para Desarrollo Software y protección de datos de prueba.

A15 Relaciones con proveedores. Cumplimiento: 53%

Si bien se cuenta con el documento M-SG-002 Políticas de Direccionamiento estratégico, con el formato informe complementario de supervisión periódico o final de los contratos (F-CT-022) no se cuenta con un tratamiento de la seguridad dentro de los acuerdos con los proveedores, ni una cadena de suministro de tecnología de información y comunicación; Se debe establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la Entidad y se debe definir acuerdos con los

proveedores y estos incluyen requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.

A16 Gestión de los Incidentes de la seguridad de la información. Cumplimiento: 74%

En cuanto a responsabilidades y procedimientos de gestión para asegurar respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información, así como procedimientos formales para reportar los eventos de seguridad de la información y su respectiva clasificación se cuenta con el procedimiento P-SG-SI-001 Gestión de Incidentes de Seguridad de la Información, con el formato F-SG-SI-001 - Registro de Fallas e informes de análisis de incidentes, no obstante no se cuenta con evidencia objetiva de su debida implementación, Igualmente, se cuenta con el manual de responsabilidades M-SG-SI-001 Manual de Responsabilidades y el formato F-SG-SI-001 registro de fallas, pero no se exige a la totalidad de empleados, contratistas y usuarios de terceras partes de los sistemas de y servicios de información a reportar todas las debilidades observadas o sospechadas en los servicios.

No se cuenta con documentos formalizados e implementados sobre mecanismos utilizados cuantificar, monitorear los tipos, los volúmenes, y los costos de los incidentes de seguridad de la información y de mal funcionamientos.

El procedimiento P-SG-SI-001 Gestión de Incidentes de Seguridad de la Información no define lineamientos para recolectar, retener y presentar evidencia cuando un evento de seguridad implica acciones legales (civiles o penales) contra una persona u organización, para cumplir las reglas establecidas en la jurisdicción pertinente.

A17 Aspectos de Seguridad de la información de la gestión de continuidad del negocio. Cumplimiento: 0%

No se cuenta con plan de continuidad del negocio, la Entidad no ha diseñado, formalizado e implementado los requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre. Se observa en el PETI 2019-2022 actividades planeadas para atender este punto, pero a la fecha la entidad adolece de esta estrategia.

La entidad no ha establecido, documentado, implementado ni mantenido procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.

La entidad no ha verificado en intervalos regulares los controles de continuidad de la seguridad de la información implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas. En las instalaciones de procesamiento de información no se han implementado controles con redundancia suficiente para cumplir los requisitos de disponibilidad. Aunque la entidad cuente con infraestructura tecnológica redundante se hace necesario evidenciar documentalmente esta situación para apoyar tecnológicamente la recuperación de la operación de los procesos misionales ante el caso de presentarse una situación adversa en el marco de un plan de recuperación ante desastres.

A.18 Cumplimiento con requerimientos legales y contractuales. 71%
La entidad ha referenciado normativas y disposiciones legales vigentes relacionadas con el resguardo de la propiedad intelectual y las demás concordantes de aplicabilidad identificadas en el Nomograma - Proceso Gestión de Tecnologías de la Información, Proceso Gestión de Recursos Tecnológicos. Sin embargo, durante el desarrollo de la auditoria, no se evidenció adecuados controles para la protección de los registros, privacidad y protección de información de datos personales; lo anterior así lograr cumplir con el 100% de su implementación para este dominio.

3. CONCLUSIONES DE LA AUDITORÍA

CONCLUSIONES Y RECOMENDACIONES

Sobre la encuesta de satisfacción a usuarios internos sobre el aplicativo GLPI:

- Evaluar la forma de fortalecer las capacitaciones en el manejo del aplicativo, tanto para los colaboradores que son vinculados a la entidad, como suministrar reentrenamientos a quienes ya conocen el GLPI, con el fin de lograr el entendimiento del mismo, su manejo y beneficios por parte de los colaboradores de la CNSC, lo anterior en razón a que en un número importante de respuestas se recomendó fortalecer la capacitación no solo para los que ingresan por primera vez a la entidad, si no para quienes ya están vinculados, en el manejo del sistema de información.

- Evaluar la forma de permitir que los usuarios del sistema de información GLPI de manera fácil y amigable en lenguaje que a todos se les facilite entender, puedan tipificar correctamente la categoría adecuada para el servicio que se requiere, lo anterior en razón a que un porcentaje importante de respuestas de usuarios, manifestaron que no es claro no pueden tipificar las diferentes categorías.

- Realizar seguimiento y dejar trazabilidad de los mismos, a las soluciones brindadas con ocasión de los incidentes y requerimientos resueltos y que han sido registrados en el aplicativo GLPI, con el objetivo de fortalecer la cobertura, atención a requerimientos e incidentes y propiciar acciones que promuevan la mejora continua al SGSI. Lo anterior, debido a que se evidenció que no se realiza seguimiento a las soluciones brindadas con ocasión de los incidentes y requerimientos resueltos.

Sobre los procesos:

- La Oficina Asesora de Informática, cuenta con dos procesos de gestión, que busca un único objetivo común y es la adecuada gestión de los recursos de la tecnología, para atender las necesidades de la CNSC generando un desgaste Administrativo, por lo anterior se recomienda que se unifique en un único proceso estratégico

Sobre los procedimientos

- Revisar, actualizar, ajustar, formalizar y socializar los procedimientos: Mesa de Servicio con código P-RT-003 versión 2.1., del 10 de octubre de 2016, Gestión y Operación de la Infraestructura Tecnológica con código P-RT-001 versión 1.0 del 29 de febrero de 2016, Mantenimiento de Soluciones Informáticas P-RT-002, Procedimiento verificación acuerdo de niveles de servicio del sistema de comunicaciones, de la capacidad computacional y de carácter procedimental, que use la universidad o IES - P-TI-002 Procedimiento Proyección de Adquisición y Crecimiento de Infraestructura - P-IT-003, Procedimiento Recibo de Discos Duros Universidades P-TI-004 versión 2.1., del 12 de octubre 2016. Tanto en la normatividad vigente aplicable, como en la descripción y secuencia de las actividades registradas, de modo que den respuesta adecuada y coherente a la actualidad del proceso.

- Llevar a cabo el Plan de Contingencia consignado en el PETIC 2019 - 2022 y políticas que permitan un adecuado sistema de seguridad física y lógica en previsión de desastres, estableciendo medidas destinadas a salvaguardar la información contra los daños producidos por hechos naturales o por el hombre. La información como uno de los activos más importantes de la entidad, debe ser el fundamento más importante en el Plan de Contingencia.

Sobre la gestión y administración de Riesgos de los procesos objeto de la evaluación:

- Revisar, ajustar, fortalecer y complementar los 18 controles asociados a los 18 riesgos del proceso Gestión de Recursos tecnológicos, así como los 12 controles asociados a los 12 riesgos del proceso Gestión de Tecnologías de la información, de modo que cada control cuente con los seis (6) componentes definidos en la "Guía para la administración del riesgo y el diseño de controles en entidad públicas del DAFP" versión 4 de octubre de 2018, con el objetivo de dar efectivo cubrimiento y mitigar correctamente los riesgos identificados, analizados, y valorados para los dos (2) procesos.

- Revisar y ajustar de ser necesario, los riesgos identificados, valorados, analizados y registrados en la matriz de riesgos institucionales por proceso, para el proceso de Gestión de Recursos Tecnológicos, de modo que se cuente con riesgos que realmente estén relacionados con el objetivo del proceso y no que sean aplicables a otros procesos.

  Lo anterior, en razón a que se evidenció que 4 de 18 riesgos del proceso Gestión de Recursos Tecnológicos, no son aplicables a dicho procesos, sino al proceso responsable de las instalaciones físicas de la Entidad.

Sobre la verificación del grado de implementación del Sistema de Seguridad de la información (SGSI) de la CNSC en el marco de los requisitos definidos en la NTC-ISO- IEC 207001:2013

- Presentar resultados del grado de avance en la implementación del SGSI al comité del

Sistema Integrado de Gestión – SIG, con el fin de contar con información sobre la gestión adelantada, de modo que la Alta Dirección pueda tomar acciones sobre la mejora continua. Aunque actualmente, se cuenta con el comité, se evidenció mediante, correo enviado el pasado 22 de agosto de 2019 a la Oficina de Control Interno, que no se presentan resultados sobre el grado de avance de la implementación del SGSI, tal como lo demanda la NTC-ISO 27001:2013.

- Dar efectivo cumplimiento a lo enunciado en la NTC-ISO 27001:2013, específicamente en realizar y evidenciar resúmenes de los análisis de incidentes y vulnerabilidades de seguridad de la información, así como su respectiva presentación a la Alta Dirección para que se cuente con información necesaria para la toma de decisiones que encaminen al SGSI hacia la mejora continua. Lo anterior en razón a que durante la realización del diagnóstico se evidenció que en la Entidad no se realizan y tampoco son presentados ante la gerencia de la Entidad, incumpliendo lo definido en la norma mencionada.

- Contar con el equipo necesario la implementación de la NTC-ISO 27001 en la Entidad, ya que se evidenció que no existe un equipo de trabajo completo, generando así incumplimiento en el numeral 5.1 de la norma enunciada.

- Elaborar, formalizar, oficializar y realizar asignación sobre la protección de activos individuales claramente definidos en la Entidad, lo anterior ya que no se evidenciaron registros que demuestren lo enunciado, incumpliendo el numeral A12 de la NTC-ISO 27001, pues el archivo enviado a la Oficina de Control Interno, por parte de la Oficina Asesora de Informática mediante CD y/o correo electrónico del 25 de Julio de 2019, no se encuentra adoptado ni controlado por el Sistema Integrado de Gestión.

- Fortalecer las campañas de sensibilización para asegurar que los empleados y contratistas tomen conciencia y den cumplimiento a sus responsabilidades en materia de seguridad de la información.

- Implementar un canal de reporte anónimo de incumplimiento de políticas o procedimientos de seguridad de la información ("Denuncias internas") de modo que los clientes internos de la Entidad, puedan participar y aportar propuesta de mejora en lo que respecta a la gestión de la seguridad de la información. Lo anterior ya que no se evidenció dicho mecanismo, tal y como lo establece el numeral 7.2.1, de la GTC-ISO/IEC 27001:2013.

- Fortalecer e implementar estrategias para el cumplimiento adecuado de la política de puesto de trabajo despejado y bloqueo de pantalla asegurando así que los empleados y contratistas tomen conciencia de sus responsabilidades y la cumplan. Lo anterior con el fin de implementar correctamente el SGSI y garantizar la adecuada seguridad de la información que es responsabilidad de los colaboradores de la CNS

- Fortalecer los procedimientos de operación documentándolos y poniéndolos a

disposición de todos los usuarios que los necesitan, con el fin de que todos los colaboradores tengan acceso a la documentación del SGSI y se fomente la cultura de la mejora continua en lo que respecta al SGSI, tal como lo define la NTC-ISO-IEC 27001:2013.

- Fortalecer las copias de respaldo de información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con las políticas de copias de respaldo acordadas, incluyendo: Requisitos de retención y protección, así como, terminar de implementar la herramienta con que se hace el backups VEAM de modo que se de adecuado cumplimiento con lo establecido en el numeral 8.11.3 Copias de Seguridad de la Información del Manual de Políticas de Seguridad de la Información 1 que menciona: "Seguridad del almacenamiento de backups... Los controles aplicados a los medios del sitio principal deben ser extendidos al sitio de respaldo externo..." (Subrayado fuera del texto).

- Fortalecer las políticas de desarrollo seguro, así como los respectivos controles para establecer y aplicar las reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la Entidad y los cambios de los sistemas dentro del ciclo de vida de desarrollo de software, de modo que se dé adecuado cumplimiento a lo definido en la NTC-IEC-ISO 27001:2013.
- Fortalecer la política para el reporte y tratamiento de incidentes de seguridad mediante controles que permitan asegurar una respuesta rápida eficaz y ordenada a los incidentes de Seguridad de la Información, sensibilizar a los empleados y contratistas para tomar conciencia de su responsabilidad de reportar eventos de seguridad de la información.

- Según lo establecido en el PETIC 2019 – 2022 realizar los planes de continuidad de negocio, análisis de impacto del negocio (planes de contingencias, sedes alternas) y planes de recuperación desastre, a través de la generación de estrategias diversas tales como sensibilizaciones, capacitaciones, ejercicios de suplencia escalonados, etc., para disminuir el nivel de impacto, en la posibilidad de materializarse un evento que pudiese afectar la operación del negocio. Así mismo verificar a intervalos regulares los controles de continuidad de la Seguridad de la Información establecidos e implementados, con el fin de asegurar que son eficaces durante situaciones adversas.

- Desde la Alta Dirección, se debe demostrar liderazgo y compromiso con respecto al SGSI como lo establece la norma en su numeral 5. Liderazgo , que indica lo siguiente:

a. Asegurando que se establece la política y los objetivos del SGSI.
b. Asegurando la integración de los requisitos del SGSI con los procesos de negocio
c. Asegurando la disponibilidad de los recursos necesarios
d. Comunicando la importancia de una gestión eficaz y de conformidad con los requisitos del SGSI.
e. Asegurando que el SGSI logre los resultados previstos.

f. Dirigiendo y apoyando al personal para aportar a la eficacia del SGSI.
g. Promoviendo mejora continúa.

Lo anterior se menciona dado el porcentaje de implementación que se obtuvo, con respecto al SGSI y a que no se evidenciaron soportes (actas d comité) de que la Alta Dirección tome decisiones sobre la implementación de dicho sistema.

- Revisar y dar adecuado cumplimiento a las siguientes directrices de control de cambio en sistemas: a) llevar un registro de los niveles de autorización acordados; b) asegurar que los cambios se presenten a los usuarios autorizados; c) revisar los controles y procedimientos de integridad para asegurar que no se vean comprometidos por los cambios; d) identificar todo el software, información, entidades de bases de datos y hardware que requieren corrección; e) identificar y verificar el código crítico de seguridad para minimizar la posibilidad de debilidades de seguridad conocidas; f) obtener aprobación formal para propuestas detalladas antes de que el trabajo comience; g) revisar antes de la implementación, asegurar que los usuarios autorizados aceptan los cambios; h) asegurar que el conjunto de documentación del sistema está actualizado al completar cada cambio, y que la documentación antigua se lleva al archivo permanente, o se dispone de ella; i) mantener un control de versiones para todas las actualizaciones de software; j) mantener un rastro de auditoría de todas las solicitudes de cambio; k) asegurar que la documentación de operación y los procedimientos de los usuarios experimenten los cambios que les permitan seguir siendo apropiados; l) asegurar que la implementación de los cambios ocurre en el momento correcto y no afecta los procesos de negocio involucrados contratado externamente; m) seguir adelantando los acuerdos de licenciamiento, propiedad de los códigos y derechos de propiedad intelectual relacionados con el contenido contratado.

- Revisar las siguientes directrices: revisión técnica de las aplicaciones después de cambios en la plataforma de operación: a) revisar los procedimientos de integridad y control de aplicaciones para asegurar que no estén comprometidos debido a los cambios en las plataformas de operaciones; b) asegurar que la notificación de los cambios en la plataforma operativa se hace a tiempo para permitir las pruebas y revisiones apropiadas antes de la implementación; c) asegurar que se hacen cambios apropiados en los planes de continuidad del negocio. Lo anterior en razón a que el procedimiento gestión de cambios P-TI-005 no cuenta con directrices a lo enunciado, ni con evidencias de su correcta implementación y en la entidad no se protege adecuadamente los ambientes de trabajo seguro para las actividades de desarrollo e integración de los sistemas que comprenden todo el ciclo de vida de desarrollo de sistemas.

- Revisar las siguientes directrices para dar respuesta a incidentes de seguridad de la información:

  - Los incidentes son contenidos y la probabilidad de que vuelvan a ocurrir mitigada.
  - Se debe contar con un plan de recuperación de incidentes durante o después del

mismo.

- Recolectar evidencia lo más pronto posible después de que ocurra el incidente;
- Llevar a cabo análisis forense de seguridad de la información, según se requiera
- Llevar el asunto a una instancia superior, según se requiera;
- Asegurar que todas las actividades de respuesta involucradas se registren adecuadamente para análisis posterior; Comunicar la existencia del incidente de seguridad de la información o de cualquier detalle pertinente a él, al personal interno o externo a las organizaciones que necesitan saberlo;
- Tratar las debilidades de seguridad de información que se encontraron que causan o
- contribuyen al incidente;
- Establecer que una vez que el incidente se haya tratado lo suficiente, cerrarlo formalmente y hacer un registro de esto.

Lo anterior en razón a que si bien se cuenta con el procedimiento P-SG-SI-001 Gestión de Incidentes de Seguridad de la Información, el formato F-SG-SI-001 registro de fallas e informes de análisis de incidentes, dichos documentos no establecen los lineamientos definidos en la norma NTC-ISO-IEC 27001:2013.

- Diseñar e implementar mecanismos para cuantificar y monitorear los tipos, los volúmenes y los costos del incidente de la Seguridad de la Información. Lo anterior en razón a que, en la entidad, no existen implementados mecanismos para cuantificar, monitorear los tipos, los volúmenes, y los costos de los incidentes de seguridad de la información y de mal funcionamiento.

- Diseñar e implementar un BCP (Bussines Continuity Plan) y un DRP (Disaster Recovery Plan) y el BIA (Bussines Impact Analysis) que contenga:

  - Una estructura organizacional adecuada para prepararse, mitigar y responder a un evento contingente, usando personal con la autoridad, experiencia y competencia necesarias.
  - Personal formalmente asignado de respuesta a incidentes con la responsabilidad, autoridad y competencia necesarias para manejar un incidente y mantener la seguridad de la información.
  - Planes aprobados, procedimientos de respuesta y recuperación documentados, en los que se especifique en detalle como la organización gestionará un evento contingente y mantendrá su seguridad de la información en un límite predeterminado, con base en los objetivos de continuidad de seguridad de la información aprobados por la dirección.
  - Realizar pruebas de la funcionalidad de los procesos, procedimientos y controles de continuidad de la seguridad de la información, para asegurar que son coherentes con los objetivos de continuidad de la seguridad de la información.
  - Tener arquitecturas redundantes, ya sea un centro de cómputo principal y otro alterno o componentes redundantes en el único centro de cómputo.

Sobre el Sistema de Información SIMO

- El sistema de información Módulo SIMO cuenta con una arquitectura que permite centralizar el almacenamiento y administración de la información, incrementando de manera significativa los niveles de seguridad con respecto a los aplicativos cliente/servidor; la interrelación con el usuario final es amigable e intuitiva; sin embargo, presenta problemas de disponibilidad (conectividad y/o concurrencia de usuarios) que afectan de manera negativa el nivel de satisfacción de los usuarios, debido a que constantemente se presentan cortes en el servicio durante la ejecución de las operaciones en el registro de la información, afectando el normal funcionamiento a nivel nacional.
- Las herramientas utilizadas para el desarrollo del SIMO (Lenguaje de Programación (PHP DOJO), Motor de Base de Datos (POSTGRES) y Sistema Operativo (LINUX CENTOS)) garantizan niveles de seguridad adecuados y operan de manera sincronizada para alcanzar los objetivos propuestos.
- La confidencialidad del aplicativo SIMO, está basada en la adecuada segregación de funciones establecidas a nivel de roles y perfiles, lo cual permite que cada ciudadano, pueda visualizar únicamente sus procesos.
- Se sugiere que para el ingreso y/o consulta al público se cuente con un sistema de seguridad, tipo capcha, el cual permite realizar la consulta de procesos para el usuario externo, permitiendo ver información solo de sus procesos.
- Diseñar e implementar el sistema de, chat en línea para el SIMO, debido a que la página web de la Entidad ni en la del SIMO se evidenció lo enunciado, por lo tanto, se recomienda implementarlo con el fin de facilitar y/o agilizar la información que requiera la ciudadanía mediante dicho canal de comunicación.

4. FORTALEZAS

El apoyo y disposición brindados por el Jefe de La Oficina Asesora de Informática junto con su equipo de trabajo, así como la entrega oportuna de la información solicitada.

La concientización y/o empeño por parte del equipo de la oficina Asesora de Informática, en cuanto al desarrollo de los procedimientos mejorando y corrigiendo los que están presentes tanto de Gestión de Recursos Tecnológicos como de Gestión de Tecnologías de la Información.

El crecimiento de la infraestructura (Red de Datos, solución de Hiperconvergencia y solución de almacenamiento digital) con el fin de mejorar la calidad, seguridad y rendimiento de la operación tecnológica.

La implementación de soluciones informáticas basadas en software libre y ejercicios InHouse, lo que ahorros significativos a la CNSC y apropiarse del conocimiento tecnológico de las soluciones desarrolladas.

Los sistemas de información que se están desarrollando incluyen plataformas abiertas que permiten facilitar los procesos de interoperabilidad que requiere la Entidad.

La visión e iniciativa de la Oficina Asesora de Informática de desarrollar un proyecto de Arquitectura Empresarial como lo consigna en su PETI 2019 – 2022 permitirá a la entidad contar con una estrategia empresarial que le permita su desarrollo digital alineando procesos de negocio con los procesos de tecnología.

La Oficina Asesora de Informática, a través del Plan Estratégico Tecnológico (PETI 2019 - 2022), ha realizado un análisis de las necesidades y/o oportunidades de mejora, con el fin que la entidad cumpla con el objetivo Misional alineando los objetivos estratégicos con las estrategias operacionales de TI y la formulación de proyectos encaminados al cumplimiento de las metas establecidas.

5. PLAN DE MEJORAMIENTO

Como mecanismo de control y con base en los hallazgos encontrados, la Oficina Asesora de Informática, deberá elaborar un plan de mejoramiento interno, tendiente a corregir y subsanar los puntos susceptibles de mejora, el cual será dado a conocer a la Oficina de Control Interno cinco días hábiles después de la entrega final del informe (30 de septiembre de 2019.)

6. ANEXOS

Matriz ejecutada del ISO27001:2013
Matriz de Riesgos Tecnológicos
Encuesta satisfacción
PQR SIMO
Soportes entregados por OAI

Elaboró	Aprobó
Luz Marlenny Cano Romero **Auditor Líder**	Myriam Nelly Borda **Jefe Oficina de Control Interno**
Gustavo Adolfo Vélez Achury **Jefe Oficina Asesora de Informática**	