	INFORME FINAL DE AUDITORÍA INTERNA	Código: EL_FO_04
		Versión: 9
		Vigente desde: 15/09/2021

PARQUES NACIONALES NATURALES DE COLOMBIA

DIRECCIÓN GENERAL
GRUPO DE CONTROL INTERNO

INFORME FINAL AUDITORIA ESPECIAL
VERIFICACIÓN SEGUIMIENTO REQUISITOS LEGALES EN MATERIA DE TICS EMITIDOS A PARTIR DE LA
EMERGENCIA SANITARIA POR LA PANDEMIA COVID 19

Bogotá, 02 de septiembre del 2022

	INFORME FINAL DE AUDITORÍA INTERNA	Código: EL_FO_04
		Versión: 9
		Vigente desde: 15/09/2021

1. INFORMACIÓN GENERAL

PROCESO O ACTIVIDAD:	Gestión de Tecnologías y Seguridad de la Información.
AUDITOR LÍDER:	Gladys Espitia Peña.
EQUIPO AUDITOR:	Raymon Sales Contreras.
AUDITADO:	Subdirección de Gestión y Manejo de Áreas Protegidas - Grupo de Tecnologías de la Información y las Comunicaciones GTIC.
OBJETIVO:	Realizar seguimiento a la verificación de las acciones realizadas por parte de la Subdirección de Gestión y Manejo de Áreas Protegidas, Grupo de Tecnologías de la Información y las Comunicaciones GTIC de Parques Nacionales Naturales de Colombia PNNC, en lo que corresponde al Decreto 417 del 17 de marzo de 2020 de la Presidencia de la República.
ALCANCE:	Cumplimiento de los Requisitos Legales emitidos a partir de COVID 19 por parte de la Subdirección de Gestión y Manejo de Áreas Protegidas, Grupo de Tecnologías de la Información y las Comunicaciones GTIC del 01 al 30 de junio del 2022.
CRITERIOS-MARCO LEGAL:	Decreto 417 del 17 de marzo de 2020: "...Por el cual se declara un Estado de Emergencia, Económica, Social y Ecológica en todo el territorio Nacional...". Directiva Presidencial 02 de 2020 "Medidas para atender la contingencia generada por el COVID-19, a partir del uso de las tecnologías de la información y las telecomunicaciones – TIC.", Artículo 59 del Decreto Ley 403 de 2020 "acceso y análisis a la información" y la Circular 009 de 2020 de la contraloría general de la república "plan de transición de acceso a fuentes de información de forma periódica a acceso en tiempo real".
TIPO DE AUDITORIA:	Auditoría Especial.

REUNIÓN DE APERTURA				EJECUCIÓN DE LA AUDITORÍA				REUNIÓN DE CIERRE				
Día	Mes	Año		Desde	Hasta			Día	Mes	Año		
				01-06-2022		30-06-2022						
				DD / MM /AA		DD / MM /AA						

2. DETERMINACIÓN DE LA MUESTRA DE AUDITORÍA

Para la verificación del cumplimiento de los requisitos legales expedidos por el Gobierno Nacional a partir de la Emergencia Sanitaria por la pandemia COVID 19, el Grupo de Control Interno solicitó a la Subdirección de Gestión y Manejo de Áreas Protegidas, Grupo de Tecnologías de la Información y las Comunicaciones GTIC, los soportes de avance y cumplimiento del Decreto 417 del 17 de marzo del 2020 y las actualizaciones de la información.

	INFORME FINAL DE AUDITORÍA INTERNA	Código: EL_FO_04
		Versión: 9
		Vigente desde: 15/09/2021

3. METODOLOGÍA

Para la verificación del cumplimiento de los requisitos legales expedidos por el Gobierno Nacional a partir de la Emergencia Sanitaria por la pandemia COVID 19, el Grupo de Control Interno solicitó con memorando No. 20221200008253 del 25 de agosto de 2022 al Grupo de Tecnologías de la Información y las Comunicaciones GTIC las evidencias de avance y cumplimiento “...Por la cual se establecen normas para promover el teletrabajo y se dictan otras disposiciones” y la Directiva Presidencial No. 02 de 2020, mediante la cual se adoptan “Medidas para atender la contingencia por Covid-19, a partir uso de las Tecnologías de la Información y las Telecomunicaciones – TIC...”.

El Grupo de Tecnologías de la Información y las Comunicaciones GTIC dio respuesta al Grupo de Control Interno mediante Orfeo radicado No 20221600006423 del 30 de agosto del 2022.

4. ASPECTOS EVIDENCIADOS DURANTE EL EJERCICIO DE LA AUDITORÍA

En el desarrollo del seguimiento se evidenció la siguiente información:

- Estadísticas de Conexión de Trabajo remoto implementado por la entidad.
- Estadísticas de Protocolos de Comunicación adoptado por PNNC.

4.1 ASPECTOS POSITIVOS: FORTALEZAS

Reporte de la información relacionada con las medidas para atender la contingencia generada por el COVID-19, a partir del uso de las tecnologías de la información y las telecomunicaciones – TIC.

4.2 LIMITACIONES

No se presentaron limitaciones en el alcance y desarrollo de la auditoría interna que no permitieran dar cumplimiento al plan de auditoria establecido por el Grupo de Control Interno.

4.3 DESCRIPCIÓN DE LAS OBSERVACIONES / NO CONFORMIDADES

CRITERIO – MARCO LEGAL	DESCRIPCION DE LA SITUACION:
Directiva Presidencial No. 02 del 12 de marzo de 2020 , medidas para atender la contingencia generada por el COVID-19, a partir del	La Subdirección de Gestión y Manejo en la responsabilidad y competencia del Grupo de Tecnologías de la Información y las Comunicaciones GTIC, ejecutaron las siguientes actividades con corte al 30 de junio del 2022 relacionadas con el componente de Trabajo en Casa por medio del Uso de las TIC como se relaciona a continuación:



INFORME FINAL DE AUDITORÍA INTERNA

Código: EL_FO_04

Versión: 9

Vigente desde: 15/09/2021

uso de las tecnologías de la información y las telecomunicaciones – TIC.

1. Trabajo en Casa por medio del Uso de las TIC.

Como medida preventiva de carácter temporal y extraordinario, y hasta que se “supere la decretada mediante la Resolución 385 12 de marzo 2020 "Por medio de la cual se declara emergencia sanitaria por causa del coronavirus COVID-19 y se adoptan medidas para hacer frente al virus" por el Ministerio de Salud y Protección Social, los organismos y entidades de la rama ejecutiva del orden nacional deberán revisar las condiciones particulares de salud de los servidores públicos, así como funciones y actividades que desarrollan, con el fin de adoptar mecanismos que permitan su cumplimiento en la casa. Por ello, se podrá acudir a las tecnologías la información y las comunicaciones, sin que esto constituya la modalidad de teletrabajo, de conformidad con lo previsto en el numeral 4 artículo 6 de la Ley 1221 de 2008 "Por la cual se establecen normas para promover y el teletrabajo y se dictan otras disposiciones”.

Desde el Grupo de Tecnologías de la Información y las Comunicaciones, se implementó el teletrabajo como herramienta fundamental para el desempeño de las labores de los funcionarios de la entidad, así como también y en aras de garantizar la disponibilidad de servicios críticos como portal web y sistemas de información, se migro a un esquema de nube pública estos servicios para ser accedidos desde cualquier lugar y a través de cualquier medio informático, teniendo en cuenta las directrices de seguridad y privacidad de la información adoptadas por la entidad como se ilustra a continuación:

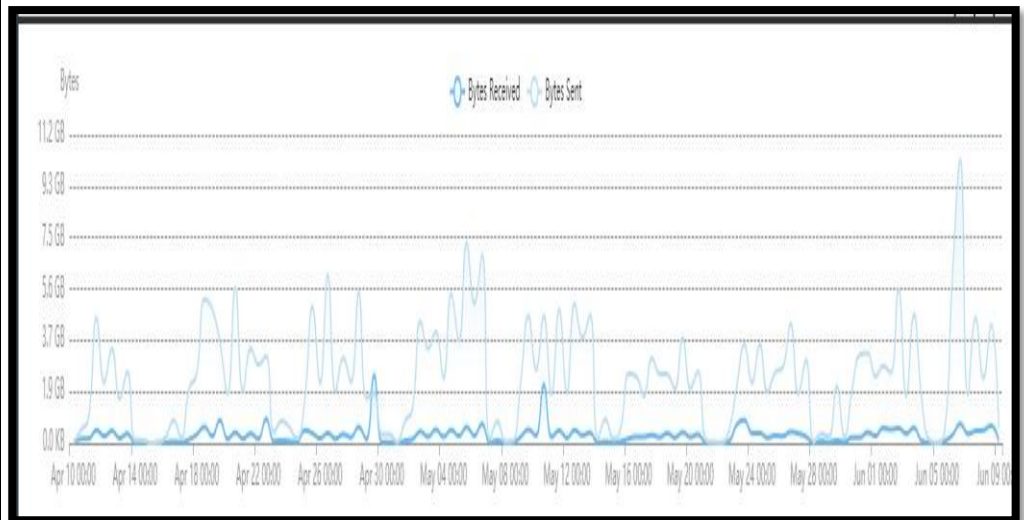


Figura 1: Estadísticas de Conexión Trabajo Remoto


Imagen No: 1: Fuente GTIC.

El alcance anterior está relacionado con el anexo que corresponde al listado del directorio de VPN aportado como evidencia en el avance del cumplimiento de las directrices de seguridad y privacidad de la información adoptada por la entidad como herramienta fundamental para el desempeño de las labores de los funcionarios de PNNC.

De igual forma se reporta que a la fecha se tienen creadas 378 cuentas de VPN, de las cuales actualmente se están usando en promedio el 70% con un tráfico promedio de 50 GB por usuario, lo que demuestra el cumplimiento del marco normativo.

OBSERVACION / NO CONFORMIDAD:

No se presentaron Observaciones y No Conformidades.

	INFORME FINAL DE AUDITORÍA INTERNA	Código: EL_FO_04
		Versión: 9
		Vigente desde: 15/09/2021

CRITERIO – MARCO LEGAL	DESCRIPCION DE LA SITUACION:
<p>Directiva Presidencial No. 02 del 12 de marzo de 2020, medidas para atender la contingencia generada por el COVID-19, a partir del uso de las tecnologías de la información y las telecomunicaciones – TIC.</p> <p>2. Uso de Herramientas Colaborativas.</p> <p>2.1. Minimizar las reuniones presenciales de grupo, y cuando sea necesario realizarlas, propender por reuniones virtuales mediante el uso de las tecnologías de la información y las comunicaciones.</p>	<p>La Subdirección de Gestión y Manejo de Áreas Protegidas SGM en la competencia y responsabilidad del Grupo de Tecnologías de la Información y las Comunicaciones GTIC, ha dispuesto, implementado y ejecutado la plataforma Corporativa Google Meet, para la realización de reuniones virtuales con corte al 30 de junio del 2022, fecha del levantamiento de la Emergencia Sanitaria por COVID 19.</p> <p>De igual forma, se permite el uso de otras plataformas como las que se relacionan a continuación:</p> <ul style="list-style-type: none"> ➤ Cisco Webex. ➤ Microsoft Teams. ➤ Skype. ➤ Zoom. ➤ Discord. <p>Con el contexto anterior se refleja que a través del Grupo de Tecnologías de la Información y las Comunicaciones GTIC, se provee los permisos necesarios a través de la plataforma de seguridad perimetral para el acceso a conversatorios, foros, congresos o cualquier tipo de evento masivo que requiera de estas herramientas.</p>
<p>OBSERVACION / NO CONFORMIDAD:</p> <p>No se presentaron Observaciones y No Conformidades.</p>	

CRITERIO – MARCO LEGAL	DESCRIPCION DE LA SITUACION:
<p>Directiva Presidencial No. 02 del 12 de marzo de 2020, medidas para atender la contingencia generada por el COVID-19, a partir del uso de las tecnologías de la información y las telecomunicaciones – TIC.</p> <p>2. Uso de Herramientas Colaborativas.</p> <p>2.2. Acudir a canales virtuales institucionales,</p>	<p>En cuanto al cumplimiento de acudir a canales virtuales institucionales, transmisiones en vivo y redes sociales, para realizar conversatorios, foros, congresos o cualquier tipo de evento masivo con corte al 30 de junio del 2022.</p> <p>La Subdirección de Gestión y Manejo de Áreas Protegidas, en la competencia y responsabilidad del Grupo de Tecnologías de la Información y las Comunicaciones GTIC; provee los permisos necesarios a través de la plataforma de seguridad perimetral para el acceso a conversatorios, foros, congresos o cualquier tipo de evento masivo como se ilustra en la imagen:</p>



INFORME FINAL DE AUDITORÍA INTERNA

Código: EL_FO_04

Versión: 9

Vigente desde: 15/09/2021

transmisiones en vivo y redes sociales, para realizar conversatorios, foros, congresos o cualquier tipo de evento masivo.

Protocol	Hits	Bytes Sent(MB)	Bytes Received	Total Bytes(MB)
1 realaudio ✓	2149	53.12	140.48	193.6
2 RTSP	2207	0.12	0.02	0.13
3 chat ✓	367	0.02	0	0.03
4 h323 ✓	216	0.01	0	0.01
5 irc	73	0	0	0
6 lrcs	40	0	0	0
7 yak-chat	37	0	0	0
8 videotex ✓	38	0	0	0
9 conference ✓	38	0	0	0
10 slam	34	0	0	0
11 smpte	37	0	0	0
12 Quicktime ✓	35	0	0	0
13 rtmp	36	0	0	0
14 ideafarm-chat	35	0	0	0
15 bell	33	0	0	0
16 ipserver	31	0	0	0
17 digital-vrc	30	0	0	0
18 phillips-vc	12	0	0	0

Figura 2: Estadísticas Protocolos de Comunicación

Imagen No: 2: Fuente GTIC.

El contexto anterior evidencia la aplicación, ejecución e implementación de las herramientas y mecanismos que permiten dar cumplimiento al marco normativo de la Directiva Presidencial y facilita la conectividad para el desarrollo de reuniones y espacios virtuales al interior de la entidad como alternativas en el marco de la emergencia sanitaria.

OBSERVACION / NO CONFORMIDAD:

No se presentaron Observaciones y No Conformidades.

CRITERIO – MARCO LEGAL	DESCRIPCION DE LA SITUACION:
<p>Directiva Presidencial No. 02 del 12 de marzo de 2020, medidas para atender la contingencia generada por el COVID-19, a partir del uso de las tecnologías de la información y las telecomunicaciones – TIC.</p> <p>2. Uso de Herramientas Colaborativas.</p> <p>2.3. Usar las herramientas tecnológicas para comunicarse, el acuerdo marco de precios de nube pública vigente, trabajo</p>	<p>La Subdirección de Gestión y Manejo de Áreas Protegidas y en la competencia y responsabilidad del Grupo de Tecnologías de la Información y las Comunicaciones GTIC, hace uso e implementa los canales adoptados por la entidad para trabajo colaborativo, videoconferencia, con el fin de evitar la impresión y manipulación de papel como se ilustra en la imagen:</p>



INFORME FINAL DE AUDITORÍA INTERNA

Código: EL_FO_04

Versión: 9

Vigente desde: 15/09/2021

colaborativo y telepresencial - videoconferencia-, para evitar el uso, impresión y manipulación de papel.

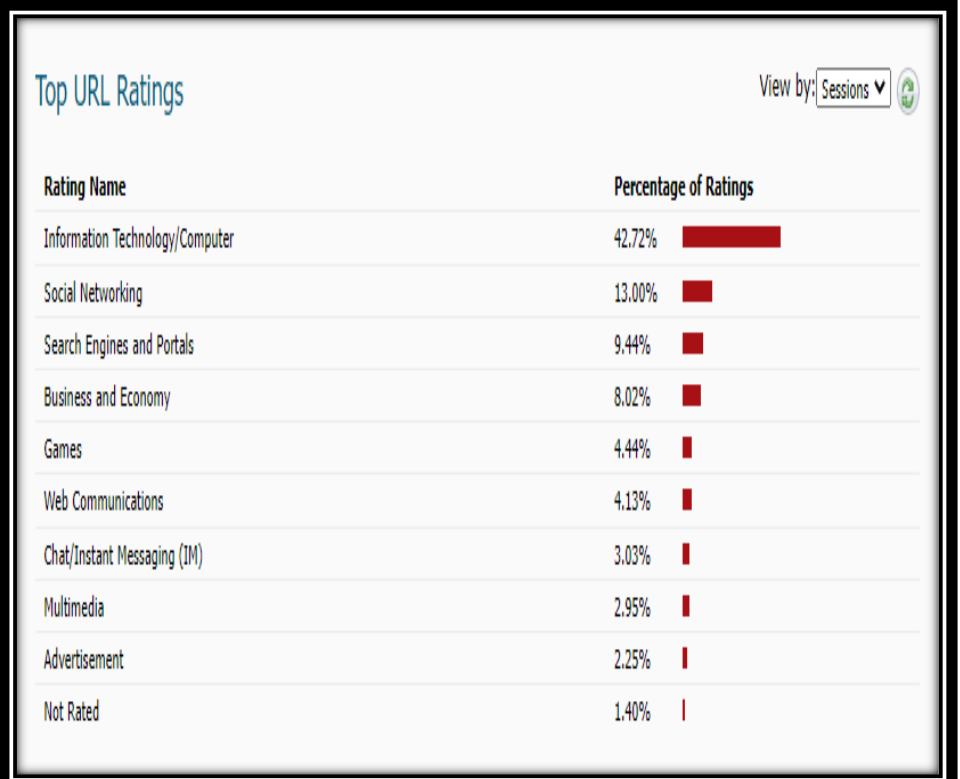



Figura 3: Estadísticas Trafico general Internet por Categoría Aplicaciones
Imagen No: 3: Fuente GTIC.

Con el alcance anterior se evidencia el anexo relacionado con los permisos implementados y adoptados por la entidad con corte al 30 de junio del 2022 para las conexiones necesarias que permitan asegurar el acceso a todos los eventos programados, ejecutados y desarrollados en la plataforma de seguridad perimetral como alternativas para minimizar los impactos en lo que compete a impresiones y manipulación de papel en el marco de la emergencia sanitaria en PNNC.

OBSERVACION / NO CONFORMIDAD:

No se presentaron Observaciones y No Conformidades.

	INFORME FINAL DE AUDITORÍA INTERNA	Código: EL_FO_04
		Versión: 9
		Vigente desde: 15/09/2021

CRITERIO – MARCO LEGAL	DESCRIPCION DE LA SITUACION:
<p>Directiva Presidencial No. 02 del 12 de marzo de 2020, medidas para atender la contingencia generada por el COVID-19, a partir del uso de las tecnologías de la información y las telecomunicaciones – TIC.</p> <p>2. Uso de Herramientas Colaborativas.</p> <p>2.4. Adoptar las acciones que sean necesarias para que los trámites que realicen los ciudadanos se adelanten dándole prioridad a los medios digitales.</p>	<p>Dentro de los mecanismos, acciones y herramientas de gestión aplicadas por el Grupo de Tecnologías de la Información y las Comunicaciones GTIC, se identifican todos los sistemas de información como aplicaciones y plataformas críticas para la operación de la entidad, así como las siguientes:</p> <ul style="list-style-type: none"> ➤ Gestor Documental (Orfeo). ➤ Portal Web. ➤ Geo Visor. ➤ Plataforma DashBoard. ➤ Guardaparques. ➤ Runap. ➤ Visor 360. ➤ Acuerdos. ➤ Plataformas Colaborativas (Correo Electrónico, Suite de Google). <p>Aplicaciones que fueron implementadas y migradas a la nube, con el fin de garantizar su operatividad y disponibilidad en todo momento y desde cualquier medio tecnológico en la entidad para las labores y actividades adelantadas en el marco de la emergencia sanitaria por PNNC con corte al 30 de junio del 2022.</p>
<p>OBSERVACION / NO CONFORMIDAD:</p> <p>No se presentaron Observaciones y No Conformidades.</p>	

CRITERIO – MARCO LEGAL	DESCRIPCION DE LA SITUACION:
<p>Directiva Presidencial No. 02 del 12 de marzo de 2020, medidas para atender la contingencia generada por el COVID-19, a partir del uso de las tecnologías de la información y las telecomunicaciones – TIC.</p> <p>2. Uso de Herramientas Colaborativas.</p>	<p>Desde la Subdirección de Gestión y Manejo de Áreas Protegidas en la responsabilidad del Grupo de Tecnologías de la Información y las Comunicaciones GTIC, se proveen las herramientas necesarias para actividades de e-learning habilitando los canales de comunicaciones de manera bidireccional y sin restricciones como se ilustra en la imagen:</p>



INFORME FINAL DE AUDITORÍA INTERNA

Código: EL_FO_04

Versión: 9

Vigente desde: 15/09/2021

2.5. Hacer uso de herramientas como e-learning, portales de conocimiento, redes sociales y plataformas colaborativas, para adelantar los procesos de capacitación y formación que sean inaplazables.

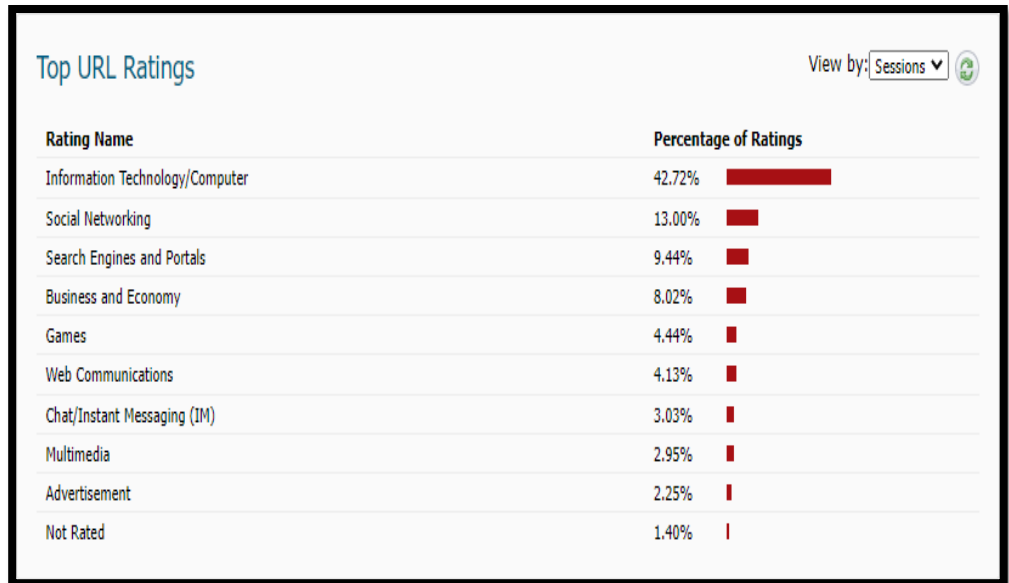


Figura 4: Estadísticas Trafico general Internet por Categoría Aplicaciones

Imagen No: 4: Fuente GTIC.

El contexto anterior evidencia el anexo con el desarrollo y ejecución de las actividades de e-learning habilitando los canales de comunicaciones de manera bidireccional y sin restricciones en la entidad como alternativas en el marco de la emergencia sanitaria dando cumplimiento al marco normativo

El uso de las tecnologías de la información y telecomunicaciones deberá garantizar el cumplimiento de los lineamientos establecidos en materia de ciberseguridad por la entidad y con sujeción a la legislación vigente en materia de habeas data.

OBSERVACION / NO CONFORMIDAD:

No se reportaron Observaciones y No Conformidades.

CRITERIO – MARCO LEGAL	DESCRIPCION DE LA SITUACION:
Directiva Presidencial No. 02 del 12 de marzo de 2020, medidas para atender la contingencia generada por el COVID-19, a partir	A través del Grupo de Tecnologías de la Información y las Comunicaciones GTIC y la adopción del modelo de seguridad y privacidad de la información a través del SGSI, se garantiza el cumplimiento de lineamientos establecidos en materia de ciberseguridad como se ilustra en la imagen:



INFORME FINAL DE AUDITORÍA INTERNA

Código: EL_FO_04

Versión: 9

Vigente desde: 15/09/2021

del uso de las tecnologías de la información y las telecomunicaciones – TIC.

“...El uso de las tecnologías de la información y telecomunicaciones deberá garantizar el cumplimiento de los lineamientos establecidos en materia de ciberseguridad por la entidad y con sujeción a la legislación vigente en materia de habeas data...”

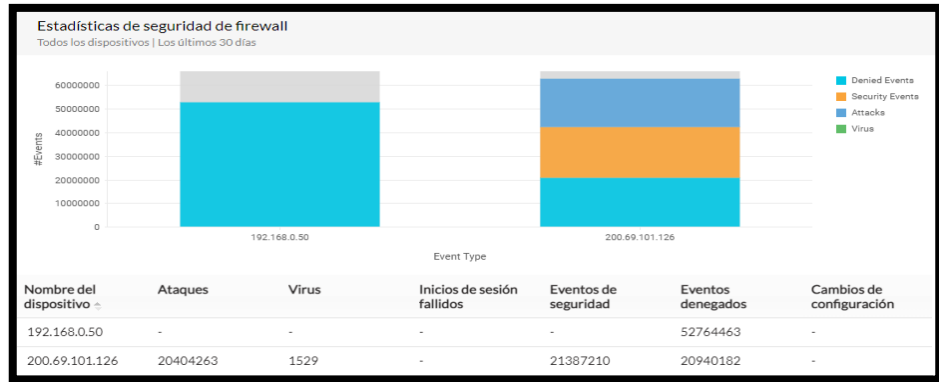


Figura 5: Estadísticas Ciberseguridad

Imagen No: 5: Fuente GTIC.

#	Botnet Name	Sessions
1	Botnet Detected	10
2	Botnet Blocked	10

Figura 6: Estadísticas Botnets

Imagen No: 6: Fuente GTIC.

#	Intrusion Name	Sessions	
1	NetBIOS Name Request Probe	32.01K	92%
2	Echo Reply	21.15K	34%
3	Time-To-Live Exceeded in Transit	4.57K	7%
4	Oversize ICMP Packet	1.19K	1%
5	PING	666	1%
6	SSLv2.0 Client Hello 2	566	<1%
7	Destination Unreachable (Network Unr...	113	<1%
8	HTTP Request with Irregular Request ...	85	<1%
9	HTTP Request URI with SQL Statement ...	74	<1%
10	HTTP Request with Irregular Request ...	73	<1%
11	SSL/TLS Channel Carrying Plain Text ...	49	<1%
12	example.com DNS Query	18	<1%
13	SSLv2.0 Client Hello	16	<1%
14	HTTP Request with Malformed Host Hea...	13	<1%
15	OpenSSL Heartbeat 1	6	<1%
16	SSL/TLS Channel Carrying Plain Text ...	5	<1%
17	Downgraded TLS Traffic	5	<1%
18	Obfuscated VBScript/Javascript Code 27	4	<1%
19	Web Application Default Account Logi...	4	<1%
20	Web Application XXE Injection 2	3	<1%
21	Web Application Remote Code Executio...	2	<1%
22	Web Application Remote Code Executio...	2	<1%
23	Web Application Directory Traversal 48	2	<1%
24	Web Application XXE Injection 2 - c2	2	<1%
Total: 29 Item(s)		60.63K	

Figura 7: Ataques Contenidos

Imagen No: 7: Fuente GTIC.

	INFORME FINAL DE AUDITORÍA INTERNA	Código: EI_FO_04
		Versión: 9
		Vigente desde: 15/09/2021

	El alcance anterior evidencia las acciones y actividades de conectividad desarrolladas con corte al 30 de junio del 2022 por la entidad y verificadas y monitoreadas por el GTIC en cumplimiento de los lineamientos establecidos en materia de Habeas Data.
--	--

OBSERVACION / NO CONFORMIDAD:	
No se reportan Observaciones y No Conformidades.	

CRITERIO – MARCO LEGAL	DESCRIPCION DE LA SITUACION:
<p>Artículo 59 del Decreto Ley 403 de 2020 “acceso y análisis a la información” y la Circular 009 de 2020 de la contraloría general de la república “plan de transición de acceso a fuentes de información de forma periódica a acceso en tiempo real.</p> <p>Se requiere informar los documentos remitidos, las actividades realizadas para dar cumplimiento a la Circular 09 y los acuerdos a que se llegó en mesas de trabajo con la Contraloría General de la República, para la transmisión de dichos datos.</p> <p>“...Cumplimiento de la disposición normativa: artículo 59 del Decreto Ley 403 del 16 de marzo de 2020...”</p>	<p>En el marco de la suscripción del Acuerdo de Confidencialidad firmado por la Contraloría General de la República y Parques Nacionales Naturales de Colombia PNNC realizada el 22 de septiembre del 2021 con corte al 30 de junio del 2022, la Subdirección de Gestión y Manejo de Áreas Protegidas, Grupo de Tecnologías de la Información y las Comunicaciones GTIC; manifiesta que no se han realizado solicitudes de información en el marco de la Circular 09, de igual forma se tiene conocimiento del alcance del acto administrativo y se mantiene la disponibilidad para atender los requerimientos en los acuerdos establecidos y la transmisión de datos que se requieran por el ente de control.</p>

OBSERVACION / NO CONFORMIDAD:	
No se reportan Observaciones y No Conformidades.	

5. RECOMENDACIONES

- El Grupo de Tecnologías de la Información y las Comunicaciones GTIC como responsable de la aplicación del Plan Estratégico de Tecnologías de la Información PETIC, se recomienda seguir asegurando que las herramientas Tecnológicas adoptadas y establecidas por la entidad, las cuales deben estar disponibles para certificar el cumplimiento del trabajo remoto y reportar los soportes y evidencias que demuestren su desarrollo e implementación a las entidades que lo requieran con corte al 30 de junio del 2022, fecha en la cual se levanta la Emergencia Sanitaria por COVID 19..
- Asegurar que los lineamientos, mecanismos y controles establecidos por la entidad, permitan asegurar, la eficacia de las actividades realizadas y ejecutadas en el marco de los lineamientos establecidos en lo que

	INFORME FINAL DE AUDITORÍA INTERNA	Código: EL_FO_04
		Versión: 9
		Vigente desde: 15/09/2021

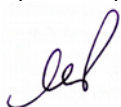
corresponde a las Medidas para atender la contingencia generada por el COVID-19, a partir del uso e implementación de las tecnologías de la información y las telecomunicaciones – TIC con corte al 30 de junio del 2022 de las actividades que hacen parte de la gestión y que son susceptibles de verificación por cualquier ente de control externo que demuestren cumplimiento.

- Dar cumplimiento por parte de la entidad a los reportes establecidos en el marco del acuerdo de confidencialidad firmado con la Contraloría General de la Republica CGR sobre la Información Transferida en Cumplimiento de la Constitución y la Ley, Celebrado entre Parques Nacionales Naturales de Colombia – PNNC y la CGR, con el fin de adelantar el reporte, validación y transmisión de datos solicitados por el ente de control.

6. CONCLUSIONES

- Se debe continuar con la implementación por parte del Grupo de Tecnologías de la Información y las Comunicaciones GTIC de las acciones y actividades que demuestren el cumplimiento de las medidas que atendieron la contingencia generada por el COVID-19 con corte al 30 de junio del 2022 en lo que corresponde al uso de las tecnologías de la información y las telecomunicaciones – TIC.

Aprobado por:



GLADYS ESPITIA PEÑA
 Coordinador(a) Grupo de Control Interno
 Elaborado por: Raymon Sales Contreras- Funcionario
 Revisado por: Gladys Espitia Peña.