Para contestar cite:
Radicado ANI No.: **20201020069633**
Fecha: **29-05-2020**

MEMORANDO

Bogotá D.C.

PARA: **Dr. MANUEL FELIPE GUTIÉRREZ TORRES**
Presidente Agencia Nacional de Infraestructura

Dr. DIEGO ALEJANDRO MORALES SILVA
Vicepresidente de Planeación Riesgos y Entorno

DE: **GLORIA MARGOTH CABRERA RUBIO**
Jefe Oficina de Control Interno

ASUNTO: Informe de evaluación integral a los componentes de hardware, software y seguridad de la información marco sobre el cual se evaluó el cumplimiento de la Entidad en materia de ciberseguridad y trabajo en casa por la emergencia sanitaria por causa del covid-19.

Respetados Doctores:

La Oficina de Control Interno, en el mes de mayo de 2020, realizó la evaluación integral a los componentes de hardware, software y seguridad de la información marco sobre el cual se evaluó el cumplimiento de la Entidad en materia de ciberseguridad y trabajo en casa por la emergencia sanitaria por causa del covid-19.

Las conclusiones, fortalezas y recomendaciones se describen en el capítulo 10 del informe que se anexa a la presente comunicación, con el fin que se coordinen las acciones tendientes a la atención de las recomendaciones realizadas.

Atentamente,

GLORIA MARGOTH CABRERA RUBIO

Para contestar cite:
Radicado ANI No.: **20201020069633**
Fecha: **29-05-2020**

MEMORANDO

Jefe Oficina de Control Interno

Anexos: 1 Informe en PDF

cc: 1) DIEGO ALEJANDRO MORALES SILVA (VICE) Vicepresidencia de Planeacion Riesgos y Entorno BOGOTA D.C.

Proyectó: Juan Diego Toro – Contratista OCI
VoBo: GLORIA MARGOTH CABRERA RUBIO (JEFE)
Nro Rad Padre:
Nro Borrador: 20201020024356
GADF-F-010

INFORME DE AUDITORÍA



EVALUACIÓN INTEGRAL A LOS COMPONENTES DE HARDWARE, SOFTWARE Y SEGURIDAD DE LA INFORMACIÓN

MARCO SOBRE EL CUAL SE EVALUARÁ EL CUMPLIMIENTO DE LA ENTIDAD EN MATERIA DE CIBERSEGURIDAD Y TRABAJO EN CASA POR LA EMERGENCIA SANITARIA POR CAUSA DEL COVID-19

2020

TABLA DE CONTENIDO

1. OBJETIVO 4

2. ALCANCE 4

3. METODOLOGÍA. 4

4. MARCO LEGAL Y PROCEDIMENTAL 7

5. VERIFICACIÓN DE ANTECEDENTES. 8

6. MARCO DE REFERENCIA. 8

7. TÉRMINOS Y DEFINICIONES. 11

8. DESARROLLO DEL INFORME. 13

8.1. Continuidad en la prestación de los servicios de la Entidad por causa del aislamiento preventivo obligatorio y la implementación del trabajo en casa. 13

8.2. Seguridad de la información y tratamiento de los riesgos de ciberseguridad por causa del aislamiento preventivo obligatorio y la implementación del trabajo en casa. 19

8.2.1. Seguridad de las redes (Cifrados, autenticación, contraseñas) y Protección de la información (Disponibilidad, integridad, completitud y confiabilidad) 20

8.2.2. Accesos o Conexiones Remotas (VPN u otras) 24

8.2.3. Respaldo de la información (Backups y recuperaciones) 30

8.2.4. Trabajo en casa y reuniones virtuales (Aplicaciones, Intranet, plataformas de reuniones y herramientas colaborativas). 33

8.2.5. Identificación de nuevos riesgos 34

8.2.6. Capacitación y buenas prácticas en materia de Ciberseguridad y trabajo en casa 42

8.3. Comportamiento general de la infraestructura de TI por causa del aislamiento preventivo obligatorio y la implementación del trabajo en casa. 45

8.3.1. Tratamiento de fallas o incidentes de seguridad. 45

8.3.2. Suficiencia del recurso humano y del hardware 55

8.3.3. Verificación de la cobertura de antivirus y firewall 58

8.3.4. Identificación de necesidades a partir del confinamiento y el trabajo remoto 60

9. CALIFICACIÓN DE LA AUDITORÍA Y CONCEPTO DEL AUDITOR 61

10. FORTALEZAS Y RECOMENDACIONES 61

10.1. Fortalezas 61

10.2. Recomendaciones 62

1. OBJETIVO

Evaluar la ciberseguridad de la infraestructura de tecnología de la Agencia Nacional de Infraestructura. Para el cumplimiento de este objetivo se adelantarán las siguientes actividades:

- Verificar la continuidad de la Entidad ante eventos externos.
- Validar los niveles de cumplimiento en materia de aseguramiento de la información (Disponibilidad, integridad, seguridad y completitud).
- Evaluar los riesgos nuevos de TI generados por la implementación de trabajo en casa o trabajo remoto.
- Evaluar el comportamiento de la infraestructura de TI actual y determinar sus necesidades.

2. ALCANCE

Evaluar la ciberseguridad de la infraestructura de tecnología de la Agencia Nacional de Infraestructura dispuesta para el trabajo en casa o trabajo remoto, ocasionado por el aislamiento preventivo obligatorio a causa de la pandemia del Covid 19, desde marzo hasta abril de 2020, mediante la aplicación de listas de chequeo y aplicación de pruebas de PenTest e Ingeniería Social.

3. METODOLOGÍA.

La metodología empleada por la Oficina de Control Interno fue la usualmente aceptada para la elaboración de este tipo de informes de acuerdo con las normas de auditoría, para lo cual se hizo necesario efectuar una planeación y ejecución de trabajo, donde se tuvieron en cuenta los siguientes aspectos:

- ***Remisión del plan de auditoría:*** El día 4 de mayo de 2020, mediante correo electrónico se remitió el plan de auditoría (Formato EVCI-F-037), que describe las actividades, fechas e involucrados en el ejercicio auditor.

1. ***Solicitud de información:*** El día 4 de mayo de 2020, mediante correo electrónico se solicitó información al Coordinador del Grupo Interno de Trabajo Tecnologías de la Información y las Telecomunicaciones, relacionada y agrupada bajo los siguientes ítems: i) Plan de Continuidad del Negocio (BCP), ii) Relación de conexiones remotas actuales especificando la fecha de solicitud, el modo habilitado (VPN u otro), la fecha de habilitación, software al que se accede y el nombre del usuario, iii) Soporte del monitoreo de estos accesos remotos frente a su funcionamiento y seguridad, iv) Documento con la identificación de riesgos de TI ocasionados por el Teletrabajo y su tratamiento, v) Relación de equipos que se encuentran fuera de la Entidad especificando el usuario, vi) Copia o soporte de capacitación o instructivos para teletrabajo dada a los colaboradores de la Entidad, vii) Copia o soporte de buenas prácticas en materia de seguridad de la información para teletrabajo a los colaboradores de la Entidad, viii) Reporte de monitoreo de la seguridad de la infraestructura de TI de la Entidad y reporte de fallas o incidentes de seguridad y su tratamiento, ix) Relación del personal dedicado a soporte remoto detallando porcentaje de dedicación, temática principal atendida y número de casos atendidos en marzo y abril de 2020, x) Si han identificado necesidades (personal, hardware, software seguridad u otros) a partir de la masificación del teletrabajo, remita la relación y justificación, xi) Si ha efectuado pruebas de vulnerabilidad de la infraestructura de TI recientemente, remita los resultados, xii) Si ha efectuado pruebas de restauración de copias de respaldo recientemente, remita los resultados y xiii) Si ha generado documentos adicionales relacionados con Ciberseguridad y Teletrabajo remitir copia.

   Esta información fue recibida oportuna y completamente vía correo electrónico.

- ***Apertura de la auditoría:*** El día 6 de mayo de 2020, mediante acta (Formato EVCI-F-001) se dio apertura al ejercicio auditor, informando el objetivo, alcance, criterios y las fechas de las actividades principales.

- ***Desarrollo de la auditoría****:* El 7 de mayo de 2020, mediante la aplicación de lista de chequeo, se efectuó entrevista al líder del Grupo Interno de Trabajo Tecnologías de la Información y las Telecomunicaciones, con la participación de los funcionarios de apoyo atendiendo cada uno de los criterios y documentando las evidencias. La lista de chequeo diligenciada fue remitida vía correo electrónico el día 15 de mayo de 2020 cumpliendo con los plazos establecidos. Los soportes y resultados de la lista de chequeo pueden ser consultados en https://anionline.sharepoint.com/Gestion%20VPRE/Sistemas/GD_TI/AuditoriasCI/SitePages/Home.aspx

- ***Realización de las pruebas aleatorias de PenTest e Ingeniería Social:*** Los días 13, 14 y 15 de mayo de 2020, se adelantaron pruebas de penetración de caja blanca a diferentes medios y aplicativos de la ANI.

- ***Socialización de resultados:*** El día 26 de mayo de 2020, se remitió vía correo electrónico, el informe preliminar, para lo cual y con sustento en lo dispuesto en el literal (g) del artículo cuarto de la Resolución 1478 de 2019, por la cual se establece el estatuto de auditoría y código de ética del auditor en la Agencia Nacional de Infraestructura y se dictan otras disposiciones (disponible en https://www.ani.gov.co/sites/default/files/res_1478_2019.pdf), que señala:

  > *"Comunicar las conclusiones del proceso de auditoría a los responsables, quienes tendrán la oportunidad de exponer su posición de manera soportada, dentro de los tres (3) días siguientes a la socialización de dichas conclusiones, luego de lo cual se harán las revisiones pertinentes y ajustes en caso de que procedan y se formalizará el informe de auditoría. De no existir comentarios sobre las conclusiones en el término señalado, se entenderá que no hay lugar a precisiones y se emitirá el informe definitivo".*

  Una vez expirado el plazo y sin obtener comentarios se procede a la radicación del informe.

Los resultados de estas actividades se presentan en este informe de auditoría, en el que se incluyen las recomendaciones y las oportunidades de mejora identificadas para alcanzar los niveles más altos de ciberseguridad y mitigar los riesgos a los que se ve expuesta la entidad por la implementación del trabajo en casa o trabajo remoto.

Los parámetros de calificación, definidos para determinar el porcentaje de cumplimiento, son los mismos aplicados en las auditorías anteriores:

CUMPLIMIENTO		
NO CUMPLE	**CUMPLE PARCIALMENTE**	**CUMPLE**

4. MARCO LEGAL Y PROCEDIMENTAL

A continuación, se describe el marco legal e institucional:

- Constitución Política de Colombia Artículo 209.
- Ley 87 de 1993, *"Por la cual se establecen normas para el ejercicio de control interno en la entidades y organismos del estado y se dictan otras disposiciones".*
- Ley 1273 de 2009, "*por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones"*
- Ley 1581 de 2012, "*Por la cual se dictan disposiciones generales para la protección de datos personales".*
- Decreto 1377 de 2013, "*Por la cual se reglamenta parcialmente la Ley 1581 de 2012*".
- Decreto 1078 de 2015 Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 648 de 2017 *Por el cual se modifica y adiciona el Decreto 1083 de 2015, Reglamentario Único del Sector de la Función Pública.*
- Decreto 1008 de 2018 *Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.*
- Decreto 620 de 2020 *"Por el cual se subroga el título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 Y 64 de la Ley 1437 de 2011, los literales e, j y literal a del parágrafo 2 del artículo 45 de la Ley 1753 de 2015, el numeral 3 del artículo 147 de la Ley 1955 de 2019, y el artículo 9 del Decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales".*
- Decreto 491 de 2020 *"Por el cual se adoptan medidas de urgencia para garantizar la atención y la prestación de los servicios por parte de las autoridades públicas y los particulares que cumplan funciones públicas y se toman medidas para la protección laboral y de los contratistas de prestación de servicios de las entidades públicas, en el marco del Estado de Emergencia Económica, Social y Ecológica".*
- Decreto 464 de 2020, *"Por el cual se disponen medidas con el fin de atender la situación de emergencia económica, social y ecológica de la que trata el Decreto 417 de 2020"*

- Directiva Presidencial 02 de 2020 "*Medidas para atender la contingencia por covid-19, a partir uso de las tecnologías la información y las telecomunicaciones*".
- Resolución 385 de 2020 "*Por la cual se declara la emergencia sanitaria por causa del corona virus COVID2019 y se adoptan medidas para hacer frente al virus"*
- Circular No. 7 de 2020 Agencia Nacional de Infraestructura *"Medidas de contención COVID-19".*
- Memorando No. 2020-409-000008-4 del 12 de marzo de 2020 de la Agencia Nacional de Infraestructura *"Nuevas medidas de Contención COVID-19"*

5. VERIFICACIÓN DE ANTECEDENTES.

En lo pertinente al Plan de Mejoramiento Institucional se precisa que no se evidenciaron hallazgos de la Contraloría General de la República relacionados con ciberseguridad ni con las disposiciones de trabajo en casa o remoto.

En la revisión del plan de mejoramiento por procesos devenido de las auditorías internas, tampoco se advierten no conformidades relacionadas con esta temática.

6. MARCO DE REFERENCIA.

Como mecanismo de contingencia en relación con los posibles impactos en la salud de las personas que pueda generar el COVID-19 declarado el 11 de marzo de 2020 por la Organización Mundial de la Salud – OMS – como una pandemia, y con el propósito de garantizar la prestación del servicio público, la Directiva Presidencial No. 02 del 12 de marzo de 2020, impartió las directrices de trabajo en casa por medio del uso de las TIC y el uso de herramientas colaborativas.

A raíz de la declaratoria de la emergencia sanitaria y la adopción de medidas para hacerle frente por causa del coronavirus COVID-19, decretada mediante la Resolución 385 del 12 de marzo de 2020 del Ministerio de Salud y Protección Social, la Directiva Presidencial No. 02 imparte como medida preventiva de carácter temporal y extraordinario y hasta que se supere la emergencia sanitaria, que los organismos y entidades de la rama ejecutiva del orden nacional deberán revisar las condiciones particulares de salud de los servidores públicos, así como las funciones y actividades que desarrollan, con el fin de adoptar mecanismos que permiten su cumplimiento desde la casa.

La Directiva Presidencial No. 02 determina que para lo anterior, se podrá acudir a las tecnologías de la información y las comunicaciones, sin que esto constituya la modalidad de teletrabajo, de conformidad con lo previsto en el numeral 4 del artículo 6 de la Ley 1221 de 2008, Ley por la cual se establecen normas para promover y regular el teletrabajo y se dictan otras disposiciones.

La OIT recomienda que se deben adoptar medidas para proteger el trabajo en el sector público, implementando mecanismos que promueven e intensifiquen el trabajo en casa, así como, adoptar medidas para que por razones de la emergencia no se terminen o suspendan las relaciones laborales o contractuales en el sector público.

Como medida preventiva de carácter temporal y extraordinario y hasta que se supere la emergencia sanitaria, el mencionado acto administrativo, determina la modalidad de trabajo en casa o trabajo remoto por medio del uso de las TIC (diferente a teletrabajo) e intensifica el uso de las herramientas colaborativas para minimizar las reuniones presenciales de grupo reemplazando por reuniones virtuales, acudir a canales virtuales institucionales, transmisiones en vivo y redes sociales para realizar conversatorios, foros, congresos o cualquier tipo de evento masivo, entre otras.

En esta instancia resulta importante responder a la siguiente pregunta:

¿Cuál es la diferencia entre teletrabajo y trabajo virtual en casa (Trabajo en casa o trabajo remoto)?

El teletrabajo de acuerdo con la Ley 1221 de 2008 es “una forma de organización laboral, que consiste en el desempeño de actividades remuneradas o prestación de servicios a terceros utilizando como soporte las tecnologías de la información y comunicación -TIC - para el contacto entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio específico de trabajo”.

Mientras que, el trabajo virtual en casa o trabajo en casa o trabajo remoto es un mecanismo excepcional mediante el cual los servidores públicos podrán realizar sus actividades desde un lugar diferente al de su trabajo habitual, de manera remota y colaborativa haciendo uso de las Tecnologías de la Información y las Comunicaciones existentes, sin que dicha situación constituya la adopción del teletrabajo en las condiciones establecidas en la Ley 1221 de 2008, de acuerdo con lo señalado en su numeral 4 del artículo 6.

Si bien la modalidad de trabajo en casa no es nueva, a raíz de la pandemia, la migración de millones de usuarios desde redes empresariales o estatales seguras que se protegen y se monitorean de cerca

a redes wi-fi domesticas en gran parte no supervisadas y a menudo inseguras, crea una oportunidad inmensa para los cibercriminales.

Aunque la Entidad está protegida en su entorno común, la implantación del trabajo en casa puede provocar nuevas situaciones y cambios, que dan lugar a abrir brechas y vulnerabilidades que los atacantes aprovechan. La Directiva Presidencial finaliza con el llamado a que "*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*".

Los ciberdelincuentes ya están aprovechando la situación actual para lanzar ataques enfocados en el trabajo en casa. Para ello utilizan métodos muy variados, desde acceso a sistemas con contraseñas poco seguras o robadas por otros medios (Ingeniería Social), a capturar el tráfico que pasa por redes Wi-Fi poco seguras. Además, la actual preocupación por el Coronavirus está generando muchas campañas de phishing con el que logran que los usuarios bajen la guarda atraídos por la curiosidad.

Frente a este panorama y en el marco del sistema de control interno que por mandato constitucional (art. 209 y 269) deben tener todas las entidades públicas en todos los niveles y desarrollado en el Modelo Estándar de Control Interno - MECI, los representantes legales, servidores públicos y las oficinas de control interno, dentro de sus roles y responsabilidades (las cuatro líneas de control) deberán verificar el cumplimiento de la atención y prestación de servicios, así:

▪ Los Representantes Legales y la Alta Dirección, como línea de control interno estratégica y responsable de Sistema de Control Interno, deberán definir cuáles de sus productos o servicios podrán ser prestados de manera virtual y aquellos que podrán suspenderse sin afectar los derechos fundamentales de los ciudadanos e informar y difundir por los diferentes medios con que cuenta la entidad estas decisiones. Así mismo deberá crear las condiciones adecuadas para el desarrollo del trabajo en casa. Como consecuencia de estas decisiones deberán efectuar las modificaciones a que haya lugar en la planeación institucional para asegurar la ejecución, seguimiento y control en cada área.

▪ Los Gerentes públicos, líderes de procesos o gerentes operativos de proyectos y programas de la entidad, (Primera línea de defensa) deberán definir los productos y posibles indicadores con su correspondiente periodicidad (definida de acuerdo con las características y complejidad de los servicios que se van a ofrecer, las actividades a desarrollar y las condiciones de cada entidad), los

cuales permitirán el cumplimiento a los objetivos institucionales y a las modificaciones efectuadas en la planeación y darán aplicación e Identificarán y darán tratamiento a los riesgos que se puedan derivar al cumplimiento de los compromisos y actividades establecidas y hacer los ajustes que considere convenientes.

▪ Jefes de Planeación o quienes hagan sus veces, coordinadores de equipos de trabajo, supervisores, e interventores de contratos, como Segunda Línea de Defensa , deberán coordinar con los diferentes líderes el cumplimiento a las modificaciones a la planeación y hacer seguimiento a los indicadores propuestos para cada área o proceso con el fin de tener información consolidada permanente y estratégica de la gestión y hacer seguimiento a los riesgos e identificar las alertas tempranas sobre eventos que se llegasen a presentar o que puedan estarse presentando para que se tomen las acciones necesarias.

Finalmente, corresponde a la Oficina de Control Interno como Tercera Línea de Defensa, incluir auditorias y seguimientos a los resultados de las actividades de teletrabajo y trabajo en casa y al tratamiento implementado para mitigar los riesgos de ciberseguridad, con ocasión de la emergencia.

Y es precisamente por lo anterior que surge el principal interrogante, ¿Se encuentra la Entidad preparada para operar bajo la modalidad de trabajo en casa o trabajo remoto?, pregunta que va acompañada de ¿La infraestructura de TI (hardware, software y seguridad de la información) con que cuenta la Entidad es suficiente y blinda la información ante ciber-ataques?, ¿Se encuentran alineados los procesos y los responsables para asegurar la continuidad de la prestación del servicio de la Agencia?, estos y otros interrogantes son los que se pretende contestar en la presente auditoría.

7. TÉRMINOS Y DEFINICIONES.

En el desarrollo del presente informe se usarán términos técnicos, razón por la cual es necesario introducir este acápite la definición de cada uno de ellos:

Ciberseguridad[1]**:** La seguridad informática, también conocida como ciberseguridad o seguridad de tecnología de la información, es el área relacionada con la informática y la telemática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida en una computadora o circulante a través de las redes de computadoras. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La ciberseguridad comprende software (bases de datos, metadatos, archivos), hardware, redes de computadoras y todo lo que la organización valore y signifique un riesgo si esta información confidencial llega a manos de otras personas, convirtiéndose, por ejemplo, en información privilegiada.

Herramientas colaborativas[2]**:** Las herramientas colaborativas son servicios informáticos que permiten a los usuarios comunicarse y trabajar conjuntamente sin importar que estén reunidos o no en un mismo lugar físico. Se puede compartir información y producir conjuntamente nuevos materiales resultado de una edición de archivos en equipo.

Ingeniería Social[3]**:** es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Es una técnica que pueden usar ciertas personas para obtener información, acceso o permisos en sistemas de información1 que les permitan realizar algún acto que perjudique o exponga la persona u organismo comprometido a riesgos o abusos.

El principio que sustenta la ingeniería social es el que en cualquier sistema "los usuarios son el eslabón débil".

Phishing[4]**:** es un término informático que denomina a un conjunto de técnicas que persiguen el engaño a una víctima ganándose su confianza haciéndose pasar por una persona, empresa o servicio de confianza (suplantación de identidad de tercero de confianza), para manipularla y hacer que realice acciones que no debería realizar (por ejemplo, revelar información confidencial o hacer click en un enlace). Para realizar el engaño, habitualmente hace uso de la ingeniería social explotando los instintos sociales de la gente, como es de ayudar o ser eficiente. A veces también se hace uso de procedimientos informáticos que aprovechan vulnerabilidades. Habitualmente el objetivo es robar

[1] https://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica
[2] https://empresas.blogthinkbig.com/herramientas-colaborativas-una-nueva-forma-de-trabajar/
[3] https://es.wikipedia.org/wiki/Ingenier%C3%ADa_social_(seguridad_inform%C3%A1tica)
[4] https://es.wikipedia.org/wiki/Phishing

información, pero otras veces es instalar programas malignos, sabotear sistemas, o robar dinero a través de fraudes.

Teletrabajo: de acuerdo con la Ley 1221 de 2008 es "una forma de organización laboral, que consiste en el desempeño de actividades remuneradas o prestación de servicios a terceros utilizando como soporte las tecnologías de la información y comunicación -TIC - para el contacto entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio específico de trabajo"

Trabajo en casa o remoto: es un mecanismo excepcional mediante el cual los servidores públicos podrán realizar sus actividades desde un lugar diferente al de su trabajo habitual, de manera remota y colaborativa haciendo uso de las Tecnologías de la Información y las Comunicaciones existentes, sin que dicha situación constituya la adopción del teletrabajo en las condiciones establecidas en la Ley 1221 de 2008, de acuerdo con lo señalado en su numeral 4 del artículo 6.

8. DESARROLLO DEL INFORME.

En consonancia con los aspectos mencionados en los acápites anteriores y a efectos de hacer una evaluación del cumplimiento de la Entidad en materia de ciberseguridad y trabajo en casa por la emergencia sanitaría por causa del COVID-19, se auditó teniendo en cuenta la siguiente estructura:

Los subcapítulos que conforman la auditoría se enuncian a continuación:

1. Continuidad en la prestación de los servicios de la Entidad por causa del aislamiento preventivo obligatorio y la implementación del trabajo en casa.
2. Seguridad de la información y tratamiento de los riesgos de ciberseguridad por causa del aislamiento preventivo obligatorio y la implementación del trabajo en casa.
3. Comportamiento general de la infraestructura de TI por causa del aislamiento preventivo obligatorio y la implementación del trabajo en casa.

8.1. Continuidad en la prestación de los servicios de la Entidad por causa del aislamiento preventivo obligatorio y la implementación del trabajo en casa.

La mayoría de las organizaciones de hoy son sumamente dependientes de la tecnología de la información (desde equipos portátiles hasta servidores, de escritorio hasta tabletas y smartphones), pero queda claro que esta tecnología puede verse afectada por una amplia gama de incidentes potencialmente desastrosos, en virtud de ello, es necesario asegurar la continuidad de las organizaciones en la prestación de sus servicios.

Cuando hablamos de continuidad del negocio nos referimos a la capacidad de sobrevivir a las “cosas malas” que pueden tener un impacto negativo en la Entidad: desde un brote de virus informático hasta un brote de virus biológico, y todos los demás peligros entre ambos, como incendios, inundaciones, tornados, huracanes, terremotos y tsunamis.

El estándar internacional para la continuidad del negocio, ISO 22301, la define como la “capacidad [de una organización] de continuar la prestación de productos o servicios en los niveles predefinidos aceptables tras incidentes de interrupción de la actividad”.

De acuerdo con la Guía para la preparación de las TIC para la continuidad del negocio V 1.0.0 del 15 de diciembre de 2010 del Ministerio de las Tecnologías de la Información y las Comunicaciones – MinTIC, la Norma ISO 22301 define el Plan de Continuidad del Negocio (También llamado BCP, por sus siglas en inglés) como el conjunto de procedimientos documentados que guían u orientan a las organizaciones para responder, recuperar, reanudar y restaurar la operación a un nivel pre-definido de operación debido una vez presentada o tras la interrupción de sus servicios. Este Plan incluye los recursos, servicios y actividades necesarios para garantizar la continuidad de las funciones críticas del negocio.

El Plan de continuidad del negocio, se conforma por un conjunto de directrices y procedimientos plasmados en un documento técnico, para que cada entidad pueda tomar las acciones pertinentes con miras a la recuperación y restablecimiento de los servicios e infraestructuras de TI interrumpidas por situaciones de desastre o emergencias ocurridas en cualquier instante dentro de las organizaciones.

El plan debe incluir la Gestión de la Continuidad del Negocio (también llamada BCM, por sus siglas en inglés). Gestionar la continuidad es el proceso de lograr esta capacidad y mantenerla, y conforma una parte vital de la gestión de seguridad de sistemas de información, que ahora se conoce más comúnmente como seguridad cibernética.

Entre tanto la misma Norma, define la Gestión de Continuidad del Negocio como un proceso general de gestión holístico que identifica amenazas potenciales a una organización y el impacto que se

podría causar a la operación de negocio que en caso de materializarse y el cual provee un marco de trabajo para la construcción de la resiliencia organizacional con la capacidad de una respuesta efectiva que salvaguarde los intereses de las partes interesadas claves, reputación, marca y actividades de creación de valor.

De igual manera, el plan debe contemplar el Análisis de Impacto de Negocios (También llamado BIA por sus siglas en inglés) como parte del plan de continuidad del negocio y debe entenderse como un marco conceptual sobre el cual las entidades deben planear integralmente los alcances y objetivos, que permiten proteger la información, en todas sus áreas críticas. Las entidades deben establecer un análisis de impacto del negocio, que este alineado con el Plan General de Continuidad del Negocio de la Entidad; este debe tener una estrategia de continuidad de TI, que contenga los objetivos globales de la entidad, con respecto a las dimensiones de disponibilidad de datos, infraestructura tecnológica y recurso humano.

Para desarrollar el plan de continuidad del negocio de TI se debe tener en cuenta:

- Diseñar una estrategia de continuidad de los servicios de TI, que tenga como base la reducción del impacto de una interrupción en los servicios críticos de TI del negocio, este debe estar difundido, aprobado y respaldado por los directivos de la entidad.

- Realizar un análisis e identificación de recursos críticos de TI vitales, de esta manera se establece una estrategia que genere prioridades en caso de presentarse una o varias situaciones que causen interrupciones.

- Establecer procedimientos de control de cambio, que permita asegurar que el plan de continuidad de TI, se encuentre actualizado y permita afrontar las amenazas que traen consigo las nuevas tendencias tecnológicas sin perder el alcance de los requerimientos de la Entidad.

- Elaborar un plan de pruebas de continuidad de TI, que permita verificar y asegurar que los sistemas de TI, puedan ser recuperados de forma segura y efectiva, atendiendo y corrigiendo errores, que atenten contra la disponibilidad de las operaciones.

- Realizar capacitaciones del plan de continuidad de TI y análisis de impacto del negocio, a los entes o partes involucradas de la organización (Equipo de seguridad de sistemas de información de la entidad), para que conozcan cuáles son sus roles y responsabilidades en caso de incidentes o desastres. Es necesario verificar e incrementar el entrenamiento de acuerdo con los resultados de las pruebas de contingencia generadas dentro de la entidad.

• Tanto el plan de continuidad de TI como el análisis de impacto del negocio deben estar disponibles apropiadamente dentro de la organización y en manos de los responsables de las áreas de TI quienes de forma segura deben garantizar su aplicabilidad en los momentos críticos, a su vez la entidad debe propender por un plan de sensibilización al interior de la misma con el propósito de indicar a todos sus miembros sobre la importancia de contar con un plan de continuidad y de análisis del negocio que van a garantizar el normal funcionamiento de las operaciones regulares en caso de presentarse problemas críticos en los sistemas de información y comunicaciones de la entidad.

Por tanto, este Plan que, si bien no es exigido por la Normatividad vigente, si se convierte en un documento de vital importancia para las organizaciones y bajo el presente, por causa de la pandemia, cobra mayor relevancia su implementación como derrotero de las acciones que debe realizar la Entidad para asegurar la continuidad en la prestación de los servicios, máxime cuando se trata de servicios a los ciudadanos.

¿Cómo está la Entidad en la implementación de este Plan?

Mediante correo electrónico de fecha 4 de mayo de 2020 se solicitó al Grupo Interno de Trabajo Tecnologías de la Información y las Telecomunicaciones, la información necesaria que permitiera evidenciar el documento.

El Grupo Interno de Trabajo de Tecnologías de la Información y las Telecomunicaciones remite la siguiente respuesta:

"Dentro de las funciones del G.I.T de Tecnologías de la información y las Telecomunicaciones no se encuentra la construcción de dicho plan. Un BCP comprende la intervención de un grupo interdisciplinario de diferentes áreas como, Planeación, Administrativa y Financiera, Riesgos, Talento Humano, Tecnología, Administración y cohesión de procesos, Planeación ente otros y está dirigido a recuperar y restaurar las funciones críticas ya sea parcial o totalmente ante la presencia de un evento de desastre o de interrupción no deseada".

De igual manera se realizaron preguntas relacionadas con la continuidad del negocio, mediante lista de chequeo remitida el 7 de mayo de 2020 por correo electrónico, para las cuales se obtuvieron las siguientes respuestas y soportes:

ITEM	DESCRIPTOR	CUMPLIMIENTO			OBSERVACIONES
		NO CUMPLE	CUMPLE PARCIALMENTE	CUMPLE	
		(0)	(1)	(2)	
1	¿Cuenta la Entidad con un Plan de Continuidad del Negocio?	X			Dentro de las funciones del G.I.T de Tecnologías de la información y las Telecomunicaciones no se encuentra la construcción de dicho plan.
2	¿Se cuenta con el Análisis de Impacto de Negocio y se encuentra alineado con la Guía para realizar el Análisis de Impacto de Negocios BIA del MINTIC V 2.0?			X	
23	¿Considera que la Entidad ha funcionado de manera efectiva mediante el trabajo en casa o trabajo remoto?			X	
24	¿Se han contemplado planes de contingencia ante un eventual caso de contagio de uno de sus colaboradores o de la necesidad de trabajar por turnos? En caso afirmativo remita el documento (oficial o no)	X			No es del resorte, alcance ni responsabilidad de Tecnología.

Análisis

La Entidad no dispone del Plan de Continuidad de Negocio, sin embargo, si cuenta con el documento de Análisis de Impacto de Negocios BIA, bajo el nombre *Identificación de impactos ante interrupción*

de servicios tecnológicos, con versión de 2020, el cual puede ser consultado en https://anionline.sharepoint.com/:w:/r/Gestion%20VPRE/Sistemas/GD_TI/AuditoriasCI/_layouts/15/Doc.aspx?sourcedoc=%7B31FACA78-8569-4FAF-857A-2D6727911FF2%7D&file=Identificacion%20de%20Impactos%20ante%20Interrupcion%20de%20Servicios%20de%20Tecnologicos%20ANI%202020.docx&action=default&mobileredirect=true

Este documento contempla la totalidad de las fases descritas en la Guía para realizar el Análisis de Impacto de Negocios BIA del MINTIC V 2.0, la evaluación de impactos operacionales, la identificación de procesos críticos, el establecimiento de tiempos de recuperación, la identificación de recursos, la disposición de los RTO/RPO (Recovery Time Objective / Recovery Point Objective), la gestión del riesgo, la clasificación de escenarios de riesgo, la identificación de amenazas y la identificación de vulnerabilidades.

El Grupo Interno de Trabajo de Tecnología de la Información y las Telecomunicaciones a la fecha no ha contemplado ni ha trabajado en planes de contingencia específicos ante eventuales casos de contagio de los colaboradores del GIT, bajo el argumento de que este plan no es de su competencia.

Conclusiones:

En referencia a la documentación de referencia o a las guías necesarias para asegurar la continuidad del negocio, si bien es cierto la Entidad no dispone de un Plan de Continuidad de Negocio y aunque no es exigible por la Normatividad actual, sí cuenta con un muy completo y actualizado Análisis de Impacto de Negocios – BIA.

Este Análisis de Impacto de Negocios se convierte en la piedra angular para construir el Plan de Continuidad de Negocio – BCP, sin embargo, requiere para ello la visión holística, que solo puede ser alcanzada mediante el compromiso y trabajo mancomunado de los diferentes procesos de la Entidad.

Entre tanto, la reacción de la Entidad ante la situación actual de aislamiento preventivo obligatorio a raíz de la pandemia del COVID-19 que obligó a la Entidad a implementar la modalidad del trabajo en casa de manera inmediata de cientos de colaboradores ha sido efectiva como se puede evidenciar en el reporte del funcionamiento efectivo mediante el trabajo en casa o trabajo remoto de mayo de 2020 que puede ser consultado en el siguiente link: https://anionline.sharepoint.com/:w:/r/Gestion%20VPRE/Sistemas/GD_TI/AuditoriasCI/_layouts/15/Doc.aspx?sourcedoc=%7B8CB5264B-6F4F-45FA-A820-7D6D7A9E42A4%7D&file=Evidencia%20Punto%2023.docx&action=default&mobileredirect=true

Concepto del auditor:

CUMPLE CON RECOMENDACIONES

Recomendaciones:

1. Desarrollar, bajo el liderazgo de la Vicepresidencia de Planeación, Riesgos y Entorno, articulando la participación decidida de todos los procesos, la construcción del Plan de Continuidad de Negocio, a partir del insumo, ***Identificación de impactos ante interrupción de servicios tecnológicos,*** elaborado por el Grupo Interno de Trabajo de Tecnologías de la Información y las Comunicaciones.

2. Continuar la elaboración mensual del reporte de funcionamiento de la Entidad, mediante la aplicación de indicadores que den cuenta de la continuidad de la Entidad ante la situación actual que motiva la modalidad de trabajo en casa o trabajo remoto.

3. Elaborar por parte del Grupo Interno de Trabajo de Tecnologías de la Información y las Comunicaciones un plan de contingencia específico de sus recursos (Tecnológicos, humanos, financieros, entre otros) para las eventuales problemáticas ocasionadas por la pandemia del COVID-19.

8.2. Seguridad de la información y tratamiento de los riesgos de ciberseguridad por causa del aislamiento preventivo obligatorio y la implementación del trabajo en casa.

Vivimos momentos de gran incertidumbre. En medio de esta crisis mundial, aún no somos capaces de anticipar cuáles serán las consecuencias que traerá la pandemia de Covid-19 en el plano geopolítico, económico y social, y tampoco sabemos qué ocurrirá con respecto a nuestro modelo de convivencia. Aunque es imposible pronosticar el futuro, incluso a corto plazo, todo apunta a que el Covid-19 está generando un nuevo escenario en el sector de la ciberseguridad, lleno de oportunidades y amenazas. El cibercrimen está prosperando, utilizando la pandemia y una emoción tan humana como el miedo a modo de gancho para lograr sus objetivos.

Si bien la modalidad de trabajo en casa no es nueva, a raíz de la pandemia, la migración de millones de usuarios desde redes empresariales o estatales seguras, que se protegen y se monitorean de

cerca, a redes wi-fi domesticas en gran parte no supervisadas y a menudo inseguras, crea una oportunidad inmensa para los cibercriminales.

Aunque la Entidad está protegida en su entorno común, la implantación del trabajo en casa puede provocar nuevas situaciones y cambios, que dan lugar a abrir brechas y vulnerabilidades que los atacantes aprovechan. La Directiva Presidencial 02 de 2020 al respecto declara que “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”.

Los ciberdelincuentes ya están aprovechando la situación actual para lanzar ataques enfocados en el trabajo en casa. Para ello utilizan métodos muy variados, desde acceso a sistemas con contraseñas poco seguras o robadas por otros medios (Ingeniería Social), a capturar el tráfico que pasa por redes Wi-Fi poco seguras. Además, la actual preocupación por el Coronavirus está generando muchas campañas de phishing con el que logran que los usuarios bajen la guardia atraídos por la curiosidad.

Los aspectos más críticos en materia de ciberseguridad son:

- Seguridad de las redes (Cifrados, autenticación, contraseñas) y Protección de la información (Disponibilidad, integridad, completitud y confiabilidad)
- Accesos o conexiones remotas (VPN)
- Respaldo de la información (Backups y recuperaciones)
- Trabajo en casa y reuniones virtuales (Aplicaciones, Intranet, plataformas de reuniones y herramientas colaborativas)
- Identificación de nuevos riesgos
- Capacitación y buenas prácticas

8.2.1. Seguridad de las redes (Cifrados, autenticación, contraseñas) y Protección de la información (Disponibilidad, integridad, completitud y confiabilidad)

Mediante correo electrónico de fecha 4 de mayo de 2020 se solicitó al Grupo Interno de Trabajo Tecnologías de la Información y las Telecomunicaciones, la información necesaria que permitiera evidenciar el tratamiento de la seguridad de las redes.

Si ha efectuado pruebas de vulnerabilidad de la infraestructura de TI recientemente, remita los resultados.

El Grupo Interno de Trabajo de Tecnologías de la Información y las Telecomunicaciones remite la siguiente respuesta:

"NO se han efectuado pruebas de vulnerabilidad de la infraestructura de TI recientemente. Debido a la contingencia y a la priorización definida teniendo en cuenta las condiciones de la emergencia, y que ha consistido en garantizar las condiciones técnicas y de seguridad adecuadas para una correcta accesibilidad remota a los recursos informáticos de la entidad por parte de funcionarios y contratistas, a este respecto se han concentrado los esfuerzos en hacer seguimiento y monitoreo de la Infraestructura y Servicios Tecnológicos.".

De igual manera se realizaron preguntas relacionadas con la seguridad de las redes, mediante lista de chequeo remitida el 7 de mayo de 2020 por correo electrónico, para las cuales se obtuvieron las siguientes respuestas y soportes:

ITEM	DESCRIPTOR	CUMPLIMIENTO			OBSERVACIONES
		NO CUMPLE	CUMPLE PARCIALMENTE	CUMPLE	
		(0)	(1)	(2)	
3	¿Cuenta la Entidad con Sistemas de autenticación protegidos?			X	
4	¿Cuenta la Entidad con sistema de doble autenticación?			X	
5	En caso afirmativo, ¿Se está practicando doble autenticación para todos los usuarios y en que aplicativos?			X	Se tiene implementado para la suite de Microsoft 365

ITEM	DESCRIPTOR	CUMPLIMIENTO			OBSERVACIONES
		NO CUMPLE	CUMPLE PARCIALMENTE	CUMPLE	
		(0)	(1)	(2)	
6	¿Se han adaptado las configuraciones de seguridad de la infraestructura de TI para el Trabajo en casa o trabajo remoto?			X	
7	¿Cuenta la Entidad con conexiones cifradas desde cualquier ubicación?			X	
8	¿Cuenta la Entidad con un sistema de detección de intrusiones?			X	

ITEM	DESCRIPTOR	CUMPLIMIENTO			OBSERVACIONES
		NO CUMPLE	CUMPLE PARCIALMENTE	CUMPLE	
		(0)	(1)	(2)	
25	¿Qué ocurriría si se presenta un incidente cibernético o de TI? ¿Se podría abordar el incidente de forma remota?			X	

Adjunto a la lista de chequeo se remitieron los documentos con base en los cuales se evidenció el cumplimiento de la Entidad en materia de seguridad de redes y del aseguramiento de los atributos de la información.

Autenticación.
https://anionline.sharepoint.com/:w:/r/Gestion%20VPRE/Sistemas/GD_TI/AuditoriasCI/_layouts/15

/Doc.aspx?sourcedoc=%7B23095ED8-7620-4572-8DBC-71698279138E%7D&file=SISTEMA_DE_AUTENTICACION.docx&action=default&mobileredirect=true

Doble autenticación.

https://anionline.sharepoint.com/Gestion%20VPRE/Sistemas/GD_TI/AuditoriasCI/SitePages/Home.aspx

Configuraciones de seguridad para trabajo en casa.

https://anionline.sharepoint.com/:w:/r/Gestion%20VPRE/Sistemas/GD_TI/AuditoriasCI/_layouts/15/Doc.aspx?sourcedoc=%7B5C8C2BEA-D6F8-481E-A8D6-5EFFB60D3E72%7D&file=CONFIGURACIONES_TRABAJO_EN_CASA.docx&action=default&mobileredirect=true

Conexiones cifradas.

https://anionline.sharepoint.com/:w:/r/Gestion%20VPRE/Sistemas/GD_TI/AuditoriasCI/_layouts/15/Doc.aspx?sourcedoc=%7BEC54B71A-D773-42DC-970D-6E2161B474D0%7D&file=CONEXIONES_CIFRADAS.docx&action=default&mobileredirect=true

Sistema de detección de intrusiones.

https://anionline.sharepoint.com/:w:/r/Gestion%20VPRE/Sistemas/GD_TI/AuditoriasCI/_layouts/15/Doc.aspx?sourcedoc=%7BE0E45960-0102-4A8F-8BEB-CBA36B47E97F%7D&file=SISTEMA%20DE%20DETECCI%C3%93N%20DE%20INTRUSIONES.docx&action=default&mobileredirect=true

Incidentes cibernéticos.

https://anionline.sharepoint.com/:w:/r/Gestion%20VPRE/Sistemas/GD_TI/AuditoriasCI/_layouts/15/Doc.aspx?sourcedoc=%7B115C7921-90D5-442E-879F-091E9C656D89%7D&file=Evidencia%20Punto%2025.docx&action=default&mobileredirect=true

Análisis

Se revisaron los documentos allegados como soporte de cada uno de los aspectos, evidenciando el cumplimiento de los aspectos de seguridad evaluados.

Conclusión

Se destaca como fortaleza el completo y oportuno trabajo realizado por el Grupo Interno de Trabajo de Tecnologías de la Información y las Comunicaciones, dado que se han planeado, implementado y cubierto los protocolos de seguridad necesarios para garantizar el blindaje de la red de la Entidad, el monitoreo permanente y el cubrimiento de las necesidades de la Entidad en materia de cifrado, autenticación y fortaleza en la política de contraseñas.

Al garantizar la seguridad en el acceso y al cifrado de la información que viaja a través de las redes, se asegura el cumplimiento de los atributos de la información: disponibilidad, integridad, completitud y confiabilidad

Concepto del auditor:

CUMPLE CON FORTALEZAS

8.2.2. Accesos o Conexiones Remotas (VPN u otras)

Mediante correo electrónico de fecha 4 de mayo de 2020 se solicitó al Grupo Interno de Trabajo Tecnologías de la Información y las Telecomunicaciones, la información necesaria que permitiera evidenciar la gestión de las conexiones remotas.

Relación de conexiones remotas actuales especificando la fecha de solicitud, el modo habilitado (VPN u otro), la fecha de habilitación, software al que se accede y el nombre de usuario.

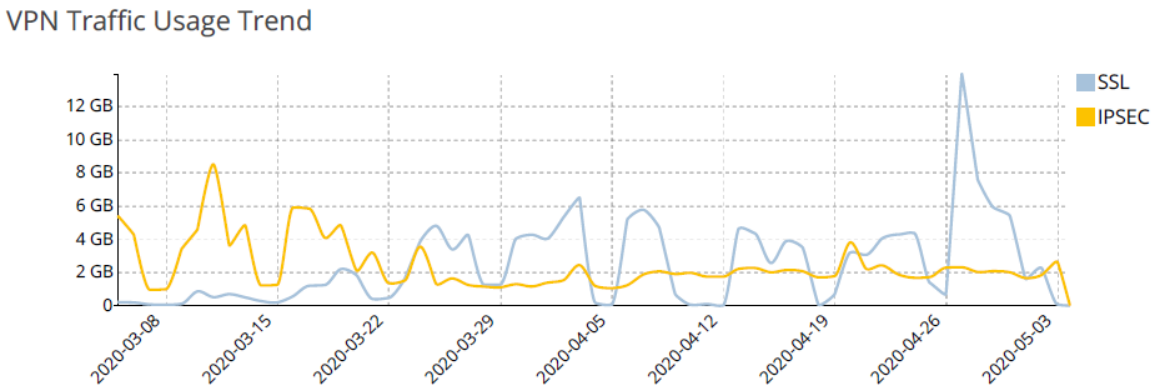
El Grupo Interno de Trabajo de Tecnologías de la Información y las Telecomunicaciones remite la siguiente respuesta:

ID	Usuario	Type	First Used
1	fparrado	ssl-tunnel	26/10/2019 18:37
2	mjaramillo	ssl-tunnel	28/10/2019 11:49
3	cbarrero	ssl-tunnel	1/11/2019 11:20
4	cfgonzalez	ssl-tunnel	26/10/2019 20:01
5	epulido	ssl-tunnel	13/03/2020 11:02

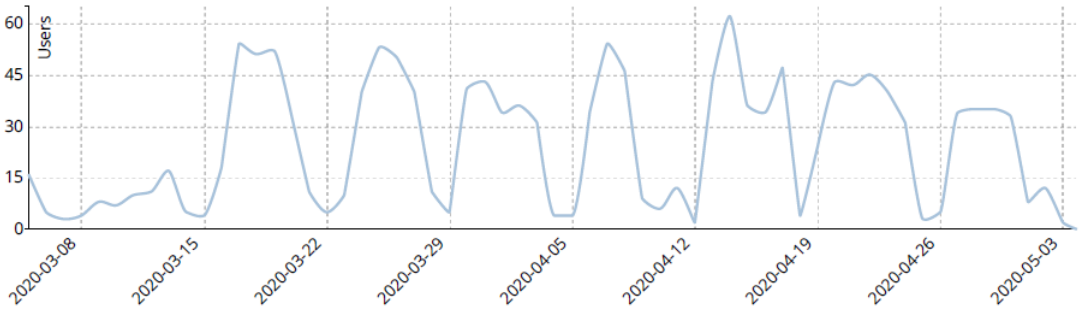
7	rlramirez	ssl-tunnel	18/03/2020 9:22
8	lgomez	ssl-tunnel	28/10/2019 10:20
9	lgil	ssl-tunnel	25/03/2020 16:51
10	scastiblanco	ssl-tunnel	29/10/2019 8:55
11	dsanchez	ssl-tunnel	21/11/2019 16:54
12	jeaguilar	ssl-tunnel	30/10/2019 21:22
13	jpalacios	ssl-tunnel	24/03/2020 19:01
14	rcubillos	ssl-tunnel	28/10/2019 13:05
15	lmrodriguez	ssl-tunnel	17/03/2020 19:11
16	lrojas	ssl-tunnel	17/03/2020 18:13
19	jrivillas	ssl-tunnel	20/03/2020 14:46
20	marcila	ssl-tunnel	18/03/2020 16:31
21	mjperalta	ssl-tunnel	25/03/2020 16:16
22	jalvarez	ssl-tunnel	25/03/2020 18:30
23	narismendy	ssl-tunnel	17/03/2020 17:58
25	amayorga	ssl-tunnel	17/03/2020 15:02
26	dbula	ssl-tunnel	20/01/2020 16:17
27	cagomez	ssl-tunnel	20/03/2020 10:09
28	lfmorales	ssl-tunnel	17/03/2020 11:49
30	gostos	ssl-tunnel	30/03/2020 12:38
31	mgonzalez	ssl-tunnel	28/10/2019 18:09
32	jzuniga	ssl-tunnel	17/11/2019 12:11
33	efranco	ssl-tunnel	18/03/2020 17:05
34	rramirez	ssl-tunnel	28/03/2020 0:16
35	jarodriguez	ssl-tunnel	25/03/2020 14:37
36	gballesteros	ssl-tunnel	18/03/2020 16:51
37	asanchez	ssl-tunnel	19/03/2020 11:38
38	ecastillo	ssl-tunnel	7/04/2020 10:10
40	nosma	ssl-tunnel	17/03/2020 12:52
41	jfernandez	ssl-tunnel	18/03/2020 15:30

42	nmaldonado	ssl-tunnel	8/04/2020 12:07
45	ljrodriguez	ssl-tunnel	17/03/2020 15:59
46	psanchez	ssl-tunnel	26/03/2020 14:46
49	egarcia	ssl-tunnel	17/03/2020 13:41
51	jgutierrez	ssl-tunnel	26/03/2020 8:49
52	imartinez	ssl-tunnel	24/03/2020 16:09
53	faguirre	ssl-tunnel	28/04/2020 19:23
54	drodriguez	ssl-tunnel	18/03/2020 12:43
55	fparradoadm	ssl-tunnel	16/03/2020 22:23
56	cfgonzalezadm	ssl-tunnel	16/04/2020 17:05
57	lovelasquez	ssl-tunnel	16/04/2020 11:03

Soporte del monitoreo de estos accesos remotos frente a su funcionamiento y seguridad



VPN User Logins



Authenticated Logins

#	Usuario	Type	First Used	Total Number of Connections	Total Duration Connected(HH:MM:SS)
1	fparrado	ssl-tunnel	2020-03-05 20:26:30	205	466:44:04
2	epulido	ssl-tunnel	2020-03-13 11:02:40	191	266:57:32
3	rlramirez	ssl-tunnel	2020-03-18 09:22:05	184	253:17:13
4	lgil	ssl-tunnel	2020-03-25 16:51:58	130	148:40:48
5	cfgonzalez	ssl-tunnel	2020-03-14 09:08:11	111	252:32:38
6	cbarrero	ssl-tunnel	2020-03-05 14:35:22	107	89:32:00
7	mjaramillo	ssl-tunnel	2020-03-05 08:53:07	99	132:53:22
8	jpalacios	ssl-tunnel	2020-03-24 19:01:12	93	37:41:33
9	dsanchez	ssl-tunnel	2020-03-08 21:07:53	84	205:34:09
10	jeaguilar	ssl-tunnel	2020-03-16 08:47:56	82	208:25:10

Failed Login Attempts

#	Usuario	Type	Total Number of Failed Attempts
1	epulido	ssl-web	55
2	fparrado	ssl-web	25
3	jeaguilar	ssl-web	24
4	jalvarez	ssl-web	21
5	cbarrero	ssl-web	16
6	jpalacios	ssl-web	16
7	aframirez	ssl-web	12
8	lgil	ssl-web	12
9	cfgonzalez	ssl-web	11
10	rlramirez	ssl-web	11

Top SSL VPN Tunnel Users by Bandwidth

#	User	IP	First Used	Bandwidth	Sent	Received
1	lmrodriguez	186.155.145.77	2020-04-22 07:58:54			23.78 GB
2	lmrodriguez	186.155.99.114	2020-03-31 17:29:54			22.04 GB
3	amayorga	181.61.204.207	2020-03-18 08:26:09			11.49 GB
4	lrojas	190.157.103.210	2020-03-20 08:11:08			10.45 GB
5	cfgonzalez	181.134.21.209	2020-03-14 09:08:11			9.60 GB
6	narismendy	181.61.209.0	2020-03-18 09:41:29			9.38 GB
7	fparrado	186.155.114.100	2020-04-18 00:25:26			7.33 GB
8	lmrodriguez	186.155.167.137	2020-03-22 18:25:50			5.97 GB
9	epulido	186.146.122.102	2020-03-13 11:02:40			4.57 GB
10	fparrado	186.155.97.165	2020-03-07 17:17:23			3.13 GB

Top SSL VPN Users by Duration

#	User	Type	Aggregated Dialed Time(HH:MM:SS)	Aggregated Bytes
1	fparrado	ssl-tunnel	466:58:52	13.07 GB
2	lmrodriguez	ssl-tunnel	298:51:18	58.69 GB
3	epulido	ssl-tunnel	266:57:32	4.57 GB
4	rlramirez	ssl-tunnel	253:17:13	2.62 GB
5	cfgonzalez	ssl-tunnel	253:12:51	9.65 GB
6	jeaguilar	ssl-tunnel	208:25:10	2.17 GB
7	dsanchez	ssl-tunnel	205:34:09	4.35 GB
8	amayorga	ssl-tunnel	181:53:19	11.50 GB
9	mjperalta	ssl-tunnel	174:52:47	1.10 GB
10	narismendy	ssl-tunnel	161:24:46	9.54 GB

De igual manera se realizaron preguntas relacionadas con las conexiones remotas, mediante lista de chequeo remitida el 7 de mayo de 2020 por correo electrónico, para las cuales se obtuvieron las siguientes respuestas y soportes:

ITEM	DESCRIPTOR	CUMPLIMIENTO			OBSERVACIONES
		NO CUMPLE	CUMPLE PARCIALMENTE	CUMPLE	
		(0)	(1)	(2)	
12	¿Que tipo de VPN se está utilizando (IPSec o SSL)?			X	Ambas, SSL y IPSEC
13	¿Cuántas VPN se encuentran			X	82 Creadas y Habiltadas

ITEM	DESCRIPTOR	CUMPLIMIENTO			OBSERVACIONES
		NO CUMPLE	CUMPLE PARCIALMENTE	CUMPLE	
		(0)	(1)	(2)	
	funcionando en la actualidad?				
14	¿Se cuenta con reportes de monitoreo de la(s) VPN en funcionamiento?			X	
15	¿Se cuenta con reportes de auditoría a la(s) VPN actualmente en funcionamiento?			X	

Adjunto a la lista de chequeo se remitieron los documentos con base en los cuales se evidenció el cumplimiento de la Entidad en materia de conexiones remotas.

Tipos de VPN.

https://anionline.sharepoint.com/Gestion%20VPRE/Sistemas/GD_TI/AuditoriasCI/SitePages/Home.aspx

VPN Actuales.

https://anionline.sharepoint.com/:x:/r/Gestion%20VPRE/Sistemas/GD_TI/AuditoriasCI/_layouts/15/Doc.aspx?sourcedoc=%7B7D794FD0-497C-4D72-976D-3F88890425BB%7D&file=VPN%20ACTIVAS.xlsx&action=default&mobileredirect=true

Monitoreo y auditoría VPN.

https://anionline.sharepoint.com/Gestion%20VPRE/Sistemas/GD_TI/AuditoriasCI/Documentos%20compartidos/CIBERSEGURIDAD%20Y%20TELETRABAJO%202020/Evidencias%20Lista%20de%20Chequeo/Punto%2015/VPN%20Report-2020-05-08-1430_479.pdf

Análisis

Se revisan los documentos allegados como soporte de cada uno de los aspectos, evidenciando el cumplimiento de los aspectos de conexiones remotas evaluados.

Conclusión

Se destaca como fortaleza el completo y oportuno trabajo realizado por el Grupo Interno de Trabajo de Tecnologías de la Información y las Comunicaciones, dado que se han planeado, implementado y monitoreado las conexiones remotas para garantizar el buen funcionamiento y el soporte permanente.

Concepto del auditor:

CUMPLE CON FORTALEZAS

8.2.3. Respaldo de la información (Backups y recuperaciones)

Mediante correo electrónico de fecha 4 de mayo de 2020 se solicitó al Grupo Interno de Trabajo Tecnologías de la Información y las Telecomunicaciones, la información necesaria que permitiera evidenciar si la información se encuentra respaldada.

Si ha efectuado pruebas de restauración de copias de respaldo recientemente, remita los resultados.

El Grupo Interno de Trabajo de Tecnologías de la Información y las Telecomunicaciones remite la siguiente respuesta:

"Sí se han efectuado pruebas de restauración de copias de respaldo recientemente. Las pruebas de restauración se han realizado sobre los servicios de Orfeo, Aniscopio y Portal ANI. Adicional a eso se ha realizado el debido monitoreo de las Copias de Seguridad implementadas en los sistemas: Directorio Activo, Intranet, UniANI, Orfeo, Aniscopio, Portal ANI."

1. PORTAL-ANI: https://www.ani.gov.co

1..1 Backups

Ver PORTAL-ANI_Backups.xlsx

1..2 Restore

Ver PORTAL-ANI_Restores.xlsx

2. INTRANET: https://intranet.ani.gov.co

2..1 Backups

Ver INTRANET_Backups.xlsx

3. UNIANI: https://uniani.ani.gov.co

3..1 Backups

Ver UNIANI_Backups.xlsx

4. DIRECTORIO ACTIVO

4..1 Backups

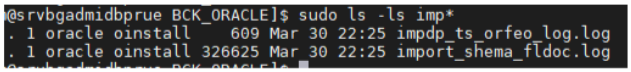
Ver AD_Backups.xlsx

5. ORFEO

5..1 Backups

Ver ORFEO_Backups.xlsx

5..2 Restore



De igual manera se realizaron preguntas relacionadas con el respaldo de la información, mediante lista de chequeo remitida el 7 de mayo de 2020 por correo electrónico, para las cuales se obtuvieron las siguientes respuestas y soportes:

ITEM	DESCRIPTOR	CUMPLIMIENTO			OBSERVACIONES
		NO CUMPLE	CUMPLE PARCIALMENTE	CUMPLE	
		(0)	(1)	(2)	
26	¿Depende de personas claves para responder al incidente? En caso afirmativo, ¿de qué manera podría reducir esa dependencia? ¿Confía en que las copias de seguridad están actualizadas y en que, en el peor escenario, se podrán recuperar los datos y sistemas corporativos clave?			X	Existe esquema multidisciplinario en la administración de la plataforma. Se cuenta con respaldos y esquemas de recuperación de datos para los sistemas Claves.

Adjunto a la lista de chequeo se remitieron los documentos con base en los cuales se evidenció el cumplimiento de la Entidad en materia de respaldo y restauración de la información.

Backups y Restore.

https://anionline.sharepoint.com/:x:/r/Gestion%20VPRE/Sistemas/GD_TI/AuditoriasCI/_layouts/15/Doc.aspx?sourcedoc=%7B595C306E-2CC8-4ADB-8D1B-1ED15D52F3BC%7D&file=Cuadro%20administracion%20Plataformas.xlsx&action=default&mobileredirect=true

Instructivo.

https://anionline.sharepoint.com/:w:/r/Gestion%20VPRE/Sistemas/GD_TI/AuditoriasCI/_layouts/15/Doc.aspx?sourcedoc=%7BB5AD2C32-2353-46F5-AF33-DD7D61EE8259%7D&file=GTEC-I-

0XX%20COPIAS_DE_SEGURIDAD_INFRAESTRUCTURA_TECNOLOGICA_Y_SISTEMAS_DE_INFORMACI%C3%93N.docx&action=default&mobileredirect=true

Análisis

Se revisan los documentos allegados como soporte de cada uno de los aspectos, evidenciando el cumplimiento de los aspectos de respaldo y restauración de la información.

Conclusión

Se destaca como fortaleza el completo y oportuno trabajo realizado por el Grupo Interno de Trabajo de Tecnologías de la Información y las Comunicaciones, dado que se han planeado, implementado y realizado las copias de seguridad y probando la restauración de estos respaldos lo cual garantiza la recuperación de información clave ante eventuales interrupciones del servicio.

Concepto del auditor:

CUMPLE CON FORTALEZAS

8.2.4. Trabajo en casa y reuniones virtuales (Aplicaciones, Intranet, plataformas de reuniones y herramientas colaborativas).

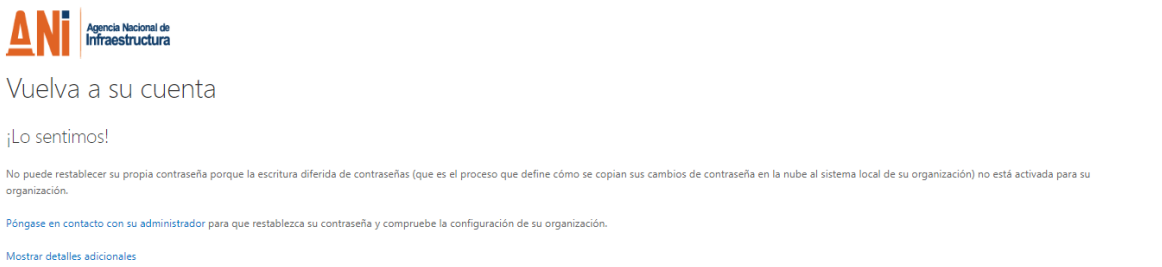
Para evaluar el comportamiento de la Agencia ante ingresos no deseados o ataques a la seguridad, se realizaron tres pruebas: la primera, mediante el uso de herramientas de revelación de claves que se encuentran fácilmente en Internet, la segunda, ingresando claves sencillas con palabras relacionadas y tercera, mediante la aplicación de ingeniería social, a través de la solicitud engañosa para la revelación de su clave de acceso.

Una vez logrado el acceso, se efectúan pruebas de penetración de caja blanca para determinar hasta donde se puede adentrar a la organización y que información sensible se puede obtener.

Las pruebas se practicaron en aplicaciones como Orfeo, ANISCOPIO, el correo de Outlook y de la Intranet de la Agencia, obteniendo los siguientes resultados:

La primera prueba se realizó usando el software Hydra 9.0, a 5 cuentas aleatorias, para las cuales resultó negativa en virtud de la fortaleza de las contraseñas que utilizan combinación de mayúsculas, minúsculas, números y caracteres especiales.

La segunda prueba se realizó probando claves con palabras relacionadas con la organización, se probó con 5 usuarios aleatorios y tampoco fue posible el ingreso, incluso se realizó el proceso de recuperación de contraseña arrojando el siguiente resultado



La tercera prueba, se obtuvo una clave de acceso, a través de ingeniería social y con ella se realizaron pruebas de penetración, y se obtuvo acceso a la información propia del usuario para el correo, archivos de onedrive y sharepoint, sin embargo, al intentar penetrar a servidores el acceso fue denegado.

De igual manera, al intentar ingresar en aplicativos como Orfeo, este requería una contraseña diferente. En el caso, de ANISCOPIO y la Intranet accedió, pero no se encuentra información diferente a la que se puede obtener públicamente de la página web de la Entidad.

En resumen, la política de contraseñas es robusta y la segmentación de usuarios y permisos se encuentra acorde. La información sensible no se encuentra accesible y no se advierte el acceso a servidores.

La penetración de caja blanca solo se pudo practicar a nivel de usuarios y estos al tener la información en la nube, no permite la obtención de información relevante.

8.2.5. Identificación de nuevos riesgos

Mediante correo electrónico de fecha 4 de mayo de 2020 se solicitó al Grupo Interno de Trabajo Tecnologías de la Información y las Telecomunicaciones, la información necesaria que permitiera

evidenciar el tratamiento de los riesgos relacionados con ciberseguridad y la identificación de nuevos riesgos.

Documento con la identificación de riesgos de TI ocasionados por el Trabajo en casa y su tratamiento.

El Grupo Interno de Trabajo de Tecnologías de la Información y las Telecomunicaciones remite la siguiente respuesta:

Se remite la Matriz de riesgos del proceso:

https://anionline.sharepoint.com/:x:/r/Gestion%20VPRE/Sistemas/GD_TI/AuditoriasCI/_layouts/15/Doc.aspx?sourcedoc=%7B9A91B145-730B-4E05-B9D1-AC6AFB4E2EC1%7D&file=Matriz_de_riesgos_gestion%20tecnologica%20Abril%202020.xlsx&action=default&mobileredirect=true

De igual manera se realizaron preguntas relacionadas con los riesgos, mediante lista de chequeo remitida el 7 de mayo de 2020 por correo electrónico, para las cuales se obtuvieron las siguientes respuestas y soportes:

ITEM	DESCRIPTOR	CUMPLIMIENTO			OBSERVACIONES
		NO CUMPLE	CUMPLE PARCIALMENTE	CUMPLE	
		(0)	(1)	(2)	
9	¿La Entidad dispone de controles proactivos y reactivos de Ciberseguridad y para trabajo en casa?			X	
10	¿Se implementaron a partir de la emergencia sanitaria nuevos controles de Ciberseguridad Proactivos (prevención de incidentes,			X	No se han implementado nuevos. Si se han afinado y ajustado los ya existentes.

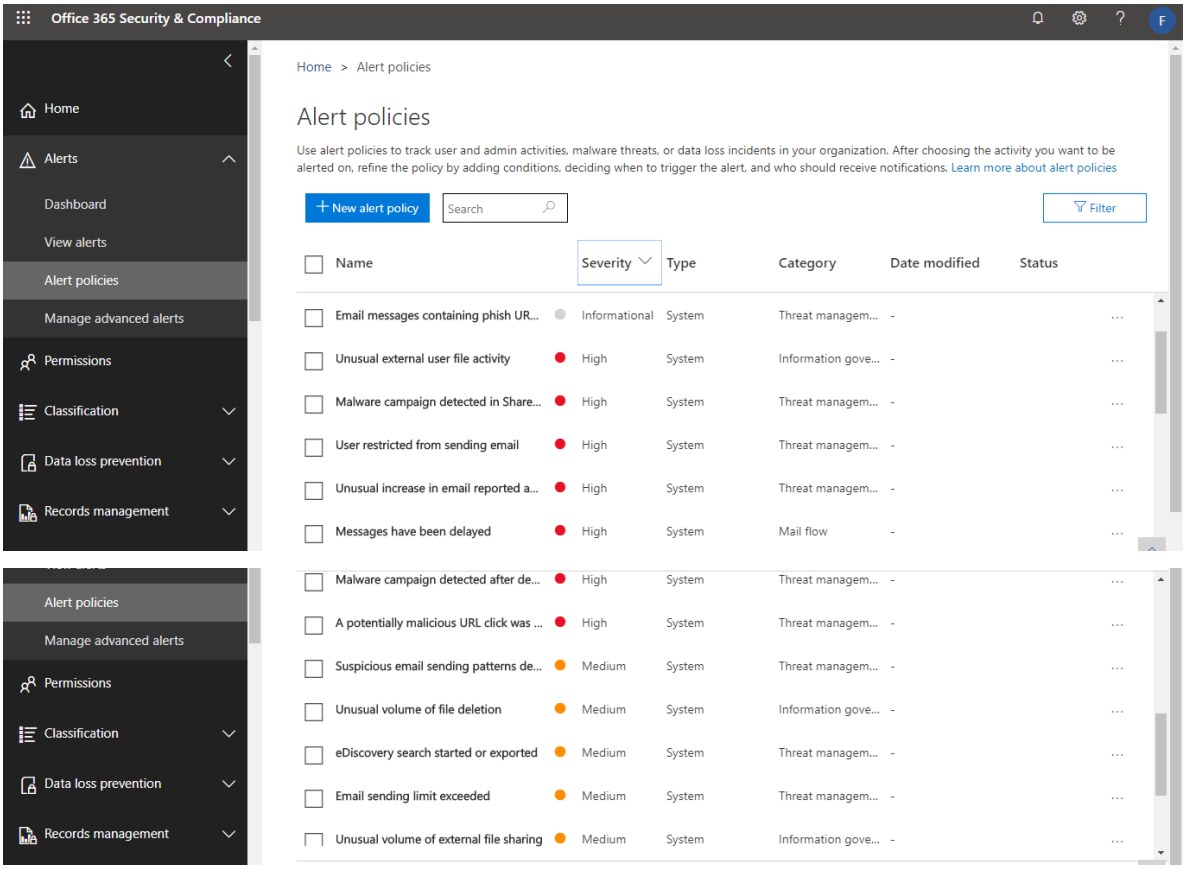
ITEM	DESCRIPTOR	CUMPLIMIENTO			OBSERVACIONES
		NO CUMPLE	CUMPLE PARCIALMENTE	CUMPLE	
		(0)	(1)	(2)	
	vulnerabilidades, riesgos, recuperaciones, entre otras)?				
11	¿Se implementaron a partir de la emergencia sanitaria nuevos controles de Ciberseguridad Reactivos (Gestión de incidentes, mitigación de amenazas en tiempo real, aplicación de parches de hw y sw, entre otros)?			X	No se han implementado nuevos. Si se han afinado y ajustado los ya existentes.
21	¿Se han identificado los nuevos riesgos surgidos a partir de la emergencia sanitaria del Covid-19?			X	No hemos identificado Nuevos Riesgos.

Adjunto a la lista de chequeo se remitieron los documentos con base en los cuales se evidenció el cumplimiento de la Entidad en materia de riesgos de ciberseguridad.

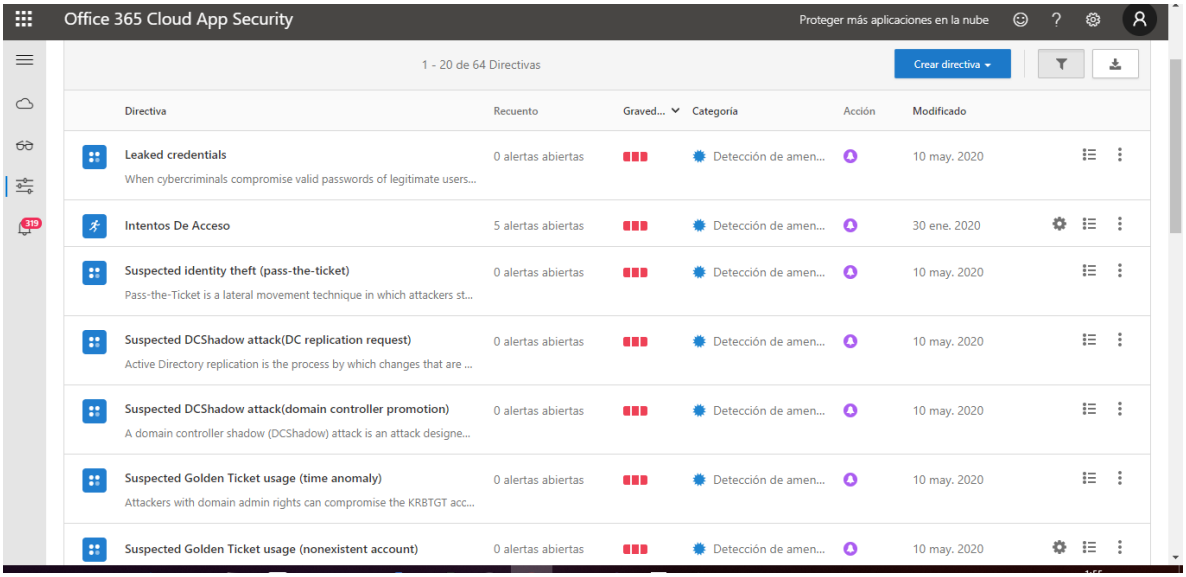
Controles proactivos y reactivos.

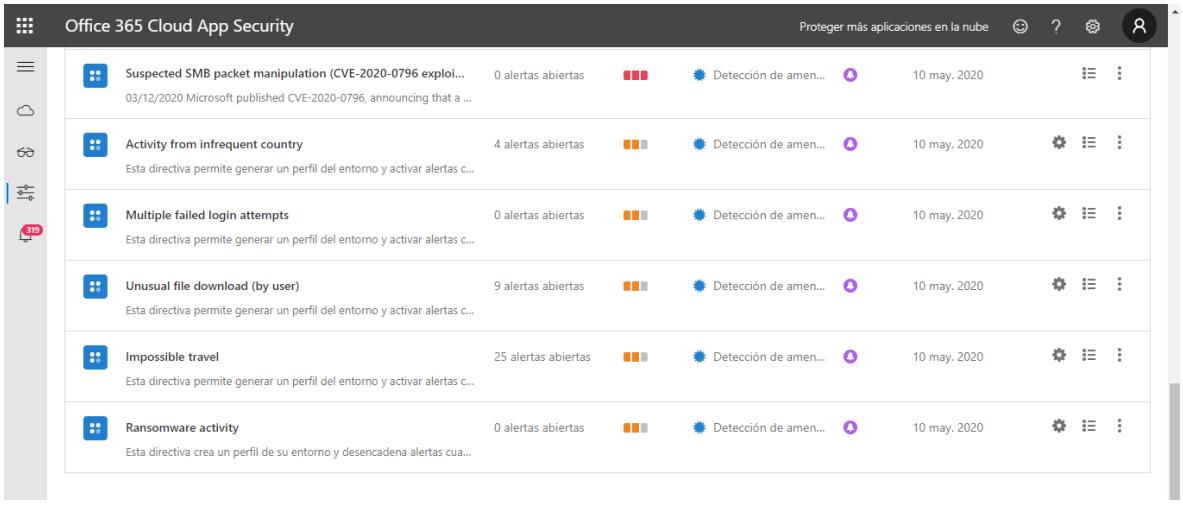
Desde el año 2019 se vienen implementando controles de Ciberseguridad proactivos a través de las diferentes plataformas que se tienen en la ANI.

En office 365 se cuentan con diferentes políticas de alertas

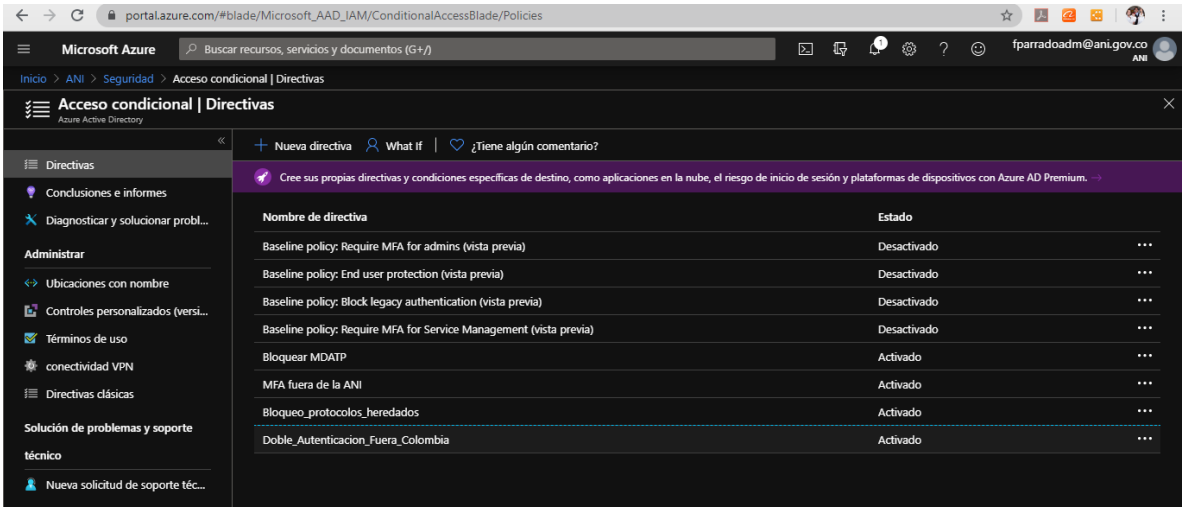


Y en el moódulo de Office 365 Cloud App Security se crearon algunas alertas como intentos fallidos, viajes imposibles entre otros, en el moódulo que se ve en la siguiente imagen:

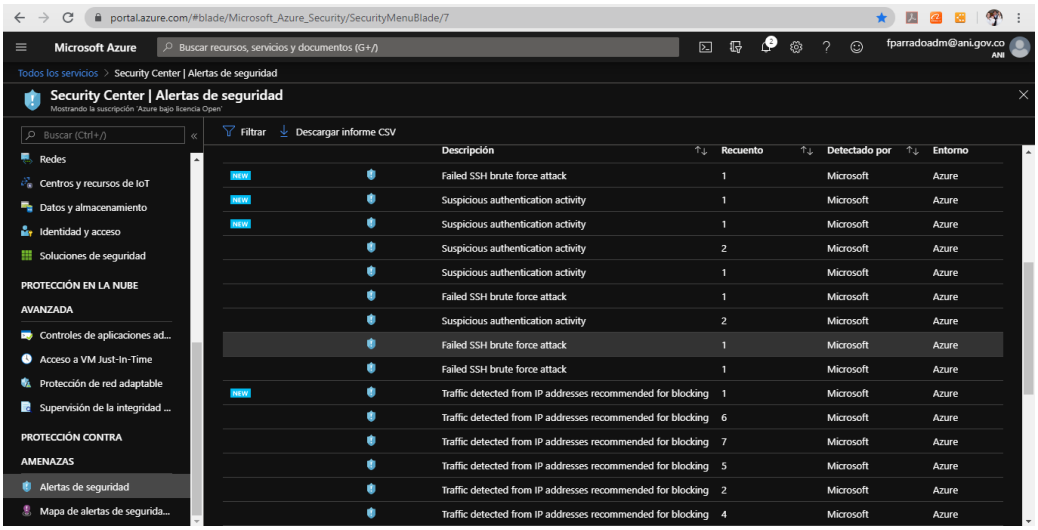




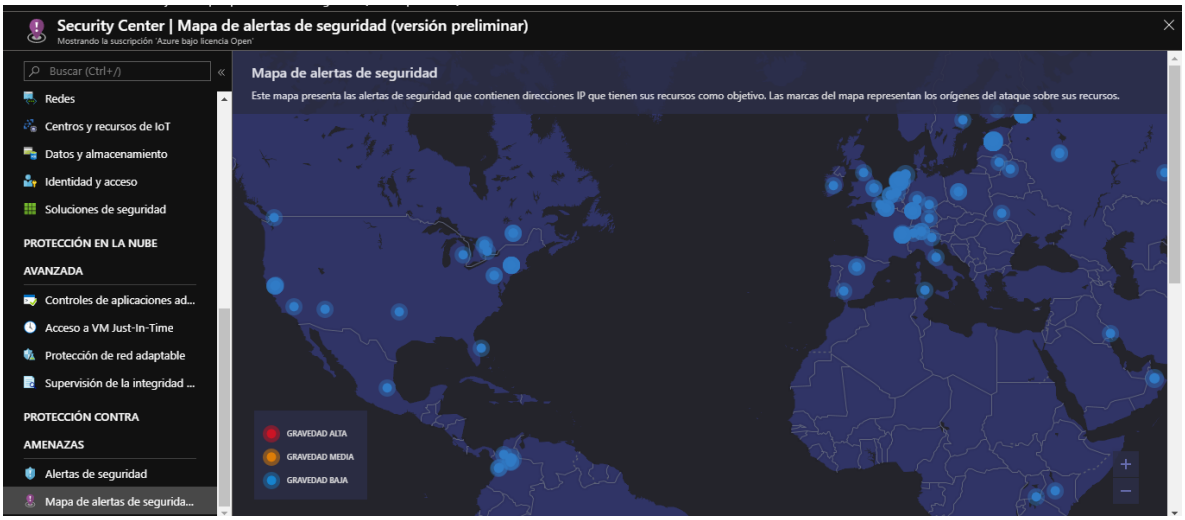
En el Active directorio se crearon accesos condicionales donde se bloquearon protocolos heredados no seguros y doble autenticación fuera de Colombia, entre otros como se observa en la imagen:

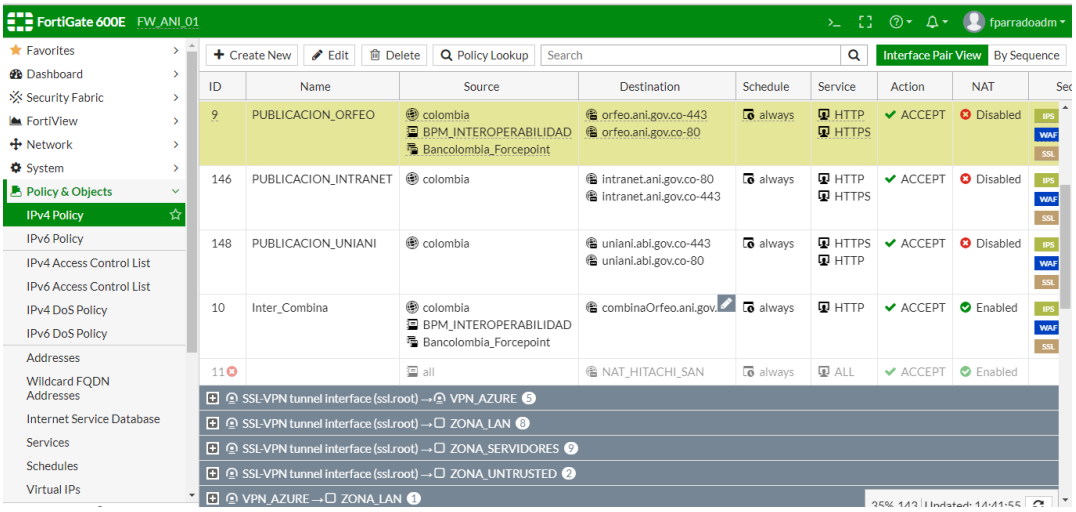


En la nube de azure se han bloqueado ips de donde se generan ataques a los servicios de la entidad, así como se reforzaron las claves de las cuentas administradoras para que cuenten con un nivel alto de seguridad y los ataques de fuerza bruta no tenga resultados en nuestros servicios.

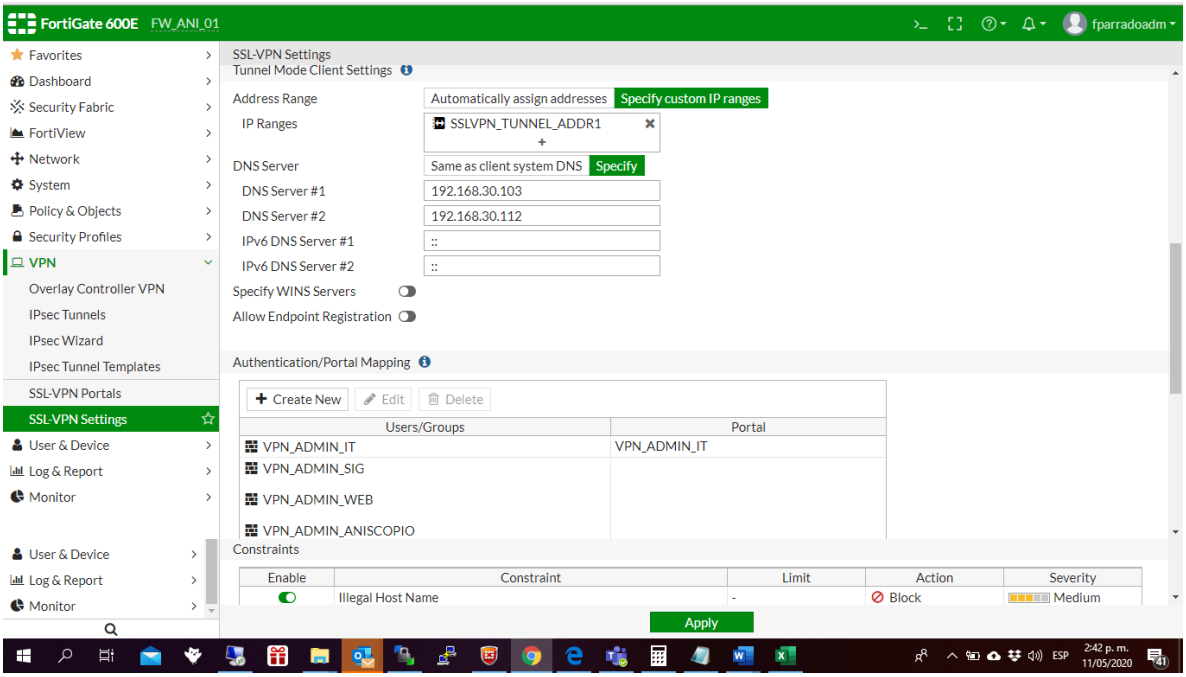


En la imagen se observa las direcciones Ips donde se han tratado de realizar ataques a la entidad y su nivel de gravedad, de lo que se observa que de varios lugares se ha intentado pero el nivel de gravedad es baja debido a los controles y configuraciones de los servicios de la ANI.





Por otro lado se han configurado servicio para mejorar la protección de las aplicaciones expuestas donde se configuró el módulo de WAF en el firewall.



Acceso a usuarios fuera de la entidad por medio de conexiones cifradas VPN SSL

Análisis

Se revisan los documentos allegados como soporte de cada uno de los aspectos, evidenciando el cumplimiento de los aspectos de tratamiento de los riesgos y el cubrimiento de los riesgos de ciberseguridad.

Conclusión

Se destaca como fortaleza el completo y oportuno trabajo realizado por el Grupo Interno de Trabajo de Tecnologías de la Información y las Comunicaciones, dado que se han identificado concienzudamente y gestionado los riesgos de ciberseguridad y como consecuencia de la situación actual han revisado la identificación de nuevos riesgos, lo que ha permitido el refinamiento en el

tratamiento de los riesgos existentes. Lo anterior se ha manifestado en la no materialización de riesgos y en la efectiva gestión de la infraestructura de TI incluida la seguridad y disponibilidad de la información.

Concepto del auditor:

CUMPLE CON FORTALEZAS

8.2.6. Capacitación y buenas prácticas en materia de Ciberseguridad y trabajo en casa

Mediante correo electrónico de fecha 4 de mayo de 2020 se solicitó al Grupo Interno de Trabajo Tecnologías de la Información y las Telecomunicaciones, la información necesaria que permitiera evidenciar la capacitación a los colaboradores de la Entidad y el acceso al banco de buenas prácticas en materia de Ciberseguridad y Trabajo en Casa.

Copia o soporte de capacitación o instructivos para trabajo en casa dada a los colaboradores de la Entidad.

El Grupo Interno de Trabajo de Tecnologías de la Información y las Telecomunicaciones remite la siguiente respuesta:

"Se adjunta soporte evidencia de los documentos y piezas informativas guía dispuestas como apoyo a los funcionarios y/o contratistas para adelantar trabajo remoto"

https://anionline.sharepoint.com/:f:/r/Gestion%20VPRE/Sistemas/GD_TI/AuditoriasCI/Documentos%20compartidos/CIBERSEGURIDAD%20Y%20TELETRABAJO%202020/Punto_06_Trabajo_en_Casa?csf=1&web=1&e=8INUra

Copia o soporte de buenas prácticas en materia de seguridad de la información para trabajo en casa a los colaboradores de la Entidad.

El Grupo Interno de Trabajo de Tecnologías de la Información y las Telecomunicaciones remite la siguiente respuesta:

"Se adjunta soporte evidencia de los documentos con recomendaciones, buenas prácticas tendientes a obtener un buen nivel de seguridad de la información y piezas informativas guía dispuestas como apoyo a los funcionarios y/o contratistas para adelantar trabajo remoto".
https://anionline.sharepoint.com/:f:/r/Gestion%20VPRE/Sistemas/GD_TI/AuditoriasCI/Documentos%20compartidos/CIBERSEGURIDAD%20Y%20TELETRABAJO%202020/Punto_07_Buenas_Practicas_Seguridad_de_la_Informacion?csf=1&web=1&e=QTPcoj

Si ha generado documentos adicionales relacionados con Ciberseguridad y Trabajo remoto remitir copia.

"*A fin de contar con apoyo técnico adicional para temas relacionados con Ciberseguridad y trabajo remoto, y teniendo en cuenta entre otros aspectos la actual contingencia, se ha construido el siguiente documento.*

- *GTEC-I-032 Tratamiento de Vulnerabilidades Técnicas.*

Adicionalmente se hace mención a 2 documentos que se encuentran en etapa de construcción (no se adjuntan)

- *Manual de políticas específicas de seguridad y privacidad de la información V2 revisión 30 abril 2020 – Se encuentra en revisión segunda versión. (G.I.T de Tecnología)*

- *Borrador del plan general del proyecto de teletrabajo. La Coordinación de Tecnología apoya y participa en la construcción, pero no administra la versión de este documento. (VAF)"*

https://anionline.sharepoint.com/:f:/r/Gestion%20VPRE/Sistemas/GD_TI/AuditoriasCI/Documentos%20compartidos/CIBERSEGURIDAD%20Y%20TELETRABAJO%202020/Punto_13_Documentos_Ciberseguridad?csf=1&web=1&e=b39Jka

De igual manera se realizaron preguntas relacionadas con la capacitación y la divulgación de buenas prácticas, mediante lista de chequeo remitida el 7 de mayo de 2020 por correo electrónico, para las cuales se obtuvieron las siguientes respuestas y soportes:

ITEM	DESCRIPTOR	CUMPLIMIENTO			OBSERVACIONES
		NO CUMPLE	CUMPLE PARCIALMENTE	CUMPLE	
		(0)	(1)	(2)	
16	¿Se ha informado a los colaboradores de la Entidad las buenas prácticas en materia de ciberseguridad y seguridad para trabajo en casa o trabajo remoto (mensajes de correo malintencionados, ingeniería social, Phishing, Corona-Phishing, Corona-Smishing, Corona-ware, asignación de claves para reuniones fuera de la plataforma de Teams, entre otros?			**X**	

Adjunto a la lista de chequeo se remitieron los documentos con base en los cuales se evidenció el cumplimiento de la socialización de buenas prácticas en materia de ciberseguridad.

https://anionline.sharepoint.com/:f:/r/Gestion%20VPRE/Sistemas/GD_TI/AuditoriasCI/Documentos%20compartidos/CIBERSEGURIDAD%20Y%20TELETRABAJO%202020/Evidencias%20Lista%20de%20Chequeo/Punto%2016?csf=1&web=1&e=4FutJa

Análisis

Se revisan los documentos allegados como soporte de cada uno de los aspectos, evidenciando el cumplimiento de los aspectos de capacitación y comunicación de buenas prácticas de ciberseguridad.

Conclusión

El Grupo Interno de Trabajo de tecnologías de la Información y las Comunicaciones ha realizado campañas para capacitar a los colaboradores de la Entidad en temas de soporte y acceso, no se evidencian capacitaciones específicas de ciberseguridad como ingeniería social, Phishing, Corona-Phishing, Corona-Smishing, Corona-ware, asignación de claves para reuniones fuera de la plataforma de Teams, por mencionar algunos temas relevantes por la situación de pandemia.

Es importante tener presente que mejorar el conocimiento y la preparación de los colaboradores de la Entidad sobre los peligros a los que se encuentra expuesto por la implementación de trabajo en casa, fortalecerá la seguridad de la Entidad.

Concepto del auditor:

CUMPLE CON RECOMENDACIONES

Recomendación:

Se recomienda revisar temas actuales relacionados con aspectos de seguridad derivados del trabajo remoto y riesgos de ciberseguridad que puedan ser compartidos con los colaboradores de la Entidad a través de capacitaciones o foros virtuales, e-cards, banners, UniANI o a través de los medios dispuestos por la Entidad para tal fin.

8.3. Comportamiento general de la infraestructura de TI por causa del aislamiento preventivo obligatorio y la implementación del trabajo en casa.

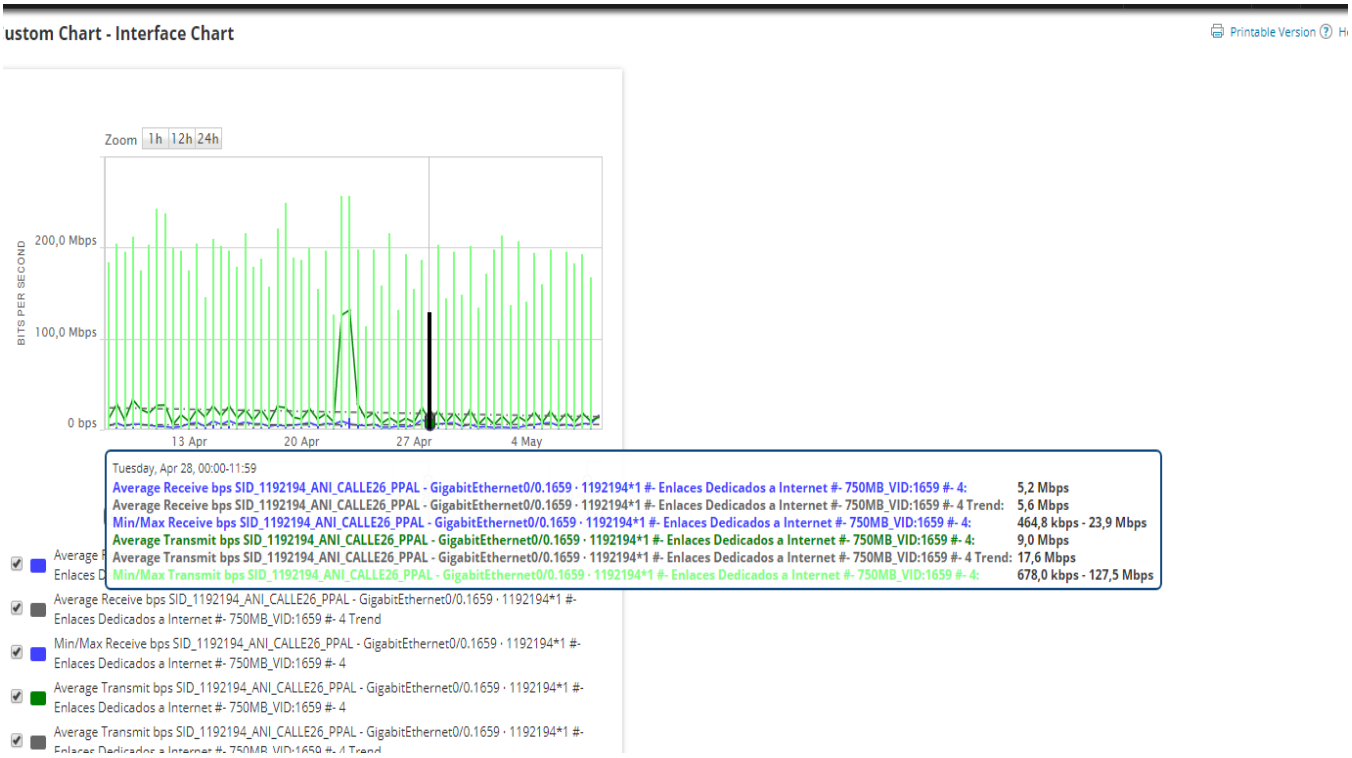
Mediante correo electrónico de fecha 4 de mayo de 2020 se solicitó al Grupo Interno de Trabajo Tecnologías de la Información y las Telecomunicaciones, la información necesaria que permitiera evidenciar el comportamiento en general de los recursos de TI, especialmente lo que tiene que ver con el tratamiento de fallas o incidentes de seguridad, suficiencia del recurso humano y del hardware, la verificación de la cobertura de antivirus y firewall y la identificación de necesidades.

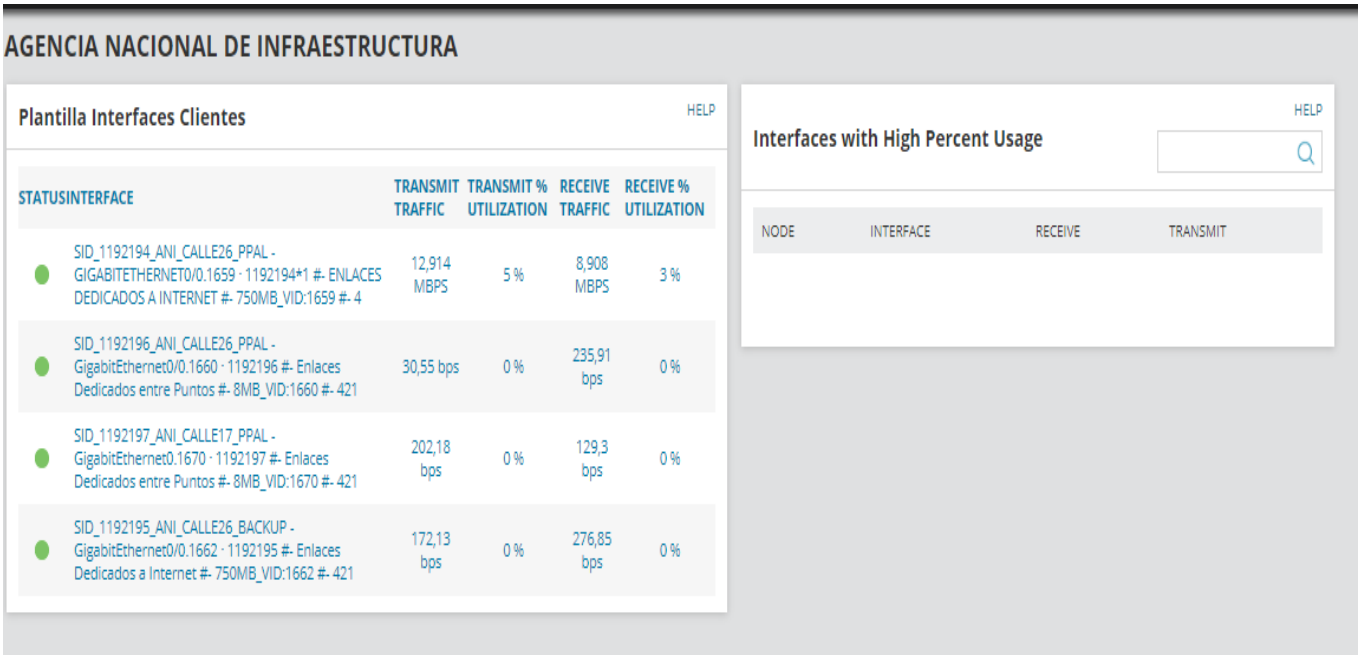
8.3.1. Tratamiento de fallas o incidentes de seguridad.

Reporte de monitoreo de la seguridad de la infraestructura de TI de la Entidad y reporte de fallas o incidentes de seguridad y su tratamiento.

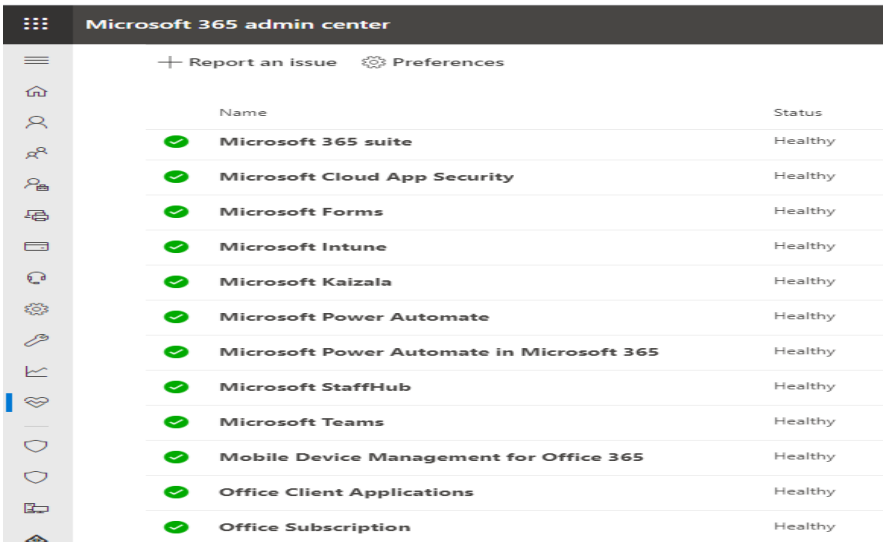
"Se adjunta soporte evidencia con la descripción de las herramientas de monitoreo, así como el reporte general del nivel de estabilidad y disponibilidad de la plataforma".

CANAL DE INTERNET

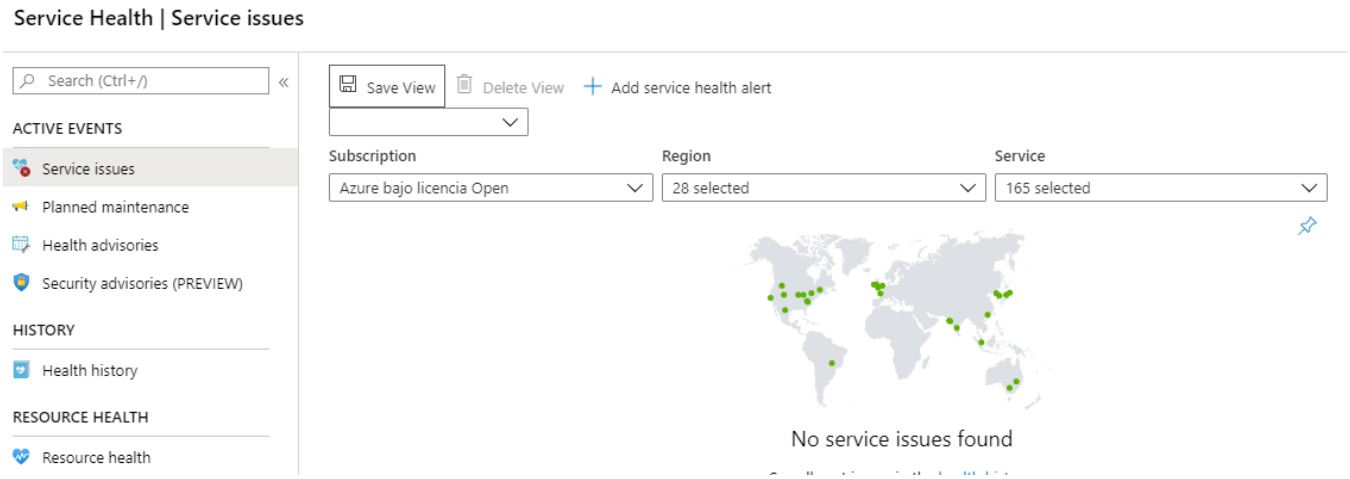




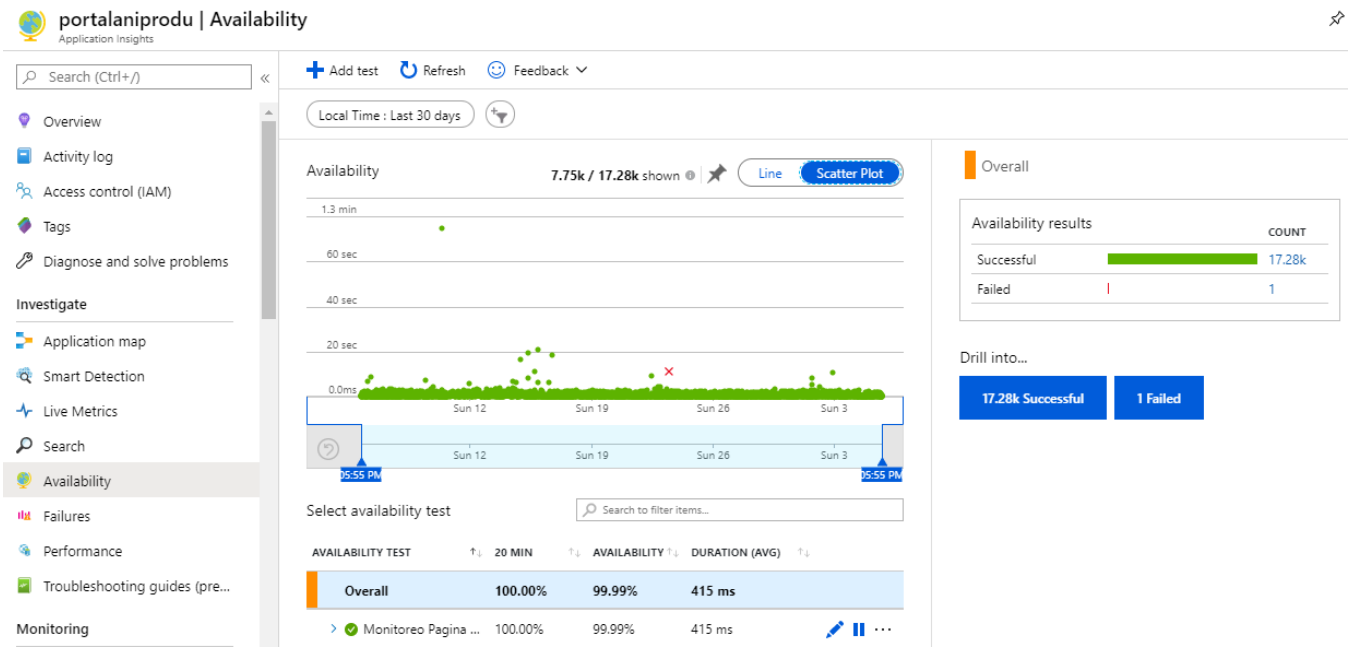
MICROSOFT OFFICE 365

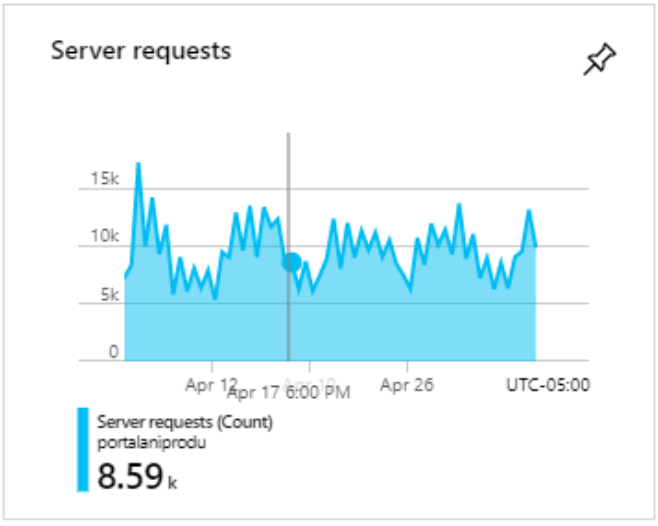


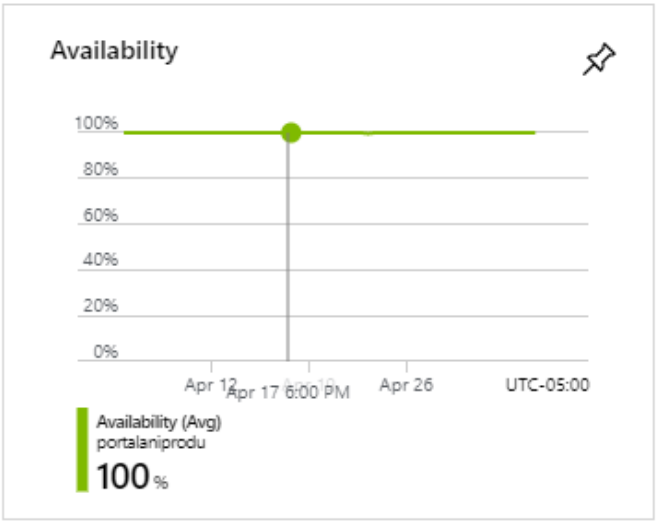
MICROSOFT AZURE



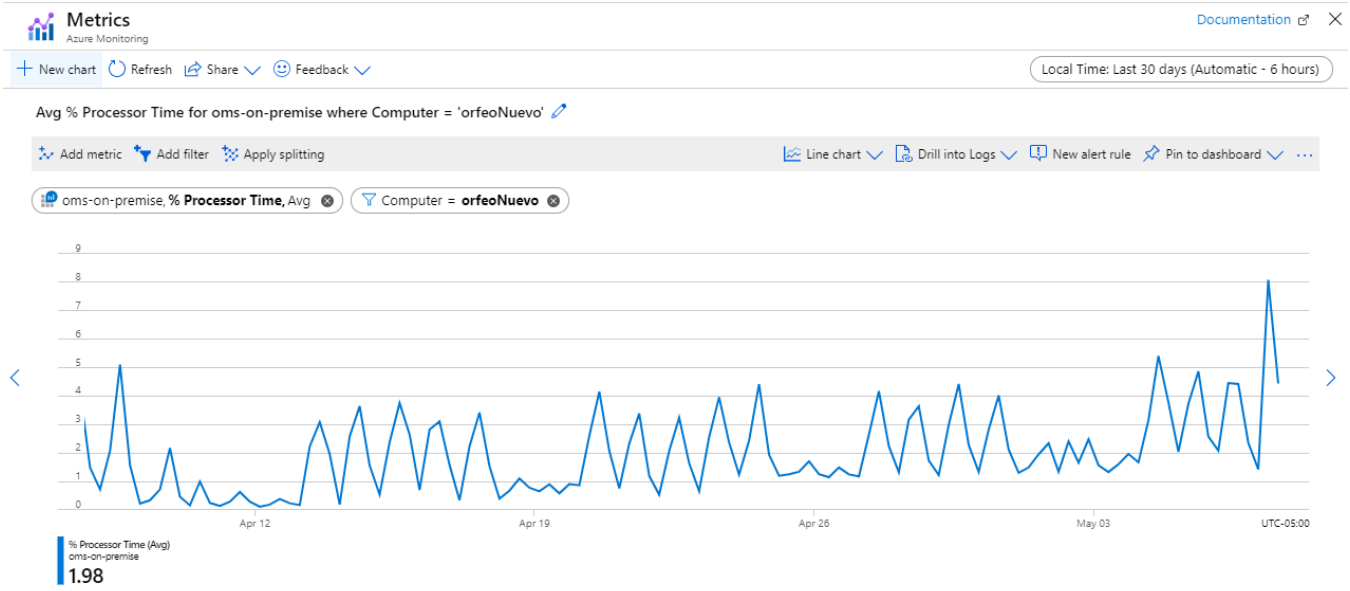
PORTAL-ANI: https://www.ani.gov.co

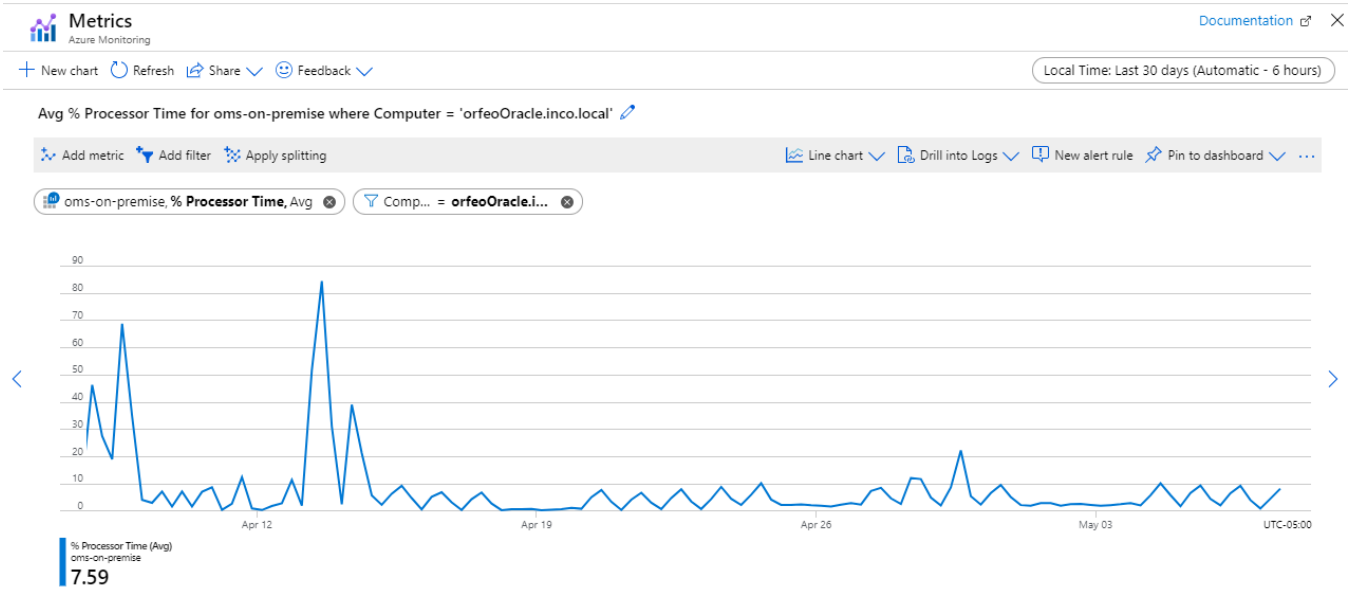

portalaniprodu | Availability
Application Insights
Search (Ctrl+/)
Add test
Refresh
Feedback
Local Time : Last 30 days
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Investigate
Application map
Smart Detection
Live Metrics
Search
Availability
Failures
Performance
Troubleshooting guides (pre...
Monitoring
Availability
7.75k / 17.28k shown
Line
Scatter Plot
1.3 min
60 sec
40 sec
20 sec
0.0ms
Sun 12
Sun 19
Sun 26
Sun 3
05:55 PM
Overall
Availability results
COUNT
Successful
17.28k
Failed
1
Drill into...
17.28k Successful
1 Failed
Select availability test
Search to filter items...
AVAILABILITY TEST
20 MIN
AVAILABILITY
DURATION (AVG)
Overall
100.00%
99.99%
415 ms
Monitoreo Pagina ...
100.00%
99.99%
415 ms


Server requests
15k
10k
5k
0
Apr 12
Apr 17 6:00 PM
Apr 26
UTC-05:00
Server requests (Count)
portalaniprodu
8.59 k

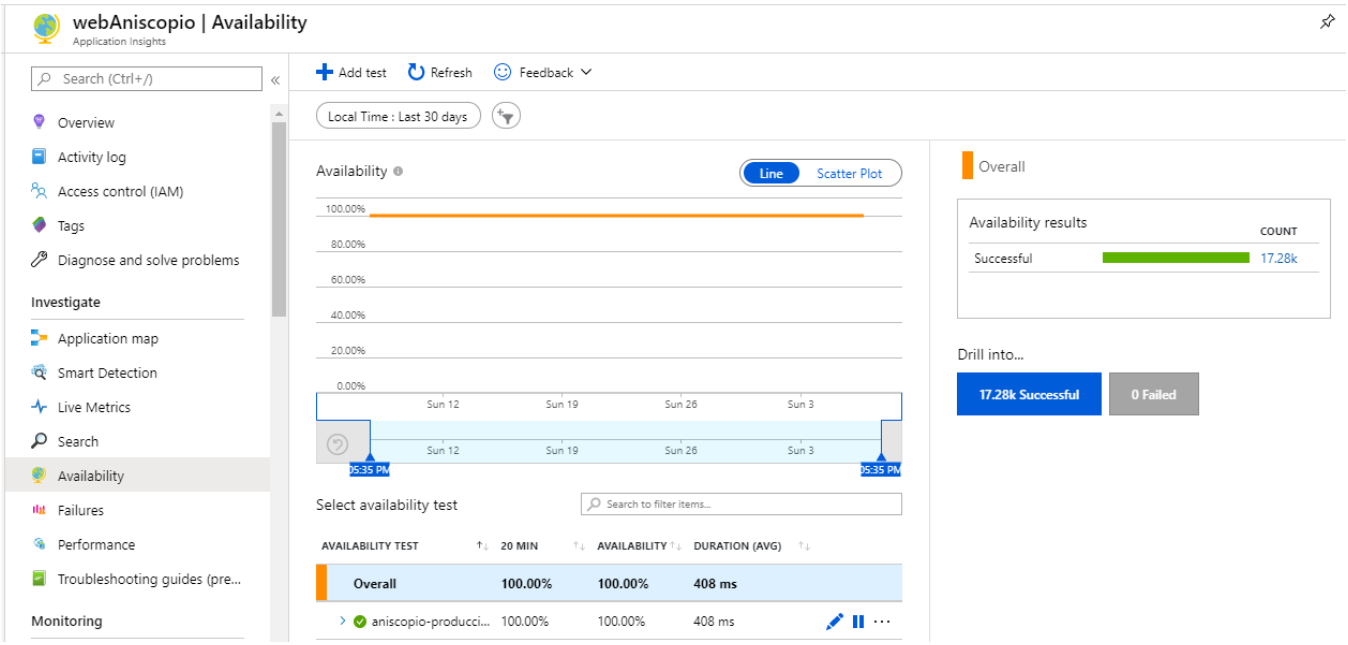

Availability
100%
80%
60%
40%
20%
0%
Apr 12
Apr 17 6:00 PM
Apr 26
UTC-05:00
Availability (Avg)
portalaniprodu
100 %

ORFEO: https://orfeo.ani.gov.co





ANISCOPIO: https://aniscopio.ani.gov.co



De igual manera se realizaron preguntas relacionadas con el tratamiento de fallas o incidentes, mediante lista de chequeo remitida el 7 de mayo de 2020 por correo electrónico, para las cuales se obtuvieron las siguientes respuestas y soportes:

ITEM	DESCRIPTOR	CUMPLIMIENTO			OBSERVACIONES
		NO CUMPLE	CUMPLE PARCIALMENTE	CUMPLE	
		(0)	(1)	(2)	
18	En caso de soporte remoto, ¿Cómo se está llevando a cabo (herramientas utilizadas, cantidad de casos y tratamiento)?			X	Correo Microsoft 365, Herramienta Teams para tomar el control remoto y Herramienta GLPI

ITEM	DESCRIPTOR	CUMPLIMIENTO			OBSERVACIONES
		NO CUMPLE	CUMPLE PARCIALMENTE	CUMPLE	
		(0)	(1)	(2)	
29	¿Depende de personas clave (incluido el apoyo de los contratistas) para operar los centros de cómputo ante una eventual interrupción del servicio? En caso afirmativo, ¿De qué manera puede gestionar esa dependencia?			X	No hay dependencia de personas clave. Existe esquema multidisciplinario en la administración de la plataforma entre los integrantes del equipo de Infraestructura (Contratistas y Funcionarios).

Soporte remoto.

https://anionline.sharepoint.com/:x:/r/Gestion%20VPRE/Sistemas/GD_TI/AuditoriasCI/_layouts/15/Doc.aspx?sourcedoc=%7B0B55D19B-118D-451B-AF61-2970610674F1%7D&file=Reporte_Casos_GLPI.xlsx&action=default&mobileredirect=true

Herramientas para soporte remoto.

https://anionline.sharepoint.com/Gestion%20VPRE/Sistemas/GD_TI/AuditoriasCI/Documentos%20compartidos/CIBERSEGURIDAD%20Y%20TELETRABAJO%202020/Evidencias%20Lista%20de%20Chequeo/Punto%2018/Herramientas_Soporte_Remoto.pdf

Administración de la plataforma.

GESTION INFRESTRUCTURA TECNOLOGICA ANI
Objetivo: Gestionar todos los elementos de la infraestructura Tecnológica ANI, relación de capacidades personal dedicado a la administración de servicios de Infraestructura de TI

	Funcionario	Contratista	Contratista	Contratista
INFRAESTRUCTURA TI	**1**[5]	**1**	**2**	**3**
Servicios de Nube				
Microsoft Azure (Maquinas Virtuales, App Service, Application Insights, Cuenta de almacenamiento, Equilibrador de carga,Grupo de seguridad de red)	X	X	X	X
Base de datos SQL Azure		X		X
Office 365(Sharepoint, Teams, Onedrive, correo, project, power apps, seguridad, cumplimiento)	X	X	X	X
Microsoft backup	X	X	X	X
Servicios Onpremise				
Servidores on premise	X	X	X	X
Plataforma antivirus Kaspersky	X	X	X	X
Almacenamiento SAN	X	X		X
Plataforma Fortinet	X	X		X
Elementos de intercambio de información vpn SharePoint ftp sftp	X	X	X	X
Canal de internet	X	X		X
switches	X	X		X
Aruba (Wifi)	X	X		X
Switch brocade	X	X		X

[5] Se reemplazan los nombres por números por protección de datos personales

Data center	X	X		X
Ups	X			X
Aire acondicionado	X	X	X	X
Cuartos técnicos p6 p7 p8	X	X		X

8.3.2. Suficiencia del recurso humano y del hardware

Relación del personal dedicado a soporte remoto detallando porcentaje de dedicación, temática principal atendida y número de casos atendidos en marzo y abril de 2020

Reporte Casos Atendidos Mesa de Servicio		
Técnico	**Grupo**	**Dedicación**
1[6]	Soporte Técnico Nivel 1	
2	Soporte Técnico Nivel 1	
3	Soporte Técnico Nivel 1	
4	Soporte Técnico Nivel 1	
5	Soporte Técnico Nivel 2	
6	Soporte Técnico Nivel 2	
7	Soporte Técnico Nivel 2	
1	Soporte Técnico Nivel 2	
8	Soporte Técnico Nivel 3	
9	Soporte Orfeo	
10	Soporte Orfeo	
11	Soporte Orfeo	
12	Soporte Portales Web	

[6] Se reemplazan los nombres por números por protección de datos personales

13	Soporte Aniscopio	
14	Soporte BPM	
15	Soporte Office 365	
16	Soporte ArcGis	

De igual manera se realizaron preguntas para determinar la suficiencia de los recursos de TI, mediante lista de chequeo remitida el 7 de mayo de 2020 por correo electrónico, para las cuales se obtuvieron las siguientes respuestas y soportes:

ITEM	DESCRIPTOR	CUMPLIMIENTO			OBSERVACIONES
		NO CUMPLE	CUMPLE PARCIALMENTE	CUMPLE	
		(0)	(1)	(2)	
6	¿Se cuenta con la infraestructura necesaria en hardware, software y seguridad de la información ante una eventual implementación de teletrabajo?			X	
27	¿Se han establecido prioridades en las tareas del equipo? ¿Hay tareas que se pueden postergar para liberar personal para la planificación de contingencias y el establecimiento de prioridades? ¿Es posible acceder a fondos de emergencia, en caso de que se deban adquirir equipos rápidamente o contar con			X	La programación de las tareas siempre se ha establecido en la definición de prioridades. Para la contingencia en sus primeras semanas nos enfocamos en apoyar a los usuarios en el uso de las herramientas tecnológicas con las que trabajaban a diario. Respecto a los fondos de emergencia, no es del alcance ni del

ITEM	DESCRIPTOR	CUMPLIMIENTO			OBSERVACIONES
		NO CUMPLE	CUMPLE PARCIALMENTE	CUMPLE	
		(0)	(1)	(2)	
	apoyo adicional de contratistas/especialistas?				resorte de la coordinación de Tecnología. No administramos el presupuesto.
28	¿Los datos de contacto de todos los colaboradores del GIT están actualizados? ¿Saben a quién contactar en caso de emergencia?			X	Si, tenemos el directorio. Adicionalmente contamos con los diferentes equipos creados en teams a través de la cual tenemos la comunicación oficial

Infraestructura necesaria.

https://anionline.sharepoint.com/:w:/r/Gestion%20VPRE/Sistemas/GD_TI/AuditoriasCI/Documentos%20compartidos/CIBERSEGURIDAD%20Y%20TELETRABAJO%202020/Evidencias%20Lista%20de%20Chequeo/Punto%206-2/RPT_MONITOREO_TI.docx?d=w244df773a8144b75a8171228413be496&csf=1&web=1&e=Fzf1HP

Priorización.

En respuesta el Grupo Interno de Trabajo de tecnologías de la Información y las Comunicaciones manifiesta que: "*La programación de las tareas siempre se ha establecido en la definición de prioridades. Para la contingencia en sus primeras semanas nos enfocamos en apoyar a los usuarios en el uso de las herramientas tecnológicas con las que trabajaban a diario. Respecto a los fondos de emergencia, no es del alcance ni del resorte de la coordinación de Tecnología. No administramos el presupuesto*".

Contactos del equipo.

https://anionline.sharepoint.com/:x:/r/Gestion%20VPRE/Sistemas/GD_TI/AuditoriasCI/Documentos%20compartidos/CIBERSEGURIDAD%20Y%20TELETRABAJO%202020/Evidencias%20Lista%20de%20Chequeo/Punto%2028/Contactos%20Personal%20T.I%20.xlsx?d=wfc71f6687fe641559e97c3d3803186b1&csf=1&web=1&e=Zdyl3G

8.3.3. Verificación de la cobertura de antivirus y firewall

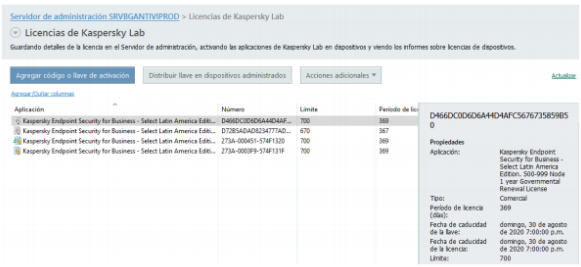
se realizaron preguntas para determinar la cobertura de las herramientas de protección antivirus y cortafuegos, mediante lista de chequeo remitida el 7 de mayo de 2020 por correo electrónico, para las cuales se obtuvieron las siguientes respuestas y soportes:

ITEM	DESCRIPTOR	CUMPLIMIENTO			OBSERVACIONES
		NO CUMPLE	CUMPLE PARCIALMENTE	CUMPLE	
		(0)	(1)	(2)	
19	¿Cuenta la Entidad con Antivirus vigente y su fecha de expiración de la licencia?			X	Karspesky - Vigente hasta 31/08/ 2020
20	¿Cuenta la Entidad con Firewall vigente y su fecha de expiración?			X	Fortigete 600 E - Fortinet - Vigente hasta 19 /10 / 2020

Antivirus.

En el año 2019 se adquirió y renovó la solución de Software de antivirus, dentro del proceso de contratación se adquirió:

Kaspersky Endpoint Security For Business Select, con un total de 700 licencias hasta 30 Agosto 2020.



Firewall.

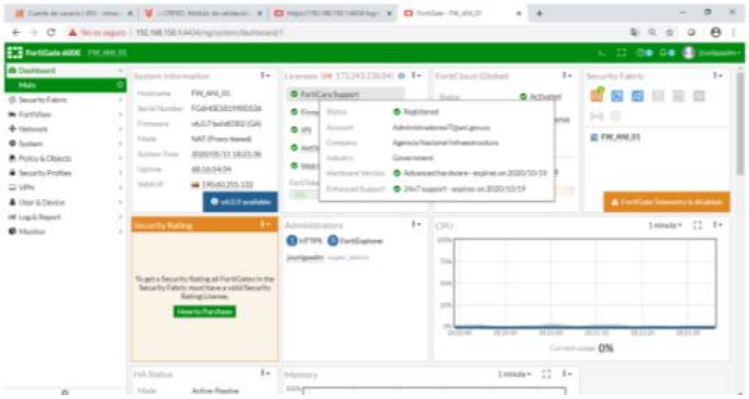
FortiCare Support 24X7 hasta el 19 de octubre de 2020

Firmware General updates hasta el 19 de octubre de 2020

IPS hasta el 19 de octubre de 2020

Antivirus hasta el 19 de octubre de 2020

Web Filtering hasta el 19 de octubre de 2020



8.3.4. Identificación de necesidades a partir del confinamiento y el trabajo remoto

Mediante correo electrónico de fecha 4 de mayo de 2020 se solicitó al Grupo Interno de Trabajo Tecnologías de la Información y las Telecomunicaciones, la información necesaria que permitiera evidenciar si han identificado nuevas necesidades.

Si han identificado necesidades (personal, hardware, software, seguridad u otras) a partir de la masificación del trabajo en casa, remita la relación y justificación.

El Grupo Interno de Trabajo de Tecnologías de la Información y las Telecomunicaciones remite la siguiente respuesta:

"Para la implementación de condiciones y nuevos esquemas como apoyo al trabajo remoto durante la actual contingencia, esta coordinación no ha identificado necesidad de contar con recursos adicionales. Las cargas de trabajo a nivel de personal y recurso técnico profesional están equilibradas y con buenos niveles de atención tanto a incidentes como a requerimientos de T.I. La plataforma tecnológica en cuanto a su capacidad y rendimiento no requiere, de acuerdo con el monitoreo realizado hasta el momento, ninguna ampliación por deficiencia en el rendimiento. Lo anterior aplica también para las plataformas y herramientas de software operativo o aplicativo.

Durante esta contingencia se han habilitado múltiples conexiones remotas tipo VPN SSL y se han publicado servicios que estaban de acceso local, para que sean accedidos de forma segura desde internet, para lo cual fue necesario la instalación y configuración del Certificados Digitales SSL en cada uno de los site. Los servicios publicados fueron: INTRANET https://intranet.ani.gov.co, UNIANI https://uniani.ani.gov.co y MESA DE SERVICIO https://mesadeservicio.ani.gov.co"

Análisis

Se revisan los documentos allegados como soporte de cada uno de los aspectos, evidenciando el buen comportamiento de la infraestructura de TI.

Conclusión

Se destaca como fortaleza el completo y oportuno trabajo realizado por el Grupo Interno de Trabajo de Tecnologías de la Información y las Comunicaciones, dado que se han planeado, implementado y monitoreado permanentemente los recursos y se evidencia una excelente distribución de los recursos con eficiencia y eficacia.

Concepto del auditor:

CUMPLE CON FORTELEZA

9. CALIFICACIÓN DE LA AUDITORÍA Y CONCEPTO DEL AUDITOR

Una vez efectuada la auditoría es el momento de responder a los interrogantes planteados en el marco de referencia:

¿Se encuentra la Entidad preparada para operar bajo la modalidad de trabajo en casa o trabajo remoto?

¿La infraestructura de TI (hardware, software y seguridad de la información) con que cuenta la Entidad es suficiente y blinda la información ante ciber-ataques?

¿Se encuentran alineados los procesos y los responsables para asegurar la continuidad de la prestación del servicio de la Agencia?

La Entidad, con el liderazgo del Coordinador y al equipo que conforma el Grupo Interno de Trabajo de Tecnologías de la Información ha realizado un buen proceso de planeación, de implementación de acciones de mejora y de cobertura a las falencias que otrora tenía la Entidad, con lo cual responde positivamente y con fortalezas a estos interrogantes.

Por tanto, el proceso **CUMPLE**, en su mayoría con fortalezas, sin embargo, esta auditoría tiene recomendaciones que será necesario atender con el fin de producir la mejora continua de la infraestructura de TI frente a los riesgos de ciberseguridad y trabajo en casa por causa del aislamiento preventivo obligatorio y enfrentar, mejor aún, estas nuevas dinámicas de la organización por causa de la pandemia y su permanencia a largo plazo en nuestra sociedad.

10. FORTALEZAS Y RECOMENDACIONES

10.1. Fortalezas

Se destaca como fortaleza el completo y oportuno trabajo realizado por el Grupo Interno de Trabajo de Tecnologías de la Información y las Comunicaciones, dado que:

1. Se han planeado, implementado y cubierto los protocolos de seguridad necesarios para garantizar el blindaje de la red de la Entidad, el monitoreo permanente y el cubrimiento de las necesidades de la Entidad en materia de cifrado, autenticación y fortaleza en la política de contraseñas.

   Al garantizar la seguridad en el acceso y al cifrado de la información que viaja a través de las redes, se asegura el cumplimiento de los atributos de la información: disponibilidad, integridad, completitud y confiabilidad.

2. Se han planeado, implementado y monitoreado las conexiones remotas para garantizar el buen funcionamiento y el soporte permanente.

3. Se han planeado, implementado y realizado las copias de seguridad y probando la restauración de estos respaldos lo cual garantiza la recuperación de información clave ante eventuales interrupciones del servicio.

4. Se han identificado concienzudamente y gestionado los riesgos de ciberseguridad y como consecuencia de la situación actual han revisado la identificación de nuevos riesgos, lo que ha permitido el refinamiento en el tratamiento de los riesgos existentes. Lo anterior se ha manifestado en la no materialización de riesgos y en la efectiva gestión de la infraestructura de TI incluida la seguridad y disponibilidad de la información.

5. Se han planeado, implementado y monitoreado permanentemente los recursos y se evidencia una excelente distribución de los recursos con eficiencia y eficacia.

10.2. Recomendaciones

1. Desarrollar, bajo el liderazgo de la Vicepresidencia de Planeación, Riesgos y Entorno, articulando la participación decidida de todos los procesos, la construcción del Plan de Continuidad de Negocio, a partir del insumo, *Identificación de impactos ante interrupción de servicios tecnológicos,* elaborado por el Grupo Interno de Trabajo de Tecnologías de la Información y las Comunicaciones.

2. Continuar la elaboración mensual del reporte de funcionamiento de la Entidad, mediante la aplicación de indicadores que den cuenta de la continuidad de la Entidad ante la situación actual que motiva la modalidad de trabajo en casa o trabajo remoto.

3. Elaborar por parte del Grupo Interno de Trabajo de Tecnologías de la Información y las Comunicaciones un plan de contingencia específico de sus recursos (Tecnológicos, humanos, financieros, entre otros) para las eventuales problemáticas ocasionadas por la pandemia del COVID-19.

4. Se recomienda revisar temas actuales relacionados con aspectos de seguridad derivados del trabajo remoto y riesgos de ciberseguridad que puedan ser compartidos con los colaboradores de la Entidad a través de capacitaciones o foros virtuales, e-cards, banners, UniANI o a través de los medios dispuestos por la Entidad para tal fin.

Realizó verificación y elaboró informe:

Juan Diego Toro Bautista
Auditor Oficina de Control Interno

Revisó y aprobó informe:

Gloria Margoth Cabrera Rubio
Jefe de Oficina de Control Interno

(versión original firmada)