INFORME DE GESTION
PLAN INSTITUCIONAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION
2021

Presentación

La política de Gobierno Digital es uno de los pilares del Estado en el proceso de transformación y modernización de las entidades públicas. Dentro de los elementos base que permiten el desarrollo de dicha política se encuentra el de Seguridad y Privacidad, el cual busca preservar la confidencialidad, integridad y disponibilidad de los activos de información de las entidades del Estado, garantizando su buen uso y la privacidad de los datos, a través de un Modelo de Seguridad y Privacidad de la Información.

Debido a los múltiples riesgos y amenazas que en la actualidad atentan contra la seguridad de la información, la protección y la privacidad de los datos, se hace indispensable que la Dirección General de Sanidad Militar implemente, mantenga y optimice de manera continua un Sistema de Gestión de Seguridad de la Información.

Para realizar este modelo se requiere elaborar una serie de procesos, políticas y procedimientos que conllevan al cumplimiento de los lineamientos establecidos por el Ministerio de las Tecnologías de la Información y las Comunicaciones. Por esta razón es necesario elaborar un Plan de Seguridad y Privacidad de la Información, con el fin de establecer las actividades que se deben realizar para la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) y de esta manera evaluar el nivel de madurez de la Dirección General de Sanidad Militar en la planificación, implementación y verificación del modelo.

Despliegue Estratégico Plan de Desarrollo Institucional SSFM 2019 – 2022

El Plan Institucional de Seguridad y Privacidad de la Información, esta alineado y contribuye al logro de la misión, visión y demás elementos del direccionamiento estratégico de la Dirección General de Sanidad Militar, los cuales se estipulan en el Plan De Desarrollo Institucional vigente (2019-2022).

Se alinea con el Objetivo 3. Fortalecer el desarrollo, implementación e integración del sistema de información en los procesos de aseguramiento y la prestación de los Servicios de Salud; y con la Dimensión 3. Gestión con Valores para Resultados-Política de Seguridad Digital.

Actividades Plan Institucional de Seguridad y Privacidad de la Información 2021

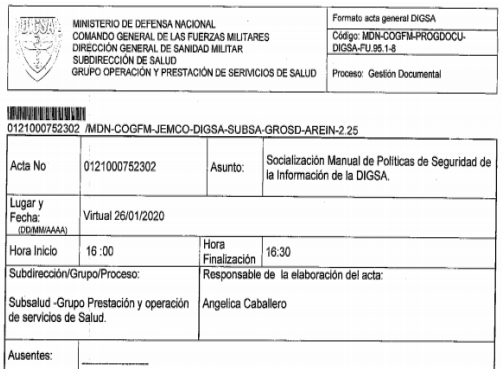
1. Actividad: Definir el modelo y esquema de gestión de políticas y directrices de la seguridad de la información. Plan Institucional de Seguridad y Privacidad de la Información DIGSA.

   Objetivo: Socializar el Manual con las políticas de seguridad y privacidad de la información al interior de la DIGSA.

   Evidencia Actividad:

   Actas de socialización del Manual de Políticas de Seguridad de la Información.

   Teniendo en cuenta el radicado No. 0120010337102 /MDN-COGFM-JEMCO-DIGSA-GSITIC-AREIN-95.6, a través del cual se socializo el Manual de Políticas de Seguridad de la Información de la DIGSA, se recibieron las actas de socialización de dicho manual, al interior de las diferentes grupos y áreas de la Dirección General de Sanidad Militar. A continuación, se muestran algunos encabezados de las mismas, así:



MINISTERIO DE DEFENSA NACIONAL
COMANDO GENERAL DE LAS FUERZAS MILITARES
DIRECCIÓN GENERAL DE SANIDAD MILITAR
SUBDIRECCIÓN DE SALUD
GRUPO OPERACIÓN Y PRESTACIÓN DE SERIVICIOS DE SALUD

Formato acta general DIGSA
Código: MDN-COGFM-PROGDOCU-DIGSA-FU.95.1-8
Proceso: Gestión Documental

0121000752302 /MDN-COGFM-JEMCO-DIGSA-SUBSA-GROSD-AREIN-2.25

Acta No	0121000752302	Asunto:	Socialización Manual de Políticas de Seguridad de la Información de la DIGSA.
Lugar y Fecha: (DD/MM/AAAA)	Virtual 26/01/2020		
Hora Inicio	16 :00	Hora Finalización	16:30
Subdirección/Grupo/Proceso: Subsalud -Grupo Prestación y operación de servicios de Salud.		Responsable de la elaboración del acta: Angelica Caballero	
Ausentes:			

MINISTERIO DE DEFENSA NACIONAL COMANDO GENERAL DE LAS FUERZAS MILITARES DIRECCIÓN GENERAL DE SANIDAD MILITAR	Formato acta general DIGSA Código: MDN-COGFM-PROGDOCU-DIGSA-FU.95.1 Proceso: Gestión Documental

MDN-COGFM-JEMCO-DIGSA-SUBTG-SISAM.

Acta No.	121001222102	Asunto:	Socialización del Manual de Políticas Seguridad de la Información de la DIGSA, personal del Grupo SISAM.
Lugar y Fecha:	Febrero 05 de 2021		
Hora Inicio	15:00 horas	Hora Finalización	16:00 horas
Subdirección/Grupo/Proceso: SUBTG-SISAM		Responsable de la elaboración del acta: Coordinación Grupo SISAM	
Ausentes:	Omitido.		

MINISTERIO DE DEFENSA NACIONAL
COMANDO GENERAL DE LAS FUERZAS MILITARES
DIRECCIÓN GENERAL DE SANIDAD MILITAR

/MDN-COGFM-JEMCO-DIGSA-GRS

Acta No.	0121001630302	Asunto:
Lugar y Fecha:	Febrero 12 de 2021	
Hora Inicio	16:00 horas	Hora Finaliza
Subdirección/Grupo/Proceso: DIGSA - GRSYE		Respon Lady G
Ausentes:	Omitido.	

MINISTERIO DE DEFENSA NACIONAL COMANDO GENERAL DE LAS FUERZAS MILITARES DIRECCIÓN GENERAL DE SANIDAD MILITAR SUBDIRECCIÓN DE SALUD GRUPO ASEGURAMIENTO EN SALUD	Formato acta general DIGSA Código: MDN-COGFM-JEMCO-DIGSA-SUBSA-GRUAS-ARPES.95.1-8 Proceso: Gestión Documental

0121001709502 / MDN-COGFM-JEMCO-DIGSA-SUBSA-GRUAS-ARPES -2.25

Acta No	0121001709502	Asunto:	Socialización Manual de Políticas de Seguridad de la Información de la DIGSA.
Lugar y Fecha: (DD/MM/AAAA)	Virtual 18/02/2020		
Hora Inicio	16 :00	Hora Finalización	16:30
Subdirección/Grupo/Proceso: Subdirección de salud -Grupo Aseguramiento en Salud.		Responsable de la elaboración del acta: Maria Paola Leguizamon Acevedo	
Ausentes:	----------		

Por otra parte, se programaron reuniones con las áreas trasversales para dar a conocer más al detalle las políticas que son de su responsabilidad y están descritas en el “Manual de Políticas de Seguridad de la Información de la Dirección General de Sanidad Militar”, las cuales son de mandatorio cumplimiento para todas las partes interesadas en la DIGSA, con el fin de garantizar la integridad, confiabilidad y disponibilidad de la información en la DIGSA.

A continuación, se muestran algunos encabezados de las actas elaboradas como evidencia de la actividad realizada con los grupos, así:

MINISTERIO DE DEFENSA NACIONAL COMANDO GENERAL DE LAS FUERZAS MILITARES DIRECCIÓN GENERAL DE SANIDAD MILITAR	Formato acta general DIGSA Código: MDN-COGFM-PROGDOCU-DIGSA-FU.95.1-8 Proceso: Gestión Documental

MDN-COGFM-JEMCO-DIGSA-SUBTG-SISAM-AREIN-95.6

Acta No.	0121000765702	Asunto:	Roles y responsabilidades asignados al Grupo de Talento Humano en el Manual de Políticas de Seguridad de la Información de la DIGSA
Lugar y Fecha:	Enero 28 de 2021		
Hora Inicio	14:15 horas	Hora Finalización	15:45 horas
Subdirección/Grupo/Proceso: SUBTG-SISAM-AREIN		Responsable de la elaboración del acta: Área Seguridad de la Información DIGSA	
Ausentes:	Omitido.		

MINISTERIO DE DEFENSA NACIONAL COMANDO GENERAL DE LAS FUERZAS MILITARES DIRECCIÓN GENERAL DE SANIDAD MILITAR	Formato acta general DIGSA Código: MDN-COGFM-PROGDOCU-DIGSA-FU.95.1-8 Proceso: Gestión Documental

MDN-COGFM-JEMCO-DIGSA-SUBTG-SISAM-AREIN-95.6

Acta No.	0121003248402	Asunto:	Roles y responsabilidades asignados al Grupo Sistema Integral de Información-Tecnologías de la Información y la Telecomunicaciones en el SGSI
Lugar y Fecha:	Marzo 17 de 2021		
Hora Inicio	08:30 horas	Hora Finalización	10:00 horas
Subdirección/Grupo/Proceso: SUBTG-SISAM-AREIN		Responsable de la elaboración del acta: Área Seguridad de la Información DIGSA	
Ausentes:	Omitido.		

2. Actividad: Continuar con la elaboración de los procedimientos de seguridad y privacidad de la información.
   Objetivo: Documentar modelo y el esquema de procedimientos de seguridad de la información.
   Evidencia Actividad: Procedimientos de seguridad de la información, debidamente documentados, socializados y aprobados.

   En cumplimiento a lo anterior, se elaboraron los procedimientos del Área de Seguridad de la Información que hacen parte del Proceso de Gestión de Tecnologías de la Información y las Comunicaciones, los cuales fueron revisados por parte del Grupo de Planeación Estratégica - Área de Sistemas Integrados de Gestión de la Dirección General de Sanidad Militar, se hicieron los ajustes requeridos y luego fueron codificados, impresos, firmados y enviados nuevamente al Grupo de Planeación Estratégica - Área de Sistemas Integrados de Gestión para ser publicados en la plataforma Suite Visión; así:

   - Procedimiento Gestión de Incidentes de Seguridad de la Información de la DIGSA, MDN-COGFM-PROGTIC-DIGSA-PT.95.1-9.

MINISTERIO DE DEFENSA NACIONAL
COMANDO GENERAL DE LAS FUERZAS MILITARES
DIRECCIÓN GENERAL DE SANIDAD MILITAR
SUBDIRECCIÓN TECNICA Y DE GESTION
GRUPO SISTEMA INTEGRAL DE INFORMACIÓN-TECNOLOGIAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

Procedimiento Gestión de Incidentes de Seguridad de la Información de la DIGSA
MDN-COGFM-PROGTIC-DIGSA-PT.95.1-9
Proceso Gestión de Tecnologías de la Información y las Comunicaciones

CONTROL DE CAMBIOS

Versión	Fecha de Aprobación	Descripción de los cambios
1	Diciembre 2020	Versión Inicial. Elaboración por primera vez del documento.

CONTROL DE APROBACIÓN

Aprobó:	CR. Luis Hernando Sandoval Pinzón Subdirector Técnico y de Gestión de DIGSA	
Revisó:	CS. Vivian Tatiana Alba Díaz Gestor de Calidad PROGTIC	CR. Carlos Dario González Villamil Coordinador Grupo Sistema Integral de Información – Tecnologías de la Información y la Comunicaciones DIGSA
	SMSM. Edna del Pilar Martínez Páez Grupo Planeación Estratégica DIGSA Líder Área Sistemas Integrados de Gestión ARSIG	PD. Alexandra Martínez Vargas Coordinadora Grupo Planeación Estratégica DIGSA Representante de la Dirección
Elaboró:	PD. Yolanda Quintero Agudelo Grupo Sistema Integral de Información – Tecnologías de la Información y la Comunicaciones DIGSA Área Seguridad de la Información DIGSA	PD. Diana Marcela López Bejarano Grupo Sistema Integral de Información – Tecnologías de la Información y la Comunicaciones DIGSA Área Seguridad de la Información DIGSA

   -

   - Procedimiento Gestión Políticas de Seguridad Información de la DIGSA, MDN-COGFM-PROGTIC-DIGSA-PT.95.1-10.

MINISTERIO DE DEFENSA NACIONAL
COMANDO GENERAL DE LAS FUERZAS MILITARES
DIRECCIÓN GENERAL DE SANIDAD MILITAR
SUBDIRECCIÓN TECNICA Y DE GESTION
GRUPO SISTEMA INTEGRAL DE INFORMACIÓN-TECNOLOGIAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

Procedimiento Gestión de Políticas de Seguridad de la Información de la DIGSA
MDN-COGFM-PROGTIC-DIGSA-PT.95.1-10
Proceso Gestión de Tecnologías de la Información y las Comunicaciones

CONTROL DE CAMBIOS

Versión	Fecha de Aprobación	Descripción de los cambios
1	Diciembre 2020	Versión Inicial. Elaboración por primera vez del documento.

CONTROL DE APROBACIÓN

Aprobó:	CR. Luis Hernando Sandoval Pinzón Subdirector Técnico y de Gestión de DIGSA	
Revisó:	CS. Vivian Tatiana Alba Díaz Gestor de Calidad PROGTIC	CR. Carlos Dario González Villamil Coordinador Grupo Sistema Integral de Información – Tecnologías de la Información y la Comunicaciones DIGSA
	SMSM. Edna del Pilar Martínez Páez Grupo Planeación Estratégica DIGSA Líder Área Sistemas Integrados de Gestión ARSIG	PD. Alexandra Martínez Vargas Coordinadora Grupo Planeación Estratégica DIGSA Representante de la Dirección
Elaboró:	PD. Yolanda Quintero Agudelo Grupo Sistema Integral de Información – Tecnologías de la Información y la Comunicaciones DIGSA Área Seguridad de la Información DIGSA	PD. Diana Marcela López Bejarano Grupo Sistema Integral de Información – Tecnologías de la Información y la Comunicaciones DIGSA Área Seguridad de la Información DIGSA

   - Procedimiento Gestión Activos Información de la DIGSA, MDN-COGFM-PROGTIC-DIGSA-PT.95.1

MINISTERIO DE DEFENSA NACIONAL
COMANDO GENERAL DE LAS FUERZAS MILITARES
DIRECCIÓN GENERAL DE SANIDAD MILITAR
SUBDIRECCIÓN TECNICA Y DE GESTION
GRUPO SISTEMA INTEGRAL DE INFORMACIÓN-TECNOLOGIAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

Procedimiento de Gestión de Activos de Información de la DIGSA
MDN-COGFM-PROGTIC-DIGSA-PT.95.1-11
Proceso Gestión de Tecnologías de la Información y las Comunicaciones

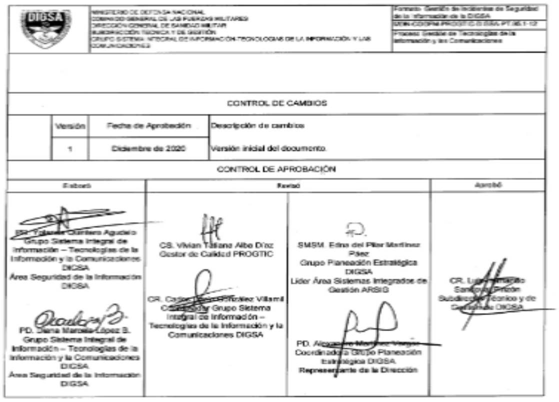
CONTROL DE CAMBIOS

Versión	Fecha de Aprobación	Descripción de los cambios
1	Diciembre 2020	Versión Inicial. Elaboración por primera vez del documento.

CONTROL DE APROBACIÓN

Aprobó:	CR. Luis Hernando Sandoval Pinzón Subdirector Técnico y de Gestión de DIGSA	
Revisó:	CS. Vivian Tatiana Alba Díaz Gestor de Calidad PROGTIC	CR. Carlos Dario González Villamil Coordinador Grupo Sistema Integral de Información – Tecnologías de la Información y la Comunicaciones DIGSA
	SMSM. Edna del Pilar Martínez Páez Grupo Planeación Estratégica DIGSA Líder Área Sistemas Integrados de Gestión ARSIG	PD. Alexandra Martínez Vargas Coordinadora Grupo Planeación Estratégica DIGSA Representante de la Dirección
Elaboró:	PD. Yolanda Quintero Agudelo Grupo Sistema Integral de Información – Tecnologías de la Información y la Comunicaciones DIGSA Área Seguridad de la Información DIGSA	PD. Diana Marcela López Bejarano Grupo Sistema Integral de Información – Tecnologías de la Información y la Comunicaciones DIGSA Área Seguridad de la Información DIGSA

   - Formato Gestión de Incidentes de Seguridad de la Información de la DIGSA, MDN-COGFM-PROGTIC-DIGSA-PT.95.1-12.



DIGSA	MINISTERIO DE DEFENSA NACIONAL COMANDO GENERAL DE LAS FUERZAS MILITARES DIRECCIÓN GENERAL DE SANIDAD MILITAR SUBDIRECCIÓN TECNICA Y DE GESTIÓN GRUPO SISTEMA INTEGRAL DE INFORMACIÓN-TECNOLOGIAS DE LA INFORMACIÓN Y LAS COMUNICACIONES	Formato: Gestión de Incidentes de Seguridad de la Información de la DIGSA MDN-COGFM-PROGTIC-DIGSA-PT-[illegible] Proceso: Gestión de Tecnologías de la Información y las Comunicaciones

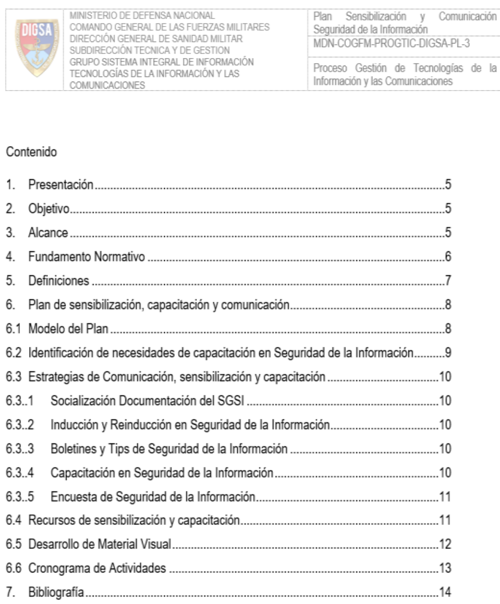
CONTROL DE CAMBIOS

Versión	Fecha de Aprobación	Descripción de cambios
1	Diciembre de 2020	Versión inicial del documento.

CONTROL DE APROBACIÓN

Elaboró	Revisó		Aprobó
[illegible] Quintero Agudelo Grupo Sistema Integral de Información – Tecnologías de la Información y la Comunicaciones DIGSA Área Seguridad de la Información DIGSA PD. [illegible] López B. Grupo Sistema Integral de Información – Tecnologías de la Información y la Comunicaciones DIGSA Área Seguridad de la Información DIGSA	CS. Vivian Tatiana Albo Díaz Gestor de Calidad PROGTIC CR. [illegible] Villamil [illegible] Grupo Sistema Integral de Información – Tecnologías de la Información y la Comunicaciones DIGSA	SMSM. Edna del Pilar Martínez Páez Grupo Planeación Estratégica DIGSA Líder Área Sistemas Integrados de Gestión ARSIG PD. [illegible] Coordinadora Grupo Planeación Estratégica DIGSA Representante de la Dirección	CR. [illegible] Subdirector Técnico y de Gestión DIGSA

El Plan de Sensibilización y Comunicación Seguridad de la Información, es un documento controlado en el Sistema Integrado de Gestión con el código MDN-COGFM-PROGTIC-DIGSA-PL-3.



DIGSA	MINISTERIO DE DEFENSA NACIONAL COMANDO GENERAL DE LAS FUERZAS MILITARES DIRECCIÓN GENERAL DE SANIDAD MILITAR SUBDIRECCIÓN TECNICA Y DE GESTION GRUPO SISTEMA INTEGRAL DE INFORMACIÓN TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES	Plan Sensibilización y Comunicación Seguridad de la Información MDN-COGFM-PROGTIC-DIGSA-PL-3 Proceso Gestión de Tecnologías de la Información y las Comunicaciones

Contenido

3. Actividad: Realizar sensibilización y comunicación en seguridad y privacidad de la información.
   Objetivo: Generar cultura de seguridad y privacidad de la información al interior de la DIGSA.
   Evidencia Actividad: Plan de Sensibilización y Comunicación de Seguridad de la Información.

   Se elaboró el Plan de Sensibilización y Comunicación en Seguridad de la Información para la Dirección General de Sanidad Militar para la vigencia 2021, el cual define las estrategias que conducen a la preservación de la confidencialidad, integridad, y disponibilidad de sus activos de información, por medio de la sensibilización capacitación y comunicación de las reglas de comportamiento adecuadas para el uso de los sistemas y de los activos de la información de la DIGSA.

   Este plan se establece como una herramienta que permite determinar los pasos a seguir y la periodicidad, para realizar actividades de comunicación, sensibilización y capacitación de seguridad de la información en la DIGSA, y aplica para todos funcionarios vinculados a la Dirección General de Sanidad Militar (personal militar, planta y prestación de servicios).

4. Actividad: Coordinar con el CCOCI, las pruebas de seguridad, el monitoreo, análisis y gestión de incidentes de los servicios de Seguridad de la Información.

   Objetivo: Gestionar de forma oportuna y eficiente los informes emitidos por el CCOCI, para evitar afectaciones en los sistemas informáticos.

   Evidencia Actividad: Informes de pruebas e incidentes cibernéticos reportados por el CCOCI.

   Con el fin de garantizar la continuidad del apoyo brindado por el Comando conjunto Cibernético a la Dirección General de Sanidad Militar, mediante oficio No.13514/MDN-COGFM-JEMCO-DIGSA-SUBTG-SISAM-AREIN-95.6, de fecha 25 de noviembre de 2020, se solicitó al Señor General Jefe de Estado Mayor Conjunto de las Fuerzas Militares, su apoyo y colaboración en el sentido de autorizar al Comando Conjunto Cibernético, continuar con el apoyo que nos han venido brindando en lo referente a la Gestión de Incidentes (servicios de monitoreo continuo que consiste recolectar los logs de los dispositivos de seguridad de la información con los que cuenta el Sistema SALUD.SIS que se encuentra en productivo, los cuales están siendo enviados al Centro de Operaciones de Seguridad (SOC) del Comando Conjunto Cibernético - CCOCI); así como la realización de las pruebas periódicas de seguridad de tipo Web Application Penetration Testing – WAPT y de Hacking Ético – HE, las cuales se ejecutan en conformidad con la Ley 1273 de 2009 y según cronograma acordado entre las partes.

   Mediante oficio No.13500/MDN-COGFM-JEMCO-DIGSA-SUBTG-SISAM-AREIN-95.6, de fecha 25 de noviembre de 2020, se solicitó al señor Representante Legal de la Unión Temporal DATAINFO, su apoyo y colaboración con la información técnica relacionada a continuación, para la ejecución de las pruebas de seguridad (lógica tipo Hacking Ético - HE y tipo Web Application Penetration Testing - WAPT), la cual será realizada por la Dirección General de Sanidad Militar – Comando Conjunto Cibernético, en conformidad con la Ley 1273 de 2009, así:

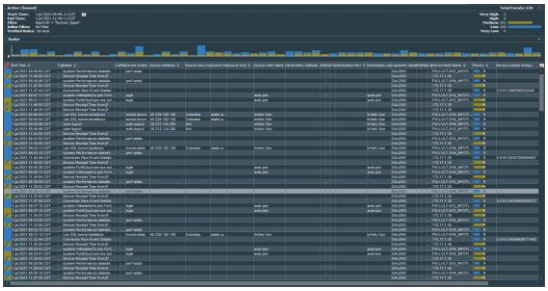
   - Diagrama de Red.
   - Direcciones IP (públicas y privadas).
   - URL de las páginas WEB.
   - Puertos, Servidores, Sistemas Operativos
   - Host-name de los servidores
   - Procesos automáticos
   - Las versiones de los sistemas Operativos
   - Las versiones de las Bases de Datos
   - Las versiones de los softwares utilizados en la capa de aplicación.

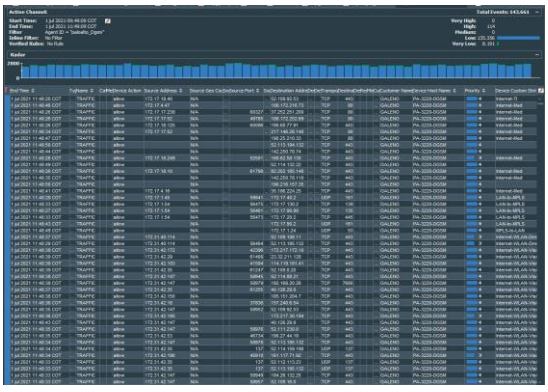
   Mediante oficio No.13502/MDN-COGFM-JEMCO-DIGSA-SUBTG-SISAM-AREIN-95.6, de fecha 25 de noviembre de 2020, se solicitó al señor Representante Legal de la Unión Temporal DATAINFO, la autorización para la realización de las pruebas de seguridad (lógica tipo Hacking Ético - HE y tipo Web Application Penetration Testing - WAPT) al sistema en productivo SALUD.SIS, en conformidad con la Ley 1273 de 2009 y de acuerdo a lo pactado dentro del Contrato No.102/DIGSA-2020.

   Con radicado No.0121005432902/MDN-COGFM-JEMCO-SEMOC-CCOCI-CIBC2-38.10, de fecha 28 de Mayo de 2021, se recibió el Informe Técnico de Análisis Vulnerabilidades 05262021 CCOCI-SALUDSIS-INF-TEC, de las pruebas de seguridad realizadas a la plataforma

tecnológica y a nivel aplicación del Sistema SALUD.SIS que se encuentra en productivo; en apoyo a lo solicitado mediante radicado No.0121000565502/MDN-COGFM-JEMCO-DIGSA-SUBTG-SISAM-AREIN-95.6.

Las siguientes imagenes muestran el monitoreo en tiempo real realizado a los logs generados del sistema SALUD.SIS en productivo y los de DIGSA a nivel central, los cuales son analizados las 24 horas del día por parte del personal técnico del Centro de Operaciones de Seguridad - SOC del Comando Conjunto Cibernético-CCOCI.





De igual forma, se dan a conocer los Boletines de ALERTAS Y ADVERTENCIAS de vulnerabilidades emitidos por el CSIRT Gobierno, colCERT y CCOCI como los relacionados a continuación a los terceros, para su conocimiento y gestión si es el caso, con miras a contribuir a salvaguardar la información de la Entidad, así:

De otra parte, mediante radicado No.0121004125702/MDN-COGFM-JEMCO-DIGSA-SUBTG-SISAM-AREIN-95.6 de fecha 22 de Abril de 2021 y No.0121005324102/MDN-COGFM-JEMCO-DIGSA-SUBTG-SISAM-AREIN-95.6 de fecha 26 de Mayo de 2021, se solicitó a la Jefatura de Estado Mayor Conjunto de las FFMM, el apoyo y colaboración en el sentido de autorizar al Comando Conjunto Cibernético, la realización de unas pruebas periódicas de seguridad de tipo Web Application Penetration Testing – WAPT y de tipo Hacking Ético – HE, a la infraestructura tecnológica que soporta la operación de la Dirección General de Sanidad Militar a nivel central, las cuales se ejecutan en conformidad con la Ley 1273 de 2009 y según cronograma acordado entre las partes (CCOCI-DIGSA).

El día 09 de junio de 2021, se recibió el radicado 0121005538002/MDN-COGFM-JEMCO-SEMOC-CCPCO-CIBC2-38.10, se confirmó con el Señor Capitán Robinson Zapata del CCOCI, la reunión programada con asunto: “Prueba de vulnerabilidades a infraestructura central DIGSA”, por la plataforma teams para el día Vie 11/06/2021, a las 11:00 a 12:00, a través del siguiente link: Haga clic aquí para unirse a la reunión.

Teniendo en cuenta el radicado 0121005538002/MDN-COGFM-JEMCO-SEMOC-CCPCO-CIBC2-38.10, y la reunión programada con asunto: “Prueba de vulnerabilidades a infraestructura central DIGSA”, por la plataforma teams, el día Vie 11/06/2021, a las 11:00 a 12:00, a través del siguiente link: Haga clic aquí para unirse a la reunión; con el liderazgo del Señor Capitán Robinson Zapata del CCOCI y personal de ingenieros de las áreas de Infraestructura tecnológica y seguridad del Grupo SISAM, se concretó la realización de la pruebas de seguridad a nivel central para el mes de agosto de 2021.

5. Actividad: Elaborar la declaración de aplicabilidad – SOA con el fin de determinar los controles del Anexo A de la norma ISO 27001 y las razones para su aplicación y/o exclusión.

   Objetivo: Establecer los controles que se deben implementar para mantener la información segura, disponible y confiable.

   Evidencia Actividad: Documento con la Declaración de aplicabilidad del Sistema de Gestión de Seguridad de la Información.

   Se elaboro la Declaración de Aplicabilidad en cumplimiento a la implementación del Sistema de Gestión de Seguridad de la Información, tomando como lineamiento lo establecido en la norma ISO 27001-Anexo A; la cual permite establecer los controles de seguridad de la información que se deben implementar en la DIGSA, para mantener la información segura, disponible y confiable.

   En dicho documento, se indica si cada uno de los controles de seguridad de la información es de aplicación o no, especificando si se cumple a través de una política, procedimiento, regla u otro tipo de control.

La Declaración de Aplicabilidad (SoA), permite la trazabilidad entre los controles de la norma ISO 27001 y lo que realmente se hace en la DIGSA, proporcionando así una visión amplia de lo que está realizando la entidad para proteger su información, y contribuyendo a la identificación, organización y registro de las medidas de seguridad implantadas.

Por otra parte, permite justificar la inclusión o exclusión de cada control del Anexo A de la norma ISO 27001.

Al documentar cada control aplicable e indicar si se ha implementado o no, se convierte en la guía principal para auditores tanto internos como externos. En general, el auditor accederá a la declaración de Aplicabilidad, y en base a ella desarrollará la auditoría y verificará el cumplimiento de lo documentado.

A continuación, se muestran algunos de los controles de la norma ISO 27001, especificados en la Declaración de aplicabilidad del Sistema de Gestión de Seguridad de la Información de la DIGSA, así: