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 Darío 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

1. Presentación

Este procedimiento surge de la necesidad de ajustar las políticas y lineamientos referentes a la gestión de incidentes de seguridad de la información, como parte integral del Sistema de Gestión de Seguridad de la Información, enmarcados dentro del Modelo de Seguridad y Privacidad de la Información - MSPI.

2. Objetivo

Definir las responsabilidades y actividades a realizar en la Dirección General de Sanidad Militar-DIGSA para la adecuada gestión de los posibles incidentes de seguridad de la información, con el fin de dar el tratamiento oportuno al momento de la materialización de un evento y/o incidente, mitigando su probabilidad de ocurrencia y generando las respectivas lecciones aprendidas.

3. Alcance

Detección, registro, atención y clasificación de los incidentes y/o eventos de seguridad; junto con su análisis, investigación, contención y erradicación del mismo, estableciendo un plan de recuperación de aquellos eventos de interrupción que afecten la confidencialidad, integridad, disponibilidad de la información, así como la continuidad del negocio, con el apoyo del Comando Conjunto Cibernético - CCOCI.

4. Políticas de Operación

<table>
<tr>
<td>Información :</td>
<td>4.1</td>
<td>La siguiente tabla describe la definición de los niveles en los que deberán ser clasificados los incidentes de seguridad que se puedan presentar en la DIGSA y su nivel de afectación en la confidencialidad, disponibilidad e integridad de la información en sus diferentes estados.

Niveles de clasificación de incidentes para la DIGSA.
<table>
<tr><th>NIVEL</th><th>RANGO</th><th>DESCRIPCIÓN</th><th>AFECTACIÓN PORCENTUAL DE LA OPERACIÓN</th></tr>
<tr><td></td><td></td><td>Este nivel de criticidad se da para aquellos incidentes o eventos que son detectados y/o notificados, porque en ellos, es posible establecer una amenaza sobre los activos de información capaz de impactar de manera considerable las características de integridad y/o confidencialidad y/o disponibilidad de los activos</td><td>80% A 100%</td></tr>
</table>
</td>
</tr>
</table>

		críticos de información de la DIGSA, afectando la continuidad del negocio en un porcentaje mayor al 80%.	
4	Mayor	Este nivel de criticidad se da para aquellos incidentes o eventos que sean reportados, debido a que pueden ser una amenaza sobre los activos de información capaz de impactar de manera considerable las características de integridad y/o confidencialidad y/o disponibilidad de los activos críticos de información de la DIGSA.	61% A 80%
3	Moderado	Este nivel de criticidad se da para aquellos incidentes o eventos que sean reportados como posibles amenazas, que pueden afectar los activos de información de la entidad, impactando de modo limitado sus características de integridad y/o confidencialidad y/o disponibilidad frente a un activo no crítico para la DIGSA.	41% A 60%
		Este nivel de criticidad se da para aquellos incidentes o eventos que sean reportados como posibles amenazas para los activos de información, es decir, que pueden impactar sus características de integridad y/o confidencialidad y/o disponibilidad, sin embargo, los controles de seguridad resultan efectivos anulando cualquier impacto para la DIGSA.	21% A 40%

		[redacted]	La materialización del incidente tiene efectos no significativos dentro de los procesos y la seguridad de la información de la DIGSA	0 A 20%

Fuente: Guía para la administración del riesgo - DAFP (matriz de riesgos para entidades públicas).

5. Definiciones

Control:	Cualquier acción o elemento del sistema de gestión cuyo propósito es el de prevenir la ocurrencia de un incidente o disminuir la severidad de las consecuencias.
Falla de Control:	Desviación detectada o no en el sistema de gestión de la seguridad de la información, que si no es corregida a tiempo causa o puede llegar a causar un incidente. Se presenta porque una regla, norma o estándar no existe, es inadecuada o no se cumple.
Herramienta Informática:	Conjunto de programas que permiten la manipulación de datos, para que el usuario obtenga la información necesaria, para la gestión de la seguridad de la información y fallas de control en tiempo real.
Incidente:	Evento o cadena de eventos no planeados, no deseados y todos previsibles que generaron (accidente) o que, bajo circunstancias ligeramente diferentes, pudieron haber generado: perdidas de información, daños, etc. Se presenta por la coincidencia en el tiempo y en el espacio de varias fallas de control.
Riesgo:	Producto de combinar la probabilidad de que un evento específico indeseado ocurra y la severidad de las consecuencias.
Ataque de fuerza bruta:	Es el método para averiguar una contraseña probando todas las combinaciones posibles hasta dar con la correcta. Los ataques por fuerza bruta son una de las técnicas más habituales de robo de contraseñas.
Alerta de seguridad:	Indicador, mensaje y/o reporte de una vulnerabilidad u ocurrencia de un incidente que afecte la confidencialidad, integridad, disponibilidad de la información o los servicios.
Oficial de Seguridad de la información:	Es la persona responsable de planear, coordinar y administrar los procesos de seguridad informática en una organización.

Políticas de Seguridad Informática:	Son las directrices de índole técnica y de organización que se llevan adelante respecto de un determinado sistema de computación a fin de proteger y resguardar su funcionamiento y la información en él contenida.
Seguridad:	Asegurar que los recursos del sistema de información (material informático o programas) o portales de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

6. Acrónimos

DIGSA:	Dirección General de Sanidad Militar.
CCOCI:	Comando Conjunto Cibernético
CGFM:	Comando General de las Fuerzas Miliares
FFMM:	Fuerzas Militares.
SISAM:	Grupo Sistema Integral de Información-Tecnologías de la Información y la Telecomunicaciones.
AREIN:	Área de Seguridad de la Información
ARECO:	Área de Infraestructura Tecnológica, Redes y Comunicaciones
ARIBD:	Área administración del Sistema y Base de Datos

7. Proveedor – entrada (insumo) para el desarrollo del procedimiento

Proveedor	Entrada - insumo
Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC).	Resolución 1652 del 2008, Artículo 5, donde se mencionan la correcta administración de dominios (usado para incidentes de seguridad).
Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC).	Guía No.21 para la Gestión y Clasificación de Incidentes de Seguridad de la Información.
Dirección General de Sanidad Militar	Funcionarios, contratistas y proveedores de DIGSA.
Dirección General de Sanidad Militar	Procedimiento Monitoreo Infraestructura Tecnología de la DIGSA.
Dirección General de Sanidad Militar	Procedimiento Gestión de Copias de Respaldo y Recuperación de la DIGSA.
Dirección General de Sanidad Militar	Procedimiento Gestión Activos Información de la DIGSA.

8. Descripción de Actividades y puntos de control

Descripción	Registro(s)
1. Reportar el incidente de seguridad de la Información al Grupo SISAM, por parte de autoridades, funcionarios, contratistas y proveedores de DIGSA. El reporte incluye alertas, causas y eventos presentados. Responsable: Autoridades (Operadores SOC del CCOCI), funcionarios, contratistas y proveedores de DIGSA. (Ver punto de control).	Reporte del incidente ya sea en medio escrito o digital – Formato de Gestion de Incidente de Seguridad de la información la DIGSA
2. Analizar la información reportada, con apoyo del Área de Infraestructura DIGSA. Si se define como un incidente de seguridad, se continua con la Actividad No. 3. Si no es un incidente de seguridad, se continua en la Actividad No. 13 para documentar la falsa alarma. Responsable: Grupo SISAM áreas (AREIN y ARECO) de la DIGSA.	Formato de Gestion de Incidente de Seguridad de la información la DIGSA
3. Realizar la evaluación del impacto del incidente de seguridad de acuerdo con la Tabla Nº 1. Criterios de evaluación del impacto del incidente de seguridad de la información o Niveles de clasificación de incidentes. Responsable: Grupo SISAM áreas (AREIN y ARECO) de la DIGSA.	N/A
4. Definir las acciones a realizar para gestionar el incidente de seguridad. Responsable: Grupo SISAM áreas (AREIN y ARECO) de la DIGSA.	Matriz de Gestión de Incidentes de Seguridad.
5. Aplicar las medidas correctivas. Responsable: Grupo SISAM áreas (AREIN y ARECO) de la DIGSA.	N/A
6. Verificar que las medidas correctivas se ejecutaron de manera correcta. Sí las medidas correctivas se ejecutan exitosamente, continuar con la Actividad No. 11. Sino continuar a la Actividad No. 7. Responsable: Grupo SISAM áreas (AREIN y ARECO) de la DIGSA.	Matriz de Gestión de Incidentes de Seguridad.
7. Escalar el incidente al Subdirector Técnico y de Gestión – Director o quien haga sus veces en la DIGSA.	Matriz de Gestión de Incidentes de Seguridad.

Descripción	Registro(s)
Responsable: Grupo SISAM áreas (AREIN y ARECO) de la DIGSA.	
8. Definir las acciones pertinentes para dar solución al incidente de seguridad de la información. Responsable: Coordinador Grupo SISAM, Subdirector Técnico y de Gestión – Director o quien haga sus veces en la DIGSA.	N/A
9. Ejecutar las acciones definidas por el Subdirector Técnico y de Gestión – Director o quien haga sus veces en la DIGSA. Responsable: Grupo SISAM áreas (AREIN y ARECO) de la DIGSA.	N/A
10. Verificar que las acciones establecidas por Subdirector Técnico y de Gestión – Director o quien haga sus veces en la DIGSA, se ejecutaron de manera correcta. Si las acciones fueron exitosas, continuar con la Actividad No. 11. Sino continuar con la Actividad No. 6. Responsable: Grupo SISAM áreas (AREIN y ARECO) de la DIGSA.	Matriz de Gestión de Incidentes de Seguridad.
11. Establecer medidas, controles o actividades para gestionar los riesgos que generaron el incidente de seguridad de la información. Responsable: Grupo SISAM áreas (AREIN y ARECO) de la DIGSA.	Matriz de Gestión de Incidentes de Seguridad.
12. Informar al Subdirector Técnico y de Gestión – Director o quien haga sus veces en la DIGSA. Responsable: Coordinador Grupo SISAM de la DIGSA.	N/A
13. Documentar el resultado de la acción realizada en la Matriz de Gestión de Incidentes de Seguridad. Responsable: Grupo SISAM áreas (AREIN y ARECO) de la DIGSA. (Ver punto de control).	Matriz de Gestión de Incidentes de Seguridad.
14. Comunicar a los interesados sobre las acciones realizadas para la gestión de incidentes. Responsable: Coordinador Grupo SISAM de la DIGSA.	Respuesta para los Interesados por correo electrónico o medio físico.
15. Evaluar trimestralmente (si se presentan incidentes), los incidentes de mayor impacto y/o recurrencia que se presenten, con el fin de definir acciones de mejora continua para eliminar o disminuir los riesgos en los servicios	Acta de reunión, si es el caso.

Descripción	Registro(s)
informáticos de DIGSA. Responsable: Coordinador Grupo SISAM, Subdirector Técnico y de Gestión – Director o quien haga sus veces en la DIGSA.	

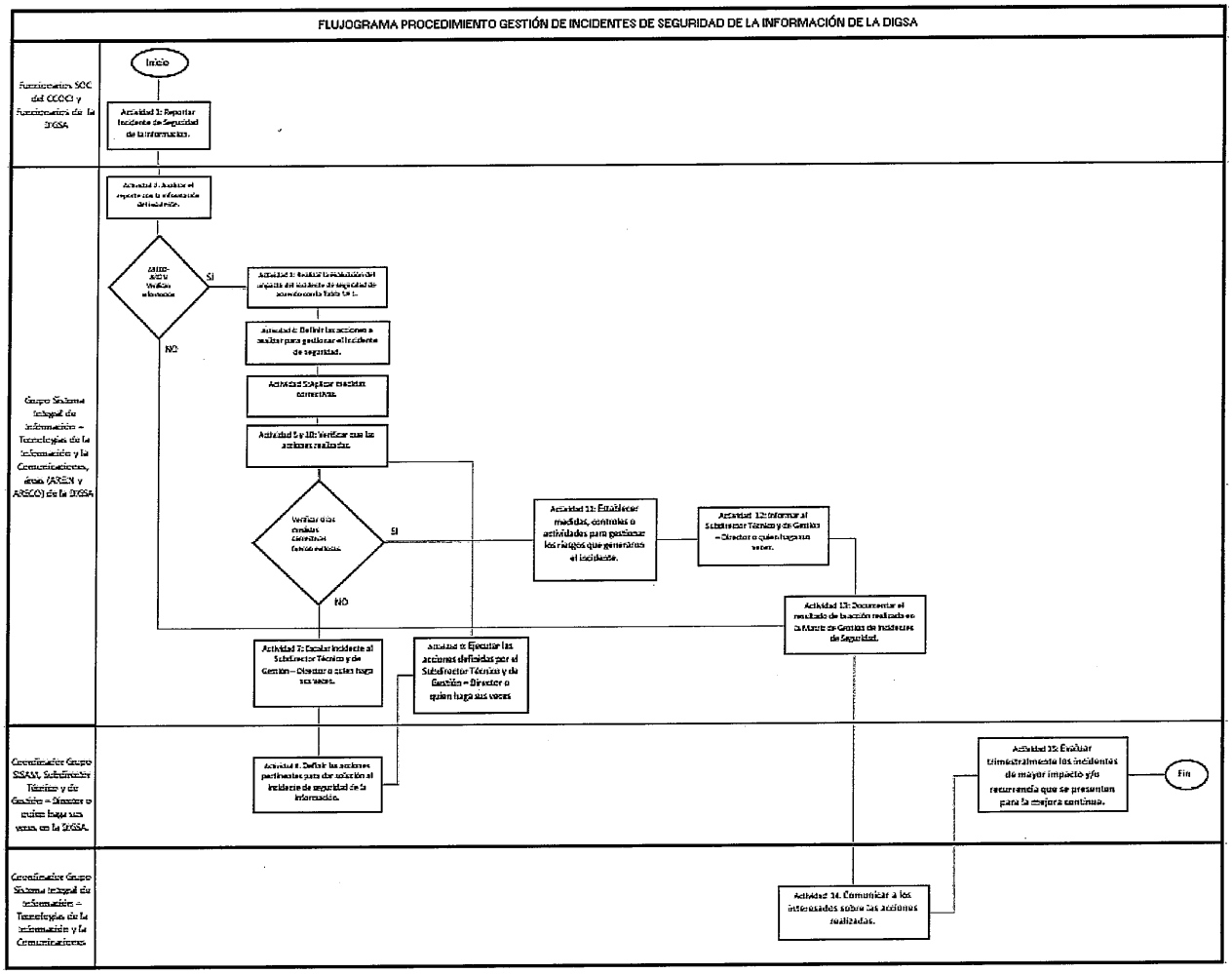
Puntos de control

Actividad donde se controla:	1. Reportar el incidente de seguridad de la Información al Grupo SISAM, por parte de autoridades, funcionarios, contratistas y proveedores de DIGSA. El reporte incluye alertas, causas y eventos presentados.
Como se controla:	Verificando que estén los registros o reportes de los incidentes de seguridad generado por parte de autoridades, funcionarios, contratistas y proveedores de DIGSA. El reporte incluye alertas, causas y eventos presentados para la DIGSA.
Criterio de aceptación	Si no están los registrados de los incidentes de seguridad de la información reportados al Grupo SISAM de la DIGSA.
Acción a tomar (si no cumple criterio de aceptación):	Devolver al responsable de hacer el registro por correo electrónico especificando las observaciones de incumplimiento.
Registro de la acción tomada:	Correo electrónico enviado.
Responsable del control:	Autoridades (Operadores SOC del CCOCI), funcionarios, contratistas y proveedores de DIGSA.

Puntos de control

Actividad donde se controla:	13. Documentar el resultado de la acción realizada en la Matriz de Gestión de Incidentes de Seguridad.
Como se controla:	Verificando la Matriz de Gestión de Incidentes de Seguridad.
Criterio de aceptación	Si no está documentada la acción realizada en la matriz de gestión de incidentes de seguridad de la información de la DIGSA.
Acción a tomar (si no cumple criterio de aceptación):	Devolver la matriz de Gestión de Incidentes de Seguridad al dueño del proceso por correo electrónico especificando observaciones de incumplimiento.
Registro de la acción tomada:	Correo electrónico enviado.
Responsable del control:	Grupo SISAM áreas (AREIN y ARECO) de la DIGSA.

9. Flujograma



10. Documentos y registros relacionados

10.1. Norma Técnica Colombiana NTC-ISO 27001:2013 Anexo A.16.
10.2. Política de Gestión de Incidentes de Seguridad de la Información.
10.3. NTC–ISO–IEC 27035- 2013 para la estrategia de Gobierno Digital.
10.4. Guía para la administración del riesgo – DAFP.
10.5. Formato de Gestion de Incidente de Seguridad de la información la DIGSA.