0. CONTROL DE CAMBIOS

Versión	Fecha de Aprobación	Responsable	Descripción de Cambios realizados
1	2018-09-12	Luis Albeiro Cortés Contratista Área de TIC	Actualización del mapa de procesos de la entidad, en LDM anterior corresponde al Código: 3AP-GTI-PD-03
2	2021-07-22	EDGAR ALFONSO CIPAGAUTA PEDRAZA	Se requiere ajuste debido a cambios en la normatividad

1. LIDER DE PROCESO: CARLOS ALFONSO GAITAN SANCHEZ

1.1 OBJETIVO DEL PROCEDIMIENTO: Establecer los lineamientos para el tratamiento y las medidas necesarias para gestionar posibles afectaciones a la seguridad delos datos logrando mitigar los riesgos y daños que se puedan causar a los activos de información del Idartes

1.2 ALCANCE DEL PROCEDIMIENTO: El procedimiento para gestión de incidentes de seguridad inicia desde la identificación de un incidente, detección, contención y solución, finalizando con la documentación pertinente, se establece las directrices para solicitud, atención, tratamiento y respuesta de incidentes que puedan afectar la seguridad de la información del Idartes.

1.3 RESPONSABLES DEL PROCEDIMIENTO: 120 OFICINA ASESORA DE PLANEACION Y TECNOLOGÍAS DE LA INFORMACIÓN - 122 ÁREA DE TECNOLOGÍA DE LA INFORMACIÓN

2. GLOSARIO:

ACTIVO DE INFORMACIÓN: Se denomina activo a aquello que tiene valor para la organización y por lo tanto debe protegerse

ADMINISTRADOR MESA DE AYUDA: Recibe la información de los usuarios, registra los casos en la herramienta de mesa de ayuda y es el primer contacto para la gestión de los incidentes de seguridad de la información.

ATAQUE INFORMATICO: Conjunto de actividades realizadas por atacantes para vulnerar la seguridad informática de un sistema.

ANS: Acuerdos de niveles de servicio

ANTIVIRUS: Programa diseñado para identificar, aislar o eliminar un virus del computador.

APLICACION VAULT: Herramienta que hace parte de la Suite de Google Apps para almacenamiento y consulta de copias de seguridad de cuentas de correo de licenciamiento Basic.

BACKUP: Copia de respaldo de la información realizada en medio magnético.

CATEGORIA: Se asigna una categoría (que puede estar a su vez subdividida en más niveles) dependiendo del tipo de incidente o del grupo de Trabajo responsable de su resolución. Se identifican los servicios afectados por el incidente.

HARDWARE: Componentes eléctricos, dípticos, electrónicos, electromecánicos y mecánicos que conforman un instrumento o sistema de computador.

INFORMACIÓN: Agrupación de datos con un significado especifico

SOFTWARE: Programas que se ejecutan en el computador para realizar una función determinada.

USUARIO: Servidor público que tiene a su cargo un computador y/o una cuenta de correo por medio de los cuales puede acceder a los recursos y servicios que ofrece una red.

USUARIO ADMINISTRADOR: Usuarios con privilegios para instalación y configuración de software y hardware en el equipo asignado que por sus deberes funcionales requieren este perfil.

ACTIVOS TECNOLÓGICOS: Recursos del sistema de información o relacionados con éste, necesarios para que la entidad funcione correctamente y alcance los objetivos propuestos por su Dirección. Se pueden estructurar en las siguientes categorías: Software, Hardware, Servicios, Datos, Personal, Proveedores, instalaciones físicas, Comunicaciones, Equipamiento auxiliar.

CONFIDENCIALIDAD: Garantía que la información sea accedida únicamente por usuarios y procesos autorizados.

CONTROL: Medida que permite garantizar la reducción del nivel de un riesgo específico o mantenerlo dentro de límites aceptables

DISPONIBILIDAD: Garantía que los usuarios y procesos autorizados tengan acceso a los activos de información cuando los requieran

EVENTO: Suceso que puede ocurrir en un espacio y tiempo específico, generando impactos sobre los activos tecnológicos y activos del negocio. Un evento de seguridad de la información es la presencia identificada de un estado del sistema, del proceso, del servicio o de los recursos tecnológicos que indican un incumplimiento posible de las políticas de seguridad de la información o de las políticas operacionales, una falla de las medidas de seguridad tomadas o una situación previamente desconocida que genera riesgos para la entidad

EVENTOS DE SEGURIDAD DE LA INFORMACIÓN: Resultado de intentos intencionales o accidentales de romper las medidas de seguridad de la información impactando en la confidencialidad, integridad y disponibilidad de los datos.

INFORMACIÓN: Es un conjunto organizado de datos, que constituyen un mensaje sobre un determinado ente o fenómeno. Indicación o evento llevado al conocimiento de una persona o de un grupo. Es posible crearla, mantenerla, conservarla y transmitirla.

IMPACTO: Daño producido a la organización por la materialización de un riesgo sobre los activos tecnológicos, visto como diferencia en las estimaciones de los estados de seguridad obtenidas antes y después del evento.

INTEGRIDAD: Condición de seguridad que garantiza que la información es actualizada, en todo su ciclo de vida, sólo por el personal y procedimientos autorizados

REGISTRO DE EVENTOS: En ingles Logs. Mecanismo mediante el cual se guarda en un archivo (generalmente de texto) toda la información correspondiente a las actividades o eventos de un determinado sistema, dispositivo o equipo.

RIESGO: Probabilidad o posibilidad de que una amenaza aprovechando la vulnerabilidad o vulnerabilidades de un sistema, equipo o cualquier otro tipo de activo, se concrete, causando daños, perjuicios o pérdidas a la organización propietaria del mismo

SEGURIDAD DE LA INFORMACIÓN: Actividad que regula la protección de los recursos tecnológicos de una entidad a través de políticas, normas, procedimientos y estándares

SISTEMA DE INFORMACIÓN: Conjunto de datos, aplicaciones y equipos que de manera conjunta proveen a la empresa la información necesaria para la ejecución de las tareas y la toma de decisiones de los niveles estratégico, táctico y operativo.

TRAZABILIDAD: Conjunto de medidas, acciones y procedimientos que permiten registrar, identificar y realizar seguimiento a los incidentes en cada producto desde su origen hasta su respuesta final.

3. CONDICIONES GENERALES:

Todos los incidentes de seguridad de la información deben estar registrados en la herramienta de gestión con la que cuenta el instituto.

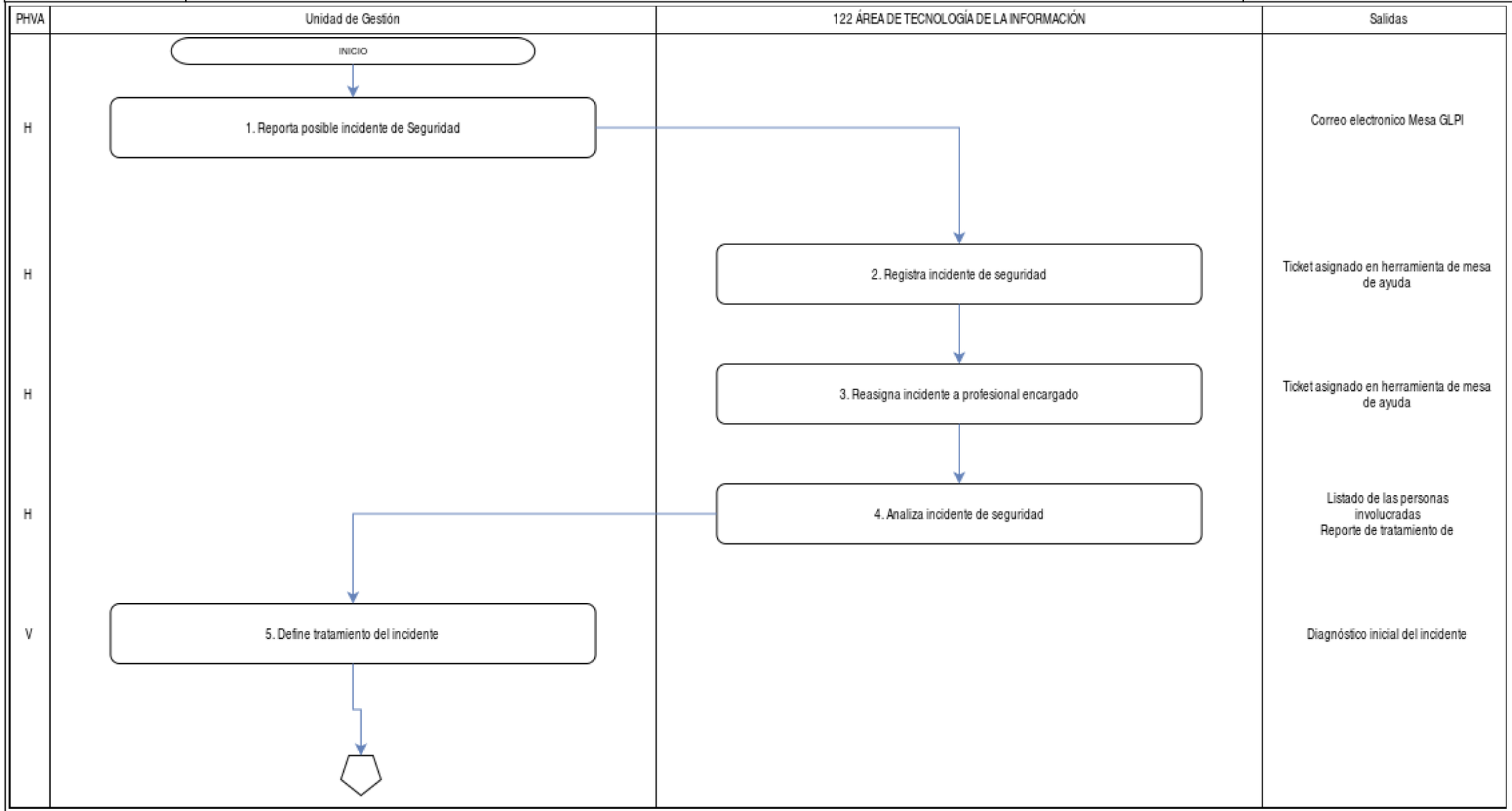
Es responsabilidad de todos los funcionarios, terceros y contratistas que tengan acceso a los activos de información del Idartes reportar a la mesa de ayuda, los eventos tecnológicos o incidentes de seguridad de la información para su respectivo trámite.

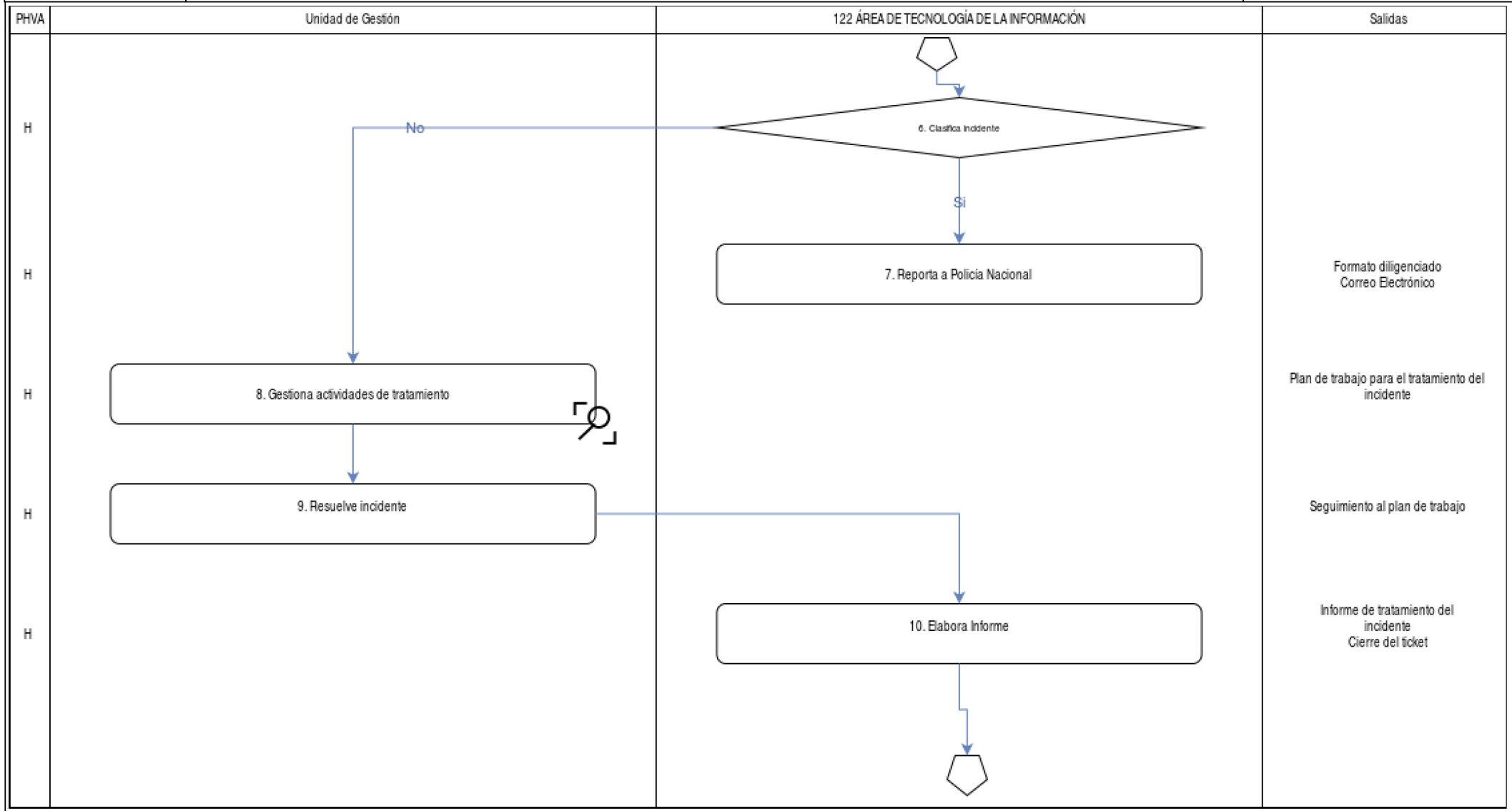
4. RELACIÓN CON OTROS PROCEDIMIENTOS Y PROCESOS: Esquema gráfico de la relación del procedimiento con otros procedimientos y/o procesos del IDARTES.

Procesos que se requieren como proveedor	Que insumos requiero del proveedor	Procedimiento	Que se obtiene del procedimiento	Para quien va dirigido el servicio o producto
• TODAS LAS ÁREAS	Reporte del incidente de seguridad en la información junto con su evidencia	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	Pasos para la solución del incidente de seguridad de la información	• TODAS LAS ÁREAS

5. ICONOGRAFÍA DEL DIAGRAMA DE FLUJO: Iconografía asociada al diagrama del flujo del procedimiento.

5.1 DIAGRAMA DE FLUJO: Secuencia lógica de las actividades establecidas en el procedimiento.


PHVA
Unidad de Gestión
122 ÁREA DE TECNOLOGÍA DE LA INFORMACIÓN
Salidas
INICIO
H
1. Reporta posible incidente de Seguridad
Correo electronico Mesa GLPI
H
2. Registra incidente de seguridad
Ticket asignado en herramienta de mesa de ayuda
H
3. Reasigna incidente a profesional encargado
Ticket asignado en herramienta de mesa de ayuda
H
4. Analiza incidente de seguridad
Listado de las personas involucradas
Reporte de tratamiento de
V
5. Define tratamiento del incidente
Diagnóstico inicial del incidente


PHVA
Unidad de Gestión
122 ÁREA DE TECNOLOGÍA DE LA INFORMACIÓN
Salidas
H
H
H
H
H
6. Clasifica Incidente
No
Si
7. Reporta a Policía Nacional
8. Gestiona actividades de tratamiento
9. Resuelve incidente
10. Elabora Informe
Formato diligenciado
Correo Electrónico
Plan de trabajo para el tratamiento del incidente
Seguimiento al plan de trabajo
Informe de tratamiento del incidente
Cierre del ticket

PHVA	Unidad de Gestión	122 ÁREA DE TECNOLOGÍA DE LA INFORMACIÓN	Salidas
A		11. Notifica solución al usuario FIN	Notificación por correo electrónico

5.2. DESCRIPCIÓN DE LAS ACTIVIDADES: Características específicas de las actividades del procedimiento.

No.	Ciclo PHVA	Ciclo de Gestión	Descripción del Ciclo de Gestión	Actores	Responsable	Tiempo (Horas)	Documento o Registro
1	H	Reporta posible incidente de Seguridad	Identifica el incidente de seguridad de la información y lo reporta a través del contacto telefónico o del chat - correo electrónico soportesistemas@idartes.gov.co	Unidad de Gestión	Unidad de Gestión	1 hora	Correo electronico Mesa GLPI
2	H	Registra incidente de seguridad	Realiza la creación del Ticket en la herramienta de mesa de ayuda de la entidad con la categorización y registro del posible incidente de seguridad.	122 ÁREA DE TECNOLOGÍA DE LA INFORMACIÓN	Administrador mesa de ayuda	1 hora	Ticket asignado en herramienta de mesa de ayuda
3	H	Reasigna incidente a profesional encargado	Realiza el escalamiento del incidente de seguridad al Profesional que apoya la gestión de incidentes de seguridad de la información para su análisis y clasificación. Ticket asignado en herramienta de mesa de ayuda	122 ÁREA DE TECNOLOGÍA DE LA INFORMACIÓN	Administrador mesa de ayuda	2 horas	Ticket asignado en herramienta de mesa de ayuda
4	H	Analiza incidente de seguridad	Analiza y clasifica el incidente de seguridad reportado de acuerdo con lo establecido en las políticas de operación	122 ÁREA DE TECNOLOGÍA DE LA INFORMACIÓN	Oficial de seguridad de la información	2 días	Listado de las personas involucradas Reporte de tratamiento de incidente
5	V	Define tratamiento del incidente	Realiza análisis pertinente con el fin de identificar la causa o causas que dieron origen al incidente de seguridad y determinar si se informa al Profesional de Gestión de Continuidad de la Operación.	Unidad de Gestión	Grupo para el tratamiento del incidente de seguridad	1 día	Diagnóstico inicial del incidente
6	H	Clasifica incidente	¿El incidente es un delito informático que requiere reporte a la Policía Nacional?	122 ÁREA DE TECNOLOGÍA DE LA INFORMACIÓN	Grupo para el tratamiento del incidente de seguridad	1 día	
7	H	Reporta a Policía Nacional	Diligencia formato de reporte de delito informático de la Policía Nacional - CSIRT (Ver formato en Mapa de Procesos - Otros)	122 ÁREA DE TECNOLOGÍA DE LA INFORMACIÓN	Oficial de seguridad de la información	1 día	Formato diligenciado Correo Electrónico
8	H	Gestiona actividades de tratamiento	Definir las actividades necesarias con el fin de erradicar la causa raíz detectada con la respectiva documentación de acciones realizadas para la solución del incidente.	Unidad de Gestión	Grupo para el tratamiento del incidente de seguridad	2 días	Plan de trabajo para el tratamiento del incidente
9	H	Resuelve incidente	Resuelve el incidente, teniendo en cuenta la categoría de seguridad de la información y del plan de trabajo establecido por el equipo	Unidad de Gestión	Grupo para el tratamiento del incidente de seguridad	5 días	Seguimiento al plan de trabajo
10	H	Elabora Informe	Elabora informe de gestión del incidente de seguridad, documenta la solución dada para el ticket generado por la mesa de ayuda y cierra el requerimiento	122 ÁREA DE TECNOLOGÍA DE LA INFORMACIÓN	Oficial de seguridad de la información	5 días	Informe de tratamiento del incidente Cierre del ticket
11	A	Notifica solución al usuario	Notifica a los afectados sobre el incidente de seguridad de a información que impacta la confidencialidad e integridad de su información, así como las medidas adoptadas para la solución	122 ÁREA DE TECNOLOGÍA DE LA INFORMACIÓN	Administrador de la mesa de ayuda	1 día	Notificación por correo electrónico

6. POLÍTICAS DE OPERACIÓN:

Los servidores públicos que administren o accedan a recursos deben reportar al área de sistemas cualquier evento o incidente de seguridad de la información.

Para la adquisición y preservación de la información que pueda servir como evidencia, se puede tomar como referencia los documentos internos y la ISO/IEC 27037 y las Guías de Evidencia Digital y la Gestión y Clasificación de Incidentes de Seguridad de la Información del MINTIC.

En caso de ser necesario se debe solicitar el apoyo de autoridades competentes (CSIRT-PONAL, CCOC: Comando Conjunto Cibernético, Grupo de Respuesta a Emergencias Cibernéticas de Colombia - colCERT, Fiscalía General de la nación) para realizar la recolección de evidencia.

La solicitud de apoyo a entes externos se realiza a través de los siguientes medios:

https://caivirtual.policia.gov.co/incidente-informatico

CAI Virtual de la Policía Nacional https://caivirtual.policia.gov.co/incidente-informatic, Centro Cibernético Policial de la Policía Nacional al teléfono 4266900 ext.104092, para recibir asesoría del caso en particular y posterior judicialización.

ColCERT Grupo de respuesta a emergencias cibernéticas de Colombia http://www.colcert.gov.co/?q=contenido/reportar-un-incidente, correos electrónicos: contacto@colcert.gov.co, malware@colcert.gov.co. o al Teléfono:(+571)2959897.

Verificar que se encuentre una orden por parte de las directivas de la entidad para poder proceder con la investigación dependiendo si el incidente requiere la intervención del proceso disciplinario o la información vulnerada es confidencial."

"De acuerdo con la categoría del incidente de seguridad de la información, se realiza el tratamiento del mismo teniendo en cuenta la gestión de conocimiento de incidentes que ya se hayan presentado o se puede tener en cuenta lo de acuerdo a lo establecido en el PLAN DE CONTINGENCIA EN TECNOLOGÍA DE LA INFORMACIÓN.

Si el Idartes no cuenta con los recursos necesarios y personal capacitado se debe recurrir a las entidades externas como CSIRT o Colcert.

El equipo de respuesta a incidentes de seguridad de información que realizó el tratamiento del incidente (El equipo encargado del tema de seguridad en la información) estará en continuo contacto a través del correo electrónico y seguimiento en el aplicativo de mesa de ayuda con el personal, unidades de gestión o procesos involucrados en el incidente."

7. POSIBLES PRODUCTOS O SERVICIOS NO CONFORME:

Actividad	Producto y/o Servicio	Criterio de Aceptación	Corrección	Registro
2. Registra incidente de seguridad: Realiza la creación del Ticket en la herramienta de mesa de ayuda de la entidad con la categorización y registro del posible incidente de seguridad.	Ticket asignado por la mesa de ayuda	Número consecutivo asignado por la herramienta GLPI para solución al incidente de seguridad reportado por el ticket usuario	registrar el incidente en el aplicativo GLPI para obtener el Ticket asignado al incidente	Ticket asignado por la mesa de ayuda dar
7. Reporta a Policía Nacional: Diligencia formato de reporte de delito informático de la Policía Nacional - CSIRT (Ver formato en Mapa de Procesos - Otros)	Formato de reporte de incidentes del CSIRT	Envío oficial del formato de reporte de incidentes del CSIRT	Tramitar el envío del formato establecido por la Policía Nacional mediando los canales establecidos por ellos	Correo electrónico- comunicación oficial externa
9. Resuelve incidente: Resuelve el incidente, teniendo en cuenta la categoría de seguridad de la información y del plan de trabajo establecido por el equipo	Plan de trabajo ejecutado	Ejecución del 100% de las actividades establecidas en el Plan de tratamiento del incidente de seguridad de la información	Revisar y ejecutar cada una de las actividades propuestas en el plan de tratamiento del incidente de seguridad de la información	Plan de trabajo
11. Notifica solución al usuario: Notifica a los afectados sobre el incidente de seguridad de a información que impacta la confidencialidad e integridad de su información, así como las medidas adoptadas para la solución	Soportes de solución de incidente	El reporte del cierre del incidente de seguridad de la información debe contener todos los documentos generados para la solución del incidente	Realizar el cargue de los documentos generados y enviados por el oficial de seguridad de la información en el aplicativo GLPI	Soportes de solución del incidente

8. DOCUMENTOS ASOCIADOS:

Los documentos asociados del presente procedimiento se pueden acceder a través del mapa de procesos

9. NORMATIVA ASOCIADA:

ACUERDO 57 DE 2002 “Por el cual se dictan disposiciones Generales para la implementación del Sistema Distrital de Información SDI, se organiza la Comisión Distrital de Sistemas”

DECRETO 3816 de 2003 “Por el cual se crea la Comisión Intersectorial de Políticas y de Gestión de la Información para la Administración Pública”

DIRECTIVA 5 de 2005 “Políticas Generales y directrices que orienten el desarrollo tecnológico”

DECRETO 619 de 2007 “Por el cual se establece la Estrategia de Gobierno Electrónico en el Distrito”

RESOLUCION 305 de 2008 “Por la cual se expiden políticas públicas para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, calidad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre”

LEY 1273 DE 2009 Congreso de la República 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

DECRETO 235 DE 2010 Ministerio del Interior y Justicia Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas.

CONPES 3701 DE 2011 Conpes Lineamientos de política para la Ciberseguridad y Ciberdefensa

LEY 1581 DE 2012 Congreso de la República Por el cual se dictan disposiciones generales para la protección de datos personales

DECRETO 2364 DE 2012 Ministerio del Interior y Justicia Por medio del cual se reglamenta el artículo 7 de la LEY 527 DE 1999, sobre la firma electrónica y se dictan otras disposiciones

DECRETO 19 DE 2012 Presidencia de Colombia Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública"

RESOLUCIÓN 396 DE 2012 Idartes Por medio de la cual se crea el Comité Técnico de Seguridad de la Información - CTSI- del Instituto Distrital de las Artes - IDARTES.

DECRETO 596 DE 2013 Alcaldía Mayor de Bogotá Por el cual se dictan medidas para la aplicación del Teletrabajo en organismos y entidades del Distrito Capital

LEY 1712 DE 2014 Congreso de la República Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones

RESOLUCIÓN 383 DE 2014 Idartes Por la cual se modifica la Resolución No 396 de 2012, "por medio de la cual se crea el Comité Técnico de Seguridad de la Información - CTSI- del Instituto Distrital de las Artes - IDARTES"

CONPES 3854 DE 2016 Conpes Política Nacional de Seguridad Digital. Lo que a su vez se traduce en una economía digital con cada vez más participantes en el país. Desafortunadamente, el incremento en la participación digital de los ciudadanos trae consigo nuevas y más sofisticadas formas para atentar contra su seguridad y la del Estado. Situación que debe ser atendida, tanto brindando protección en el ciberespacio para atender estas amenazas, como reduciendo la probabilidad de que estas sean efectivas, fortaleciendo las capacidades de los posibles afectados para identificar y gestionar este riesgo

RESOLUCIÓN 3436 DE 2017: Por la cual se reglamentan los requisitos técnicos, operativos y de seguridad que deberán cumplir las zonas de acceso a Internet inalámbrico de que trata el Capítulo 2, Título 9, Parte 2, Libro 2 del Decreto 1078 de 2015.

RESOLUCIÓN 4 DE 2017: Secretaría General Alcaldía Mayor de Bogotá D.C. - Comisión Distrital de Sistemas – CDS Por la cual se modifica la Resolución 305 de 2008 de la CDS

DECRETO 728 DE 2017: Ministerio de las Tecnologías de la Información y las Comunicaciones. Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto. Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de las zonas de acceso público a internet inalámbrico

DECRETO 1413 DE 2017: Ministerio de las Tecnologías de la Información y las Comunicaciones. En el Capítulo 2 Características de los Servicios Ciudadanos Digitales, Sección 1 Generalidades de los Servicios Ciudadanos Digitales

RESOLUCIÓN 2710 DE 2017: Ministerio de las Tecnologías de la Información y las Comunicaciones. Por la cual se establecen lineamientos para la adopción del protocolo IPv6

DECRETO 728 DE 2017: Ministerio de las Tecnologías de la Información y las Comunicaciones. Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto. Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno

CIRCULAR 30 DE 2017: Alta Consejería de Tics. Implementación CSIRT de Gobierno

CIRCULAR 36 DE 2017: Alta Consejería de Tics. Lineamientos de avance del modelo de seguridad y privacidad de la información

RESOLUCIÓN 3436 DE 2018: Ministerio de las Tecnologías de la Información y las Comunicaciones. Por la cual se reglamentan los requisitos técnicos, operativos y de seguridad que deberán cumplir las zonas de acceso a Internet inalámbrico de que trata el Capítulo 2, Título 9, Parte 2, Libro 2 del Decreto 1078 de 2015.

DECRETO 612 DE 2018: Departamento Administrativo de la Función Pública. Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.

DECRETO 1008 DE 2018: Ministerio de las Tecnologías de la Información y las Comunicaciones. 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

CIRCULAR 2 DE 2018: Ministerio de las Tecnologías de la Información y las Comunicaciones. Cumplimiento legal y normativo respecto a seguridad de la información.

CONPES 3920 DE 2018: Conpes Big Data, la política tiene por objetivo aumentar el aprovechamiento de datos, mediante el desarrollo de las condiciones para que sean gestionados como activos para generar valor social y económico. En lo que se refiere a las actividades de las entidades públicas, esta generación de valor es entendida como la provisión de bienes públicos para brindar respuestas efectivas y útiles frente a las necesidades sociales.

LEY 1955 DEL 2019: Presidencia de Colombia. Establece que las entidades del orden nacional deberán incluir en su plan de acción el componente de transformación digital, siguiendo los estándares que para tal efecto defina el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)

DECRETO 2106 DE 2019: Departamento Administrativo De La Función Pública. Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública Cap. II Transformación Digital Para Una Gestión Pública Efectiva

CONPES 3975 DE 2019: Conpes - Política Nacional de Transformación Digital e Inteligencia Artificial, estableció una acción a cargo de la Dirección de Gobierno Digital para desarrollar los lineamientos para que las entidades públicas del orden nacional elaboren sus planes de transformación digital con el fin de que puedan enfocar sus esfuerzos en este tema.

DECRETO 620 DE 2020: Departamento Administrativo De La Función Pública. Estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales

RESOLUCIÓN 0500 DE 2021. Ministerio De Tecnologías De La Información y las Comunicaciones. Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital

10. RECURSOS:

GLPI - Aplicativo mesa de ayuda

Oficial de Seguridad de la Información

Equipo transversal de solución de incidente de seguridad

EDGAR ALFONSO CIPAGAUTA PEDRAZA 2021-06-24 15:39:49	CARLOS ALFONSO GAITAN SANCHEZ 2021-07-22 11:52:58	AURORA CAMILA CRESPO MURILLO 2021-06-24 16:12:05	CARLOS ALFONSO GAITAN SANCHEZ 2021-07-22 11:58:26	

En el marco de los lineamientos del numeral 6.5 de la "Guía diseño de documentos del sistema integrado de gestión – SIG", se actualiza el código del presente documento para que se articule con la codificación vigente relacionada en la señalada guía y en el Listado Maestro de Documentos. El contenido del documento no cambia.