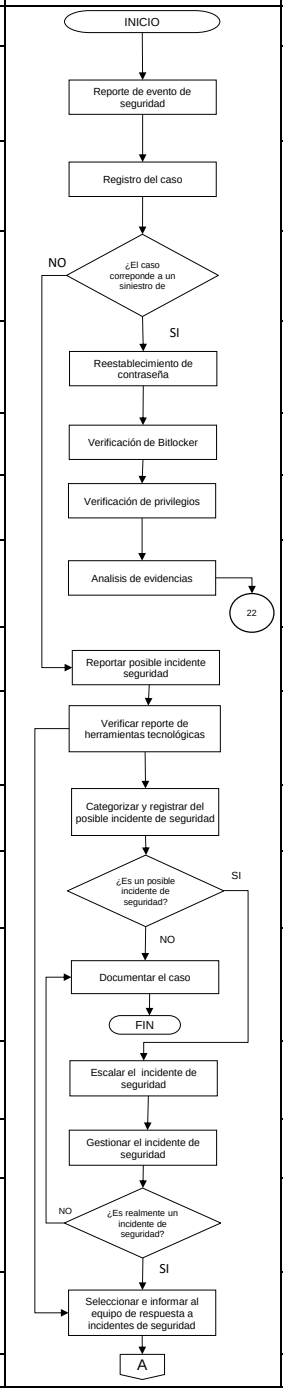
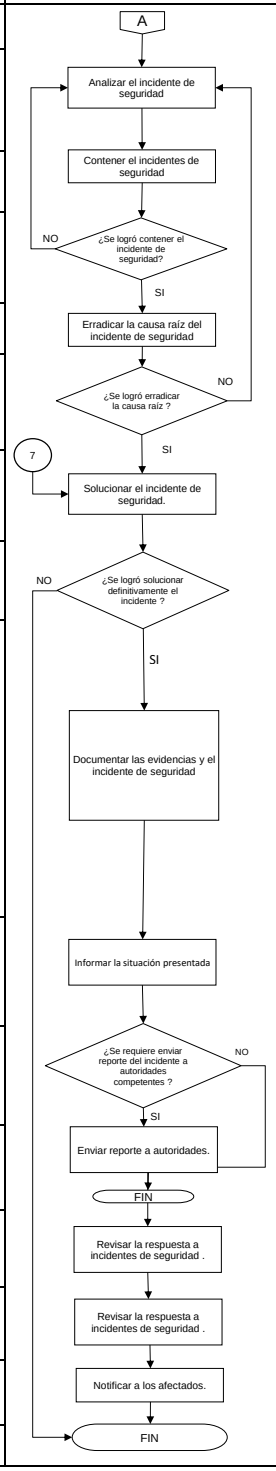
Agencia para la Reincorporación y la Normalización - ARN	GESTIÓN DE INCIDENTES DE SEGURIDAD	CÓDIGO : TI-P-03	
		FECHA : 2021-06-03	VERSIÓN : V-1

OBJETIVO	Analizar, determinar, atender, difundir, documentar y hacer seguimiento de los incidentes de seguridad detectados por las herramientas tecnológicas de análisis, reportados por los usuarios, que incluyen acciones realizadas con mitigación de los incidentes de seguridad informática y las actividades de primera atención que permitan una recuperación rápida y eficiente de los servicios que se hayan visto afectados.

No.	FLUJOGRAMA	DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE	REGISTROS
				
1		Comunicar en caso de siniestro de equipo a la mayor brevedad posible a través de la Mesa de Servicios al correo electrónico soporte@reincorporacion.gov.co. la situación presentada y anexe los soportes necesarios de acuerdo con el procedimiento GA-P-04 Procedimiento para trámite de reclamaciones ante la aseguradora**.**	Empleados públicos, contratistas, pasantes y terceros	Correo electrónico con soportes
2		Crear el caso como un incidente de seguridad en la categoria SOC (Security Operation Center)-Prevención fuga de información (DLP)- Siniestros de equipos.	Mesa de servicios	Registro de caso en la herramienta de gestión (Evidencias del siniestro de equipo)
3		Revisar si el caso creado corresponde a un siniestro de equipo	Mesa de servicios	Registro de avance en el caso en la herramienta de gestión
4		Cambiar la contraseña en el directorio activo, documentar y escalar el caso al Técnico Administrativo 17.	Mesa de servicios	Registro de avance en el caso en la herramienta de gestión
5		Verificar la configuración de Bitlocker, documentar y escalar el caso al Técnico Administrativo 17	Técnico Administrativo 17	Registro de avance en el caso en la herramienta de gestión
6		Verificar los privilegios y acceso del usuario, documentar y escalar el caso al Profesional Especializado 21	Técnico Administrativo 17	Registro de avance en el caso en la herramienta de gestión
7		Analizar los registros recolectados documentar	Profesional de Seguridad Informática	Registro de avance en el caso en la herramienta de gestión
8		Reportar si observa o sospecha de un evento o incidente de Seguridad de la Información, comunica a la mayor brevedad posible a través de la Mesa de Servicios al correo electrónico soporte@reincorporacion.gov.co.	Empleados públicos, contratistas, pasantes y terceros	Correo electrónico con soportes
9		Revisar el reporte de las herramientas tecnológicas de monitoreo y en caso de detectar una anomalía de seguridad, recopilar las evidencias necesarias. De acuerdo con lo dispuesto en el documento Guía de Gestión de eventos de Tecnologías de la información.	Analistas de SOC	Registro de caso en la herramienta de gestión (Evidencias de las anomalías presentadas que soportan el evento)
10		Realizar la categorización y registro del posible incidente de seguridad en la herramienta de gestión teniendo en cuenta el numeral 4.3 del documento TI-G-04 Guía para la gestión de incidentes de seguridad.	Mesa de Servicios o Analistas SOC	Registro de caso en la herramienta de gestión
11		Revisar si es un posible incidente de de seguridad	Analistas de SOC	Registro de caso en la herramienta de gestión
12		Documentar el caso registrado en la herramienta de gestión establecida y aplicar el documentoTI-G-04 Guía para la gestión de incidentes de seguridad.	Analistas de SOC	Registro de caso en la herramienta de gestión
13		Realizar el escalamiento del incidente de seguridad al especialista para el respectivo trámite de acuerdo con la matriz de escalamiento de la Mesa de Servicios para su análisis y clasificación.	Mesa de Servicios o Analista SOC	Registro de caso en la herramienta de gestión
14		Analizar y emitir recomendaciones de seguridad.	Analista SOC	Registro de caso en la herramienta de gestión
15		Validar si el registro es un incidente de seguridad	Especialista asignado	Registro de caso en la herramienta de gestión
16		Informar a los implicados para la solución del incidente de seguridad y conformar el equipo de acuerdo con el numeral 4.4 del documento TI-G-04 Guía para la gestión de incidentes de seguridad.	Especialista asignado SOC	Correo electrónico y registro de la acción en la herramienta de gestión

Agencia para la Reincorporación y la Normalización - ARN	GESTIÓN DE INCIDENTES DE SEGURIDAD	CÓDIGO : TI-P-03	
		FECHA : 2021-06-03	VERSIÓN : V-1

OBJETIVO	Analizar, determinar, atender, difundir, documentar y hacer seguimiento de los incidentes de seguridad detectados por las herramientas tecnológicas de análisis, reportados por los usuarios, que incluyen acciones realizadas con mitigación de los incidentes de seguridad informática y las actividades de primera atención que permitan una recuperación rápida y eficiente de los servicios que se hayan visto afectados.

No.	FLUJOGRAMA	DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE	REGISTROS
				
17		Realizar el análisis pertinente con el fin de identificar la causa o causas que dieron origen al incidente de seguridad y determinar si la solución de este supera los tiempos objetivos de recuperación de los servicios tecnológicos con el fin de activar los planes de contingencia.	Equipos de Atención de Incidentes de Seguridad-EAIS	Correo electrónico y registro de la acción en la herramienta de gestión
18		Realizar las tareas necesarias con el fin de contener el incidente de seguridad y así minimizar su impacto.	Equipos de Atención de Incidentes de Seguridad-EAIS	Correo electrónico y registro de la acción en la herramienta de gestión
19		Verificar si la (s) acción (s) realizada (s) lograron contener el incidente de seguridad	Equipos de Atención de Incidentes de Seguridad-EAIS	Correo electrónico y registro de la acción en la herramienta de gestión
20		Realizar las tareas necesarias con el fin de erradicar la causa raíz detectada.	Equipos de Atención de Incidentes de Seguridad-EAIS	Correo electrónico y registro de la acción en la herramienta de gestión
21		Verificar si la (s) acción (s) realizada (s) lograron erradicar la causa raíz	Equipos de Atención de Incidentes de Seguridad-EAIS	Correo electrónico y registro de la acción en la herramienta de gestión
22		Realizar las tareas necesarias con el fin de solucionar definitivamente el incidente Nota: en algunos casos la solución del incidente puede ser dada desde la contención del mismo, pero en otros requiere la recuperación o restauración del servicio a su estado normal de operación.	Equipos de Atención de Incidentes de Seguridad-EAIS	Registro de la acción en la herramienta de gestión
23		Verificar si la(s) acción(es) realizada(s) lograron solucionar definitivamente el incidente No: Aplicar la Guía Gestión de Problemas y finalizar el procedimiento.	Equipos de Atención de Incidentes de Seguridad-EAIS	Registro de la acción en la herramienta de gestión
24		1. Recopilar y organizar las evidencias producto de la investigación del incidente de seguridad siguiendo lo estipulado en el numeral 4.5.2 del documento TI-G-04 Guía para la gestión de incidentes de seguridad. 2. Documentar el incidente de seguridad presentado de acuerdo con lo siguiente: Los incidentes de seguridad Muy graves deben ser documentados en la herramienta de gestión y adicionalmente debe generarse un reporte independiente del mismo donde se evidencie las actividades realizadas de contención y solución. Nota 1: En caso de que se presente un incidente de seguridad relacionado con base de datos personales o información sensible, deberá ser reportado a la Superintendencia de Industria y Comercio, por el Oficial de Datos a través del formato de *F2.P5.GTI Reporte Incidentes Bases de Datos Personales Superintendencia de Industria y Comercio.* Nota 2: Para el registro del incidente, el Oficial de protección de Datos personales debe apoyarse en el Manual de Usuario RNBD, de la Superintendencia de Industria y Comercio.	Equipos de Atención de Incidentes de Seguridad-EAIS Oficial de protección de Datos personales	Registro de la acción en la herramienta de gestión Registro en el aplicativo de la SIC
25		Informar con base en la evidencia y documentación generada la situación presentada a la Alta Dirección o autoridades competentes.	Jefe de la Oficina de Tecnologías de la Información/ Coordinador Grupo de Infraestructura y Soporte / Profesional de Seguridad Informática	Presentación e informe consolidado
26		Verificar si se requiere enviar reporte del incidente a autoridades competentes según el numeral 4.6 del documento TI-G-04 Guía para la gestión de incidentes de seguridad.	Profesional de Seguridad Informática	Correo electrónico
27		Enviar la información a la autoridad competente sobre la gestión realizada del incidente solucionado. según el numeral 4.6 del documento TI-G-04 Guía para la gestión de incidentes de seguridad.	Profesional de Seguridad Informática	Correo electrónico
28		Revisar la respuesta y solución dada al incidente de seguridad y postular a la base de conocimiento las lecciones aprendidas ver el numeral 4.5.4 del documento TI-G-04 Guía para la gestión de incidentes de seguridad.	Profesional de Seguridad Informática Oficial de Seguridad de la Información	Acta de reunión y correo para postulación a la base de conocimiento.
29		Documentar las lecciones aprendidas en la base de conocimiento	Equipos de Atención de Incidentes de Seguridad-EAIS	Registro de la acción en la herramienta de gestión
30		Informar o notificar a los afectados sobre incidentes que afecten la confidencialidad o integridad de su información, así como de las medidas adoptadas para la remediación del incidente.	Oficial de Seguridad de la Información	Intranet