

 <div>ALCALDÍA MAYOR DE BOGOTÁ D.C. INTEGRACIÓN SOCIAL Instituto Distrital para la Protección de la Niñez y la Juventud</div>	GESTION DE TICS	CÓDIGO	E-GTIC-PR-007
		VERSIÓN	02
	INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	PÁGINA	1 de 5
		VIGENTE DESDE	04/10/2022

1. INFORMACIÓN GENERAL DEL PROCEDIMIENTO	
OBJETIVO	Establecer los lineamientos para la creación y registro de incidentes de seguridad de la información con el fin de ejecutar las estrategias de contención y erradicación de este y evitar así la materialización de los riesgos de seguridad de la información en el IDIPRON.
ALCANCE	El procedimiento inicia con la solicitud por parte del responsable de la secretaria General, Área, dependencias Unidades de Protección Integral y finaliza con el cierre del caso.

2. GLOSARIO	
Término	Definición
Activo	En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas...) que tenga valor para la organización.
Cadena de Custodia	Procedimiento documentado y controlado que se le aplica a toda evidencia física o elemento material probatorio desde su recolección hasta su disposición final, en donde se puede observar su descripción e identificación, una línea de tiempo, y las personas que han participado en su custodia.
Clasificación de la Información	Es el ejercicio por medio del cual se determina que la información pertenece a uno de los niveles de clasificación estipulado por la entidad. Tiene como objetivo asegurar que la información obtenga el nivel de protección adecuado. La información debe clasificarse en términos de sensibilidad e importancia para la entidad.
Confidencialidad	Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
CSIRT-PONAL	Equipo de Respuesta a Incidentes de Seguridad Informática de la Policía Nacional CSIRT-PONAL, un grupo creado para atender las necesidades de prevención, atención e investigación de los eventos e incidentes de seguridad informática, con el fin de proteger la infraestructura tecnológica, los activos de información y mitigar el impacto ocasionado por la materialización de los riesgos asociados con el uso de las tecnologías de la información y las telecomunicaciones.
Disponibilidad	Propiedad de que la información sea accesible y utilizable por solicitud de una entidad y/o persona autorizada.
Evento de Seguridad	Ocurrencia identificada de estado en un sistema de información, servicio o red que indica una posible brecha de seguridad, falla de un control o una condición no identificada que puede ser relevante para la seguridad de la información.
Incidentes de seguridad de la información	Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
Integridad	Conservar con exactitud la información que fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.
Seguridad de la información	preservación de la confidencialidad, integridad y disponibilidad de la información.
Valoración del riesgo	Proceso global de análisis y evaluación del riesgo.
Vulnerabilidad	Debilidad de un activo o control que pueda ser explotado por una o más amenazas.


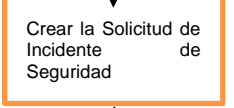
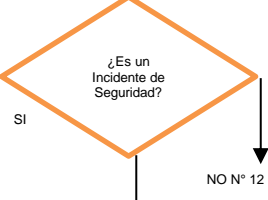
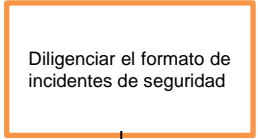
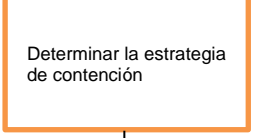
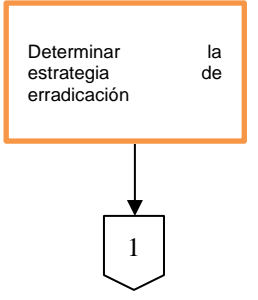
3. CONDICIONES GENERALES	
No.	Descripción
1	Clasificación de Criticidad de los Incidentes de Seguridad: Bajo >= 5 Días Medio >= 2 Días Alto <= 12 Horas Crítico <= 4 Horas
2	Bajo: este nivel de criticidad se da para aquellos incidentes o eventos que son detectados y/o registrados como posibles amenazas para los activos de información, es decir, no impactan las características de integridad y/o confidencialidad y/o disponibilidad
3	Medio: este nivel de criticidad se da para aquellos incidentes o eventos que son detectados y/o registrados como posibles amenazas, que pueden afectar los activos de información del Instituto Distrital para la Protección de la Niñez y la Juventud IDIPRON, impactando de modo limitado las características de integridad y/o confidencialidad y/o disponibilidad frente a un activo no crítico para el IDIPRON.
4	Alto: este nivel de criticidad se da para aquellos incidentes o eventos que son detectados y/o registrados, porque en ellos, es posible establecer una amenaza sobre los activos de información capaz de impactar de manera considerable las

 <div>ALCALDÍA MAYOR DE BOGOTÁ D.C. INTEGRACIÓN SOCIAL Instituto Distrital para la Protección de la Niñez y la Juventud</div>	GESTION DE TICS	CÓDIGO	E-GTIC-PR-007
		VERSIÓN	02
	INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	PÁGINA	2 de 5
		VIGENTE DESDE	04/10/2022

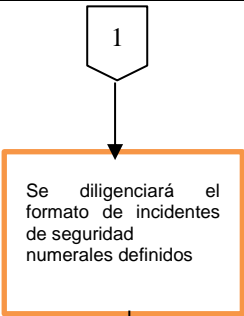
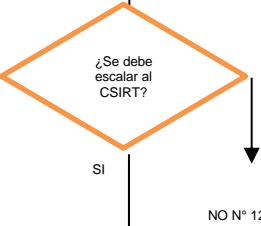
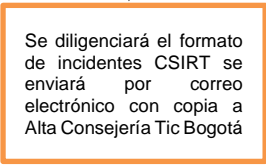

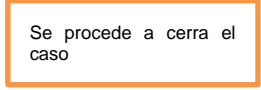
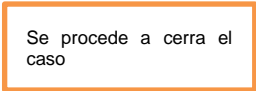
	características de integridad y/o confidencialidad y/o disponibilidad de un activo no crítico en el Instituto Distrital para la Protección de la Niñez y la Juventud IDIPRON.												
5	Crítico: Este nivel de criticidad se da para aquellos incidentes o eventos que son detectados y/o registrados, porque 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 un activo crítico para el Instituto Distrital para la Protección de la Niñez y la Juventud IDIPRON.												
6	<p>Estrategia de Contención: El Modelo de Privacidad y Seguridad de la Información MSPI sugiere algunas estrategias de contención que se pueden aplicar cuando se presente un incidente de seguridad que comprometa la Integridad, Disponibilidad y Confidencialidad de la información el Instituto Distrital para la Protección de la Niñez y la Juventud IDIPRON. Estas pueden llegar a ser sin ser limitadas así:</p> <table><tr><th>INCIDENTE DE SEGURIDAD</th><th>ESTRATEGIA DE CONTENCIÓN</th></tr><tr><td>Accesos no Autorizados</td><td>Bloqueos de cuenta Apagado de la máquina por parte del Equipo Técnico Bloqueo de puertos</td></tr><tr><td>Códigos Maliciosos</td><td>Desconexión de la red del equipo afectado Bloqueo de Puertos Actualización de Antivirus y Antimalware</td></tr><tr><td>Reconocimiento</td><td>Nuevas reglas de filtrado en el Firewall Bloqueo de Puertos</td></tr><tr><td>Denegación de Servicio</td><td>Bloqueos de cuenta Apagado de la máquina por parte del Equipo Técnico Bloqueo de puertos</td></tr><tr><td>Corrupción / Uso inapropiado de recursos</td><td>Proceso disciplinario del servidor publico Bloqueo de Cuentas</td></tr></table>	INCIDENTE DE SEGURIDAD	ESTRATEGIA DE CONTENCIÓN	Accesos no Autorizados	Bloqueos de cuenta Apagado de la máquina por parte del Equipo Técnico Bloqueo de puertos	Códigos Maliciosos	Desconexión de la red del equipo afectado Bloqueo de Puertos Actualización de Antivirus y Antimalware	Reconocimiento	Nuevas reglas de filtrado en el Firewall Bloqueo de Puertos	Denegación de Servicio	Bloqueos de cuenta Apagado de la máquina por parte del Equipo Técnico Bloqueo de puertos	Corrupción / Uso inapropiado de recursos	Proceso disciplinario del servidor publico Bloqueo de Cuentas
INCIDENTE DE SEGURIDAD	ESTRATEGIA DE CONTENCIÓN												
Accesos no Autorizados	Bloqueos de cuenta Apagado de la máquina por parte del Equipo Técnico Bloqueo de puertos												
Códigos Maliciosos	Desconexión de la red del equipo afectado Bloqueo de Puertos Actualización de Antivirus y Antimalware												
Reconocimiento	Nuevas reglas de filtrado en el Firewall Bloqueo de Puertos												
Denegación de Servicio	Bloqueos de cuenta Apagado de la máquina por parte del Equipo Técnico Bloqueo de puertos												
Corrupción / Uso inapropiado de recursos	Proceso disciplinario del servidor publico Bloqueo de Cuentas												
7	<p>Estrategia de Erradicación: El Modelo de Privacidad y Seguridad de la Información MSPI sugiere algunas estrategias de erradicación que se pueden aplicar cuando se presente un incidente de seguridad que comprometa la Integridad, Disponibilidad y Confidencialidad de la información el Instituto Distrital para la Protección de la Niñez y la Juventud IDIPRON. Estas pueden llegar a ser sin ser limitadas así:</p> <table><tr><th>INCIDENTE DE SEGURIDAD</th><th>ESTRATEGIA DE ERRADICACIÓN</th></tr><tr><td>Denegación de Servicios</td><td>Restitución del servicio caído Restauración de Backups</td></tr><tr><td>Códigos Maliciosos</td><td>Corrección de Efectos Restauración de Backups Actualización de Antivirus</td></tr><tr><td>Vandalismo</td><td>Nuevas reglas de filtrado Bloqueo de Puertos</td></tr><tr><td>Corrupción / Uso inapropiado de recursos</td><td>Recuperación del Servicio y/o Sistemas de Información Restauración de Backups</td></tr><tr><td>Intrusión</td><td>Restauración de equipos y servicios Recuperación de los Datos Restauración de Backups</td></tr></table>	INCIDENTE DE SEGURIDAD	ESTRATEGIA DE ERRADICACIÓN	Denegación de Servicios	Restitución del servicio caído Restauración de Backups	Códigos Maliciosos	Corrección de Efectos Restauración de Backups Actualización de Antivirus	Vandalismo	Nuevas reglas de filtrado Bloqueo de Puertos	Corrupción / Uso inapropiado de recursos	Recuperación del Servicio y/o Sistemas de Información Restauración de Backups	Intrusión	Restauración de equipos y servicios Recuperación de los Datos Restauración de Backups
INCIDENTE DE SEGURIDAD	ESTRATEGIA DE ERRADICACIÓN												
Denegación de Servicios	Restitución del servicio caído Restauración de Backups												
Códigos Maliciosos	Corrección de Efectos Restauración de Backups Actualización de Antivirus												
Vandalismo	Nuevas reglas de filtrado Bloqueo de Puertos												
Corrupción / Uso inapropiado de recursos	Recuperación del Servicio y/o Sistemas de Información Restauración de Backups												
Intrusión	Restauración de equipos y servicios Recuperación de los Datos Restauración de Backups												

	GESTION DE TICS	CÓDIGO	E-GTIC-PR-007
		VERSIÓN	02
	INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	PÁGINA	3 de 5
		VIGENTE DESDE	04/10/2022

4. DESARROLLO DEL PROCEDIMIENTO

No.	FLUJOGRAMA	DESCRIPCIÓN	RESPONSABLE	PUNTO DE CONTROL	REGISTRO	TIEMPO
1						
2		Crear la solicitud de incidente de seguridad de la información mediante el uso de la herramienta mesa de servicios y validar la recepción por parte del encargado del proceso o el oficial de seguridad.	Responsable de la secretaria General, del Área, dependencias Unidades de Protección Integral		Sistema de mesa de servicios	Max: 1 hora Min: 15 min Prom:
3		El profesional encargado del proceso de Gestión de TICS o el Oficial de Seguridad evaluará si es un incidente de seguridad para tal razón continuara el flujograma de no serlo continuara en el numeral 12.	El profesional encargado del proceso de Gestión de TICS o el Oficial de Seguridad	X	Sistema de mesa de servicios	Max: 1 hora Min: 30 Min Prom:
4		El profesional encargado del proceso de Gestión de TICS o el Oficial de Seguridad se contactará con la persona que crea la solicitud con el fin de solicitar información adicional para el Proceso, Área, diligenciamiento del formato de incidentes de seguridad, Clasificando el Incidente según los numerales 1,2,3,4,5 de las condiciones generales de este documento	El profesional encargado del proceso de Gestión de TICS o el Oficial de Seguridad y Persona que crea solicitud		Sistema de mesa de servicios, formato Incidentes de Seguridad E-GTIC-FT-020	Max: 1 día Min: 1 hora Prom:
5		El profesional encargado del proceso de Gestión de TICS o el Oficial de Seguridad recolectara, analizara y asegurara las evidencias encontradas o reportadas en el incidente de seguridad según el numeral 6 de las condiciones generales del presente documento, referido como Estrategia de Contención	El profesional encargado del proceso de Gestión de TICS o el Oficial de Seguridad		formato Incidentes de Seguridad E-GTIC-FT-020	Max: 1 día Min: 1 hora Prom:
6		El profesional encargado del proceso de Gestión de TICS o el Oficial de Seguridad aplicara la estrategia para prevenir daño, adecuado al incidente, para evitar daño colateral o propagación de este según el numeral 7 de las condiciones generales, referido como Estrategia de Erradicación	El profesional encargado del proceso de Gestión de TICS o el Oficial de Seguridad		formato Incidentes de Seguridad E-GTIC-FT-020	Max: 1 día Min: 1 hora Prom:

	GESTION DE TICS	CÓDIGO	E-GTIC-PR-007
		VERSIÓN	02
	INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	PÁGINA	4 de 5
		VIGENTE DESDE	04/10/2022

No.	FLUJOGRAMA	DESCRIPCIÓN	RESPONSABLE	PUNTO DE CONTROL	REGISTRO	TIEMPO
7		El profesional encargado del proceso de Gestión de TICS o el Oficial diligenciará todos los datos solicitados incluyendo el impacto, que atributo de la información (Confidencialidad, Integridad, Disponibilidad) se vio comprometida, así como las lecciones aprendidas a raíz de este incidente y si el mismo procede para crear un plan de mejoramiento y acciones para solucionar la causa raíz	El profesional encargado del proceso de Gestión de TICS o el Oficial de Seguridad		formato Incidentes de Seguridad E-GTIC-FT-020	Max: 1 día Min: 1 hora Prom:
8		El profesional encargado del proceso de Gestión de TICS o el Oficial de Seguridad con el Director General evaluará la pertinencia de enviar el reporte al CSIRT para tal razón continuará el flujograma de no serlo continuará en el numeral 12.	El profesional encargado del proceso de Gestión de TICS o el Oficial de Seguridad	X	Sistema de mesa de servicios	Max: 1 día Min: 1 hora Prom:
9		El profesional encargado del proceso de Gestión de TICS o el Oficial de Seguridad diligenciará formato del CSIRT y enviara la información por correo electrónico a CSIRT-PONAL	El profesional encargado del proceso de Gestión de TICS o el Oficial de Seguridad	Correo Electrónico Archivo del Formato	Formato Incidentes de Seguridad CSIRT	Max: 1 día Min: 1 hora Prom:
10		El profesional encargado del proceso de Gestión de TICS o el Oficial de Seguridad con el Director General analizarán la necesidad de elaborar un plan de mejoramiento para mitigar la causa raíz del incidente Si se determina crear plan de mejoramiento se continúa con la siguiente actividad, de lo contrario continúa con la actividad No. 12.	El profesional encargado del proceso de Gestión de TICS o el Oficial de Seguridad	Correo Electrónico Archivo del Formato	Formato Incidentes de Seguridad CSIRT	Max: 1 día Min: 1 hora Prom:
11		Diligenciar los campos de Lecciones Aprendidas y Plan de Mejoramiento en el formato Sistema de mesa de servicios, formato Incidentes de Seguridad E-GTIC-FT-020	El profesional encargado del proceso de Gestión de TICS o el Oficial de Seguridad		formato Incidentes de Seguridad E-GTIC-FT-020	Max:1 hora Min: 30 min Prom:
12		El profesional encargado del proceso de Gestión de TICS o el Oficial de Seguridad cerrara el caso en la mesa de servicios.	El profesional encargado del proceso de Gestión de TICS o el Oficial de Seguridad		Sistema de mesa de servicios	Max:1 hora Min: 30 min Prom:

	GESTION DE TICS	CÓDIGO	E-GTIC-PR-007
		VERSIÓN	02
	INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	PÁGINA	5 de 5
		VIGENTE DESDE	04/10/2022

5. CONTROL DE CAMBIOS

VERSIÓN	DESCRIPCIÓN DE CAMBIOS	FECHA (DD/MM/AAAA)	ELABORÓ
01	Se realiza la creación del documento para diligenciar los incidentes de seguridad de la información que se puedan llegar a presentar en el Instituto Distrital para la protección de la niñez y la juventud IDIPRON.	01/10/2021	KHAANKO NORBERTO RUIZ RODRIGUEZ / JONNY HIRLAN TORRES RUBIANO Contratistas Profesional Gestión de TICS
02	<ol style="list-style-type: none">Se realiza la actualización de las áreas / dependencias y cargos mencionados en el documento con el fin de dar cumplimiento a lo establecido en el Acuerdo “Por el cual se modifica la Estructura Organizacional del INSTITUTO DISTRITAL PARA LA PROTECCIÓN DE LA NIÑEZ Y LA JUVENTUD IDIPRON, se establecen las funciones de sus dependencias y se dictan otras disposiciones”Se realiza el ajuste de la codificación de los formatos y documentos mencionados en el procedimiento (manual, documento interno o instructivo), de acuerdo con los ajustes realizados a los códigos de los documentos del Sistema Integrado de Gestión producto del rediseño institucional.Se realiza cambio de código del documento del A-TIC-PR-007 al código E-GTIC-PR-007	04/10/2022	MARISOL MONSALVE USME PROFESIONAL OFICINA ASESORA DE PLANEACIÓN

6. REVISIÓN Y APROBACIÓN

	NOMBRE	CARGO	FECHA (DD/MM/AAAA)
REVISÓ	VIVIANA ANDREA SANCHEZ MORALES	PROFESIONAL OFICINA ASESORA DE PLANEACIÓN	04/10/2022
APROBACIÓN LÍDER DE PROCESO	FABIAN ANDRÉS CORREA ÁLVAREZ	JEFE OFICINA ASESORA DE PLANEACIÓN	04/10/2022