

	GESTION DE LAS TECNOLOGIAS DE LA INFORMACION Y DE LA COMUNICACION	CÓDIGO	E-GTIC-PR-011
		VERSIÓN	01
	PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS	PÁGINA	1 de 4
		VIGENTE DESDE	27/12/2024

1. INFORMACIÓN GENERAL DEL PROCEDIMIENTO	
OBJETIVO	Proteger la infraestructura tecnológica y los sistemas de información del IDIPRON contra amenazas representadas por códigos maliciosos, como virus, troyanos, ransomware, spyware, y otros. Se busca garantizar la confidencialidad, integridad y disponibilidad de los datos, así como la continuidad de la operación de la organización, minimizando los riesgos derivados de estos ataques.
ALCANCE	Este procedimiento aplica a todos los sistemas, aplicaciones y dispositivos que gestionan información dentro de la organización, incluidos equipos de usuarios(as) finales, servidores(as), redes y servicios en la nube. Es aplicable a todas las áreas del IDIPRON que interactúan con la infraestructura tecnológica, con un enfoque integral en la prevención y respuesta ante amenazas cibernéticas

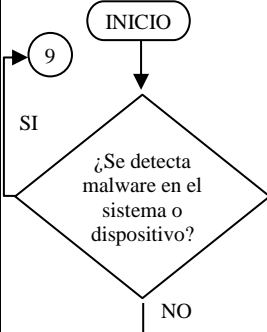
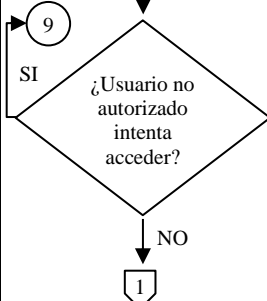
2. GLOSARIO	
Término	Definición
Aislamiento	Acción de desconectar o separar un sistema o red afectada para evitar la propagación de malware o daños adicionales.
Alta Consejería Distrital de TIC	Entidad encargada de la coordinación y dirección de la política pública en Tecnologías de la Información y Comunicaciones en el ámbito distrital, para garantizar la seguridad y gobernanza digital.
Análisis forense	Proceso de investigación de un incidente de seguridad con el fin de recolectar y preservar evidencia, para determinar el alcance y las causas del ataque.
Antivirus	Software diseñado para detectar, prevenir y eliminar programas maliciosos (malware) en sistemas informáticos, asegurando la integridad y funcionamiento adecuado del dispositivo.
Auditoría de seguridad	Evaluación sistemática de las políticas, procedimientos y controles de seguridad de un sistema para identificar vulnerabilidades y asegurar el cumplimiento de normativas.
COLCERT	Equipo de Respuesta a Emergencias Informáticas de Colombia), organismo nacional encargado de coordinar la gestión de incidentes de ciberseguridad
CSIRT	Equipo de Respuesta a Incidentes de Seguridad Informática), encargado de coordinar la respuesta ante incidentes de ciberseguridad.
Desviación de comportamiento	Acción o comportamiento que se aleja de la norma establecida, como un intento de acceso no autorizado o la ejecución de programas maliciosos en un sistema.
Escaneo en tiempo real	Función del software antivirus que realiza un análisis constante de archivos y procesos en ejecución, detectando y previniendo amenazas en tiempo real.
Firewall	Dispositivo o software que filtra y controla el tráfico de red entrante y saliente, protegiendo los sistemas de accesos no autorizados o maliciosos.
Intrusión	Acción no autorizada que busca acceder a sistemas o redes con la intención de robar, alterar o destruir datos e información.
Malware	Programa o código malicioso creado para dañar, interrumpir o acceder de manera no autorizada a un sistema o red informática...
Parches de seguridad	Actualizaciones de software proporcionadas por los desarrolladores para corregir vulnerabilidades de seguridad y mejorar la protección del sistema ante posibles amenazas.
Phishing	Técnica de ataque cibernético que consiste en engañar a los/las usuarios(as) para que revelen información confidencial, como contraseñas o datos bancarios, mediante correos electrónicos o sitios web fraudulentos.
Política de acceso	Conjunto de reglas que determinan quién puede acceder a qué recursos y en qué condiciones, garantizando la seguridad y la integridad de los sistemas y datos.
Principio de menor privilegio	Concepto que establece que los/las usuarios(as) deben tener sólo el acceso mínimo necesario para realizar sus tareas, minimizando así los riesgos de seguridad.
Ransomware	Tipo de malware que cifra los archivos de un sistema y exige un rescate para restaurar el acceso a los mismos.
Recuperación ante desastres	Conjunto de medidas, procedimientos y herramientas que permiten restaurar un sistema o infraestructura afectada por un incidente de seguridad o desastre, garantizando la continuidad de operaciones.
Respuesta ante incidentes	Conjunto de acciones coordinadas para identificar, gestionar y mitigar un incidente de seguridad, con el objetivo de reducir su impacto y restaurar los servicios afectados.
Seguridad perimetral	Estrategias y tecnologías utilizadas para proteger los límites de una red, evitando accesos no autorizados desde el exterior, como firewalls y sistemas de detección de intrusos.

3. CONDICIONES GENERALES

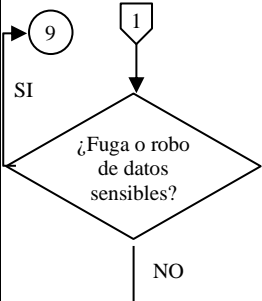
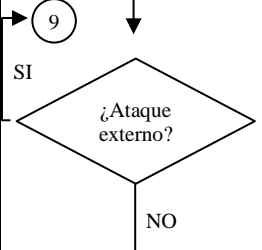
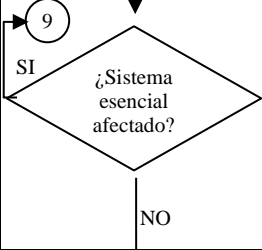
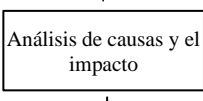
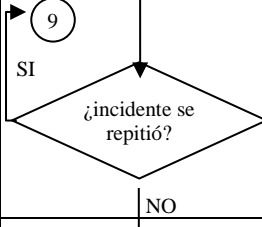
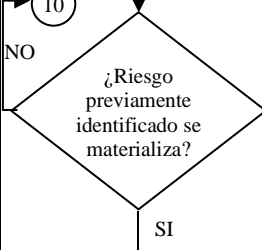
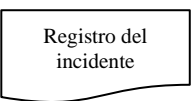
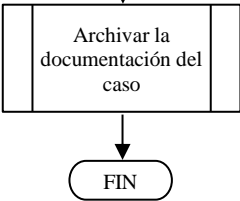
	GESTION DE LAS TECNOLOGIAS DE LA INFORMACION Y DE LA COMUNICACION	CÓDIGO	E-GTIC-PR-011
		VERSIÓN	01
	PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS	PÁGINA	2 de 4
		VIGENTE DESDE	27/12/2024

No.	Descripción
1	Antivirus y Software de Seguridad: Todos los dispositivos deberán contar con un software antivirus actualizado, que debe estar licenciado y configurado para realizar análisis en tiempo real y análisis programados. Esto garantiza la detección y eliminación de malware en los dispositivos. El responsable de implementar esta medida será un profesional universitario en tecnologías de la información, quien realizará un monitoreo continuo y asegurará que las definiciones de virus estén siempre actualizadas.
2	Monitoreo y Detección de Intrusiones: Se mantendrá un sistema de monitoreo robusto para detectar intentos de acceso no autorizado o actividades sospechosas en toda la red. Este sistema debe integrar un firewall con políticas de seguridad estrictas, lo que permite la protección del perímetro y la detección temprana de amenazas. El equipo de seguridad será responsable de revisar las alertas generadas y tomar las acciones correctivas oportunas para prevenir intrusiones.
3	Actualización de Sistemas y Aplicaciones: Todo el software de los dispositivos y servidores debe actualizarse de acuerdo con los parches de seguridad proporcionados por los fabricantes. Las actualizaciones deben ser coordinadas por el equipo de TI para garantizar que las vulnerabilidades conocidas sean corregidas a tiempo, y deben aplicarse a todas las plataformas, incluyendo sistemas operativos, aplicaciones críticas y herramientas de seguridad.
4	Control de Accesos y Privilegios: Sólo los/las usuarios(as) autorizados tendrán acceso a información sensible. Se implementará el principio de menor privilegio, garantizando que cada persona solo pueda acceder a los recursos estrictamente necesarios para realizar su trabajo. Este control se administrará de manera centralizada por el Jefe de Seguridad de la Información, quien revisará periódicamente los permisos de acceso y la asignación de privilegios.
5	Filtrado de Correo Electrónico y Navegación Web: Se implementarán filtros avanzados para evitar la recepción de correos electrónicos maliciosos (phishing, malware, etc.), además de políticas de navegación web segura. Se establecerán procedimientos para monitorear y bloquear sitios web potencialmente peligrosos, protegiendo así la red institucional contra posibles ataques. El equipo de seguridad y los responsables de redes gestionarán estos filtros, garantizando que los niveles de seguridad sean adecuados.
6	Educación y Capacitación: Todo el personal recibirá formación continua sobre los riesgos asociados al malware y las mejores prácticas para prevenirlo. Estas formaciones incluirán el uso adecuado de herramientas de seguridad, cómo identificar correos electrónicos fraudulentos, evitar enlaces maliciosos y cómo comportarse ante incidentes sospechosos.
7	Respuesta ante Incidentes: En caso de que se detecte un incidente de malware o vulnerabilidad de seguridad, el equipo de respuesta ante incidentes actuará de manera inmediata. Esto incluirá el aislamiento de sistemas afectados, la identificación y eliminación del malware, y la restauración de la funcionalidad de los sistemas afectados. La coordinación de la respuesta será liderada por el Jefe de la oficina de TI, quien asegurará que se sigan los procedimientos establecidos para mitigar el impacto y evitar futuras incidencias.
8	Gestión de Incidencias y Medidas Correctivas: Ante cualquier incidencia o anomalía detectada, el/la jefe de TI deberá documentarla en un informe detallado. Este informe debe incluir la naturaleza de la incidencia, las medidas correctivas implementadas y las recomendaciones para evitar que se repita en el futuro. De materializarse un riesgo se debe reportar el Csirt- Colcert- Alta Consejería.

4. DESARROLLO DEL PROCEDIMIENTO

No.	FLUJOGRAMA	DESCRIPCIÓN	RESPONSABLE	PUNTO DE CONTROL	REGISTRO	TIEMPO
1		Determinar si se detecta malware en el sistema o dispositivo  Si se detecta, se debe iniciar el aislamiento inmediato del sistema afectado, ejecutando un análisis completo y eliminar el malware detectado; y continuar a la actividad 9.  Si no se detecta, continuar a la actividad 2.	Administrador(a) de TI	X	Informe de análisis de malware	Min: 1 hora Max: 2 horas Prom: 1,5 horas
2		Identificar si algún usuario(a) no autorizado intenta acceder.  Si se detecta, se debe bloquear el acceso; y continuar a la actividad 9.  Si no, continuar a la actividad 3.	Coordinador(a) de Seguridad de TI	X	Formato de incidente de seguridad	Min: 30 minutos Max: 1 hora Prom: 45 minutos

	GESTION DE LAS TECNOLOGIAS DE LA INFORMACION Y DE LA COMUNICACION	CÓDIGO	E-GTIC-PR-011
		VERSIÓN	01
	PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS	PÁGINA	3 de 4
		VIGENTE DESDE	27/12/2024

No.	FLUJOGRAMA	DESCRIPCIÓN	RESPONSABLE	PUNTO DE CONTROL	REGISTRO	TIEMPO
3		<p>Comprobar si se presenta fuga de información o robo de datos sensibles para la entidad.</p> <p>En dado caso, descubrir que datos sensibles han sido divulgados o robados, para notificar a las autoridades pertinentes y comunicar a los afectados con el fin de investigar la causa del incidente y activar medidas correctivas; y continuar a la actividad 9.</p> <p>Si no, continuar a la actividad 4.</p>	Jefe de Seguridad de la Información	X	Informe de incidente de seguridad	Prom: 4 horas
4		<p>Comprobar si se presenta algún ataque externo.</p> <p>Si se detecta ataque, se debe activar el plan de recuperación de desastres tras detectar un ataque externo, restaurando el sistema afectado con la mínima interrupción posible; y continuar a la actividad 9.</p> <p>Si no, continuar a la actividad 5.</p>	Coordinador de Seguridad de TI	X	Plan de recuperación ante desastres	Min: 1 hora Max: 3 horas Prom: 2 horas
5		<p>Verificar si se afectó el sistema esencial de la entidad.</p> <p>De afectarse el sistema, documentar el incidente, evaluar su impacto, analizar las causas raíz y proponer medidas correctivas para evitar recurrencias.</p> <p>Si no, continuar a la actividad 10.</p>	Administrador de TI	X	Formato de restauración de servicios	Min: 30 minutos Max: 1 hora Prom: 45 minutos
6		Realización de un análisis de las causas y el impacto.	Líder de Seguridad de TI		Formato de análisis post-incidente	Min: 1 día Max: 2 días Prom: 1,5 días
7		<p>Comprobar si el incidente se repitió.</p> <p>De repetirse el incidente, revisar y reforzar las medidas preventivas, actualizar las políticas de seguridad y realizar auditorías adicionales para corregir debilidades.</p> <p>Si no, continuar a la actividad 10.</p>	Jefe de Seguridad de la Información	X	Informe de revisión y auditoría	Prom: 1 semana
8		<p>Comprobar si el riesgo identificado, se vuelve a materializar.</p> <p>En dado caso, notificar inmediatamente al CSIRT, COLCERT y a la Alta Consejería Distrital de TIC, seguir el protocolo establecido para la notificación y resolución del incidente.</p> <p>Si no, continuar a la actividad 10.</p>	Coordinador(a) de Seguridad de TI	X	Reporte de notificación a entidades	Min: 1 hora Max: 2 horas Prom: 1,5 horas
9		Documentar el caso para prevenir futuros incidentes.	Profesional y/o técnico Oficina de Tecnologías de la Información y las Comunicaciones		Informe de incidente de seguridad	Max: 2 horas Min: 1 hora Prom: 1,5 horas
10		Archivar la documentación generada a lo largo del procedimiento.	Profesional y/o técnico Oficina de Tecnologías de la Información y las Comunicaciones		Instructivo: Organización de archivos de gestión A-GDO-IN-001	Max: 2 horas Min: 1 hora Prom: 1,5 horas

	GESTION DE LAS TECNOLOGIAS DE LA INFORMACION Y DE LA COMUNICACION	CÓDIGO	E-GTIC-PR-011
		VERSIÓN	01
	PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS	PÁGINA	4 de 4
		VIGENTE DESDE	27/12/2024

5. CONTROL DE CAMBIOS

VERSIÓN	DESCRIPCIÓN DE CAMBIOS	FECHA (DD/MM/AAAA)	ELABORÓ
01	Se crea el procedimiento PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS, con el fin de proteger la infraestructura tecnológica y los sistemas de información del IDIPRON contra amenazas representadas por códigos maliciosos: como virus, troyanos, ransomware, spyware entre otros.	27/12/2024	<b>YEIMMY ROCIO CARDENAS CRUZ</b> TECNICO OPERATIVO CÓDIGO 314 GRADO 03  <b>WILSON ANDRES RAMIREZ URBINA</b> PROFESIONAL OFICINA DE TIC

6. REVISIÓN Y APROBACIÓN

	NOMBRE	CARGO	FECHA (DD/MM/AAAA)
REVISÓ	SANDRA PATRICIA GUERRERO RAMIREZ	ING. GOBIERNO DIGITAL OFICINA DE TIC	27/12/2024
APROBACIÓN LÍDER DE PROCESO	LUIS CARLOS OCAMPO RAMOS	JEFE OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIÓN	27/12/2024