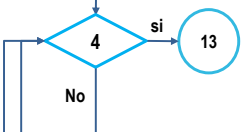
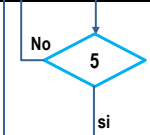
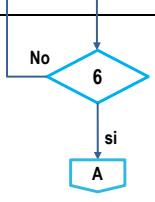
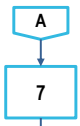
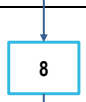
PROCEDIMIENTO: GESTIÓN DE INCIDENTES DE SEGURIDAD
PROCESO: GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES
Versión: 4 Fecha: 17/12/2024 Código: GTI-P-08

1. OBJETIVO:	Gestionar incidentes de seguridad para mitigar el impacto en la confidencialidad, integridad y disponibilidad de la información del Ministerio de Vivienda, Ciudad y Territorio, siguiendo los lineamientos y estándares establecidos.
2. ALCANCE:	Inicia con la identificación de un incidente de seguridad, continúa con la detección, contención y solución del mismo, y finaliza con la documentación y el análisis de lecciones aprendidas.
3. RESPONSABLE:	Lider del proceso Grupo de apoyo tecnologico
4. DEFINICIONES.	**Activo de Información:** Cualquier dato que una organización valora y debe proteger. **Amenaza:** Algo que podría causar daño a un sistema o activo de información. **Analista de Mesa de Servicio:** Persona que recibe y registra incidentes de seguridad y es el primer contacto en su gestión. **Ataque Informático**: Actividades realizadas para vulnerar la seguridad de un sistema. Ciberataque: Maniobra ofensiva para atacar sistemas de información o redes. **Ciberseguridad:** Protección de información frente a amenazas en sistemas interconectados. **Código Malicioso:** Programas que se replican y afectan el funcionamiento del sistema. **Contención de un Incidente:** Actividades para reducir el impacto inmediato de un incidente de seguridad. **Denegación de Servicio:** Actividades para interrumpir o degradar un servicio informático. **Equipo de Respuesta a Incidentes:** Grupo del MVCT o terceros que gestionan incidentes de seguridad. **Evento**: Ocurrencia de circunstancias específicas. **Evento de Seguridad de la Información:** Situación que indica un posible problema de seguridad de la información. **Incidente de Seguridad Informática:** Violación o amenaza de políticas de seguridad informática. **Incidente de Seguridad de la Información:** Acceso no autorizado o interrupción de sistemas que afecta la seguridad de la información. **Incidente de Continuidad Tecnológica:** Evento que afecta los servicios tecnológicos. **Infraestructura Crítica (IC):** Infraestructuras esenciales cuyo daño tendría un grave impacto. **Phishing:** Estrategia para obtener información personal mediante engaño. **Ransomware:** Software malicioso que secuestra información para pedir rescate. **Seguridad Digital:** Protección en el entorno digital, incluyendo ciberseguridad y ciberdefensa. **Suplantación de Identidad:** Actividades para hacerse pasar por otra persona con fines ilegales. **Vulnerabilidad:** Debilidad que facilita la acción de una amenaza
5. ABREVIATURAS.	**CCOCI**: Comando Conjunto Cibernético **ColCERT**: Grupo de Respuesta a Emergencias Cibernéticas de Colombia **CSIRT**: Equipo de Respuesta a Incidentes de Seguridad Informática **MVCT**: Ministerio de Vivienda, Ciudad y Territorio **BCP:** Plan de Continuidad de la Operación (Business Continuity Plan) **ISO/IEC:** Organización Internacional de Normalización / Comisión Electrotécnica Internacional **NIST:** Instituto Nacional de Estándares y Tecnología (National Institute of Standards and Technology) **TIC:** Tecnologías de la Información y las Comunicaciones
6. DOCUMENTOS Y REGISTROS ASOCIADOS.	1.GTI-F-07 Solicitud de Cambios: Formato utilizado para solicitar cambios en la infraestructura tecnológica del MVCT. 2. GTI-M-04 MANUAL PARA EL DESARROLLO DEL INVENTARIO Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN Acta de Reunión de Cierre de Incidente: Documento que recoge las conclusiones y decisiones tomadas tras la gestión de un incidente de seguridad. 3. Formato Informe de Incidente de Seguridad: Documento donde se detalla el análisis, contención, solución y documentación de un incidente de seguridad. 4. Correo Electrónico de Confirmación de Servicio Ejecutado: Comunicación enviada al usuario confirmando la ejecución de la solicitud de servicio, como la creación de cuentas o activación de servicios. 5.Matriz Consolidada de Activos de Información: Documento final que recoge todos los activos de información identificados y clasificados dentro del MVCT. 6. SIG-F-14 Plan de Mejoramiento: Documento que detalla las acciones de mejora identificadas tras la gestión de un incidente o proceso. 7. Acta de Reunión: Documento que recoge las lecciones aprendidas y la toma de decisiones durante el análisis post-incidente.
7. CONDICIONES GENERALES Y/O POLITICAS DE OPERACION:	**POLITICAS DE OPERACION:** 1. Los incidentes de seguridad se reportarán a la Mesa de Servicio de las siguientes maneras: •Usando el módulo de auto servicio de Aranda: http://aranda/usdkv8 •Enviando un correo a soportearanda@minvivienda.gov.co •Llamando a las extensiones 3522, 3405, o 2200. El personal que detecte un incidente debe recopilar evidencia relevante (como capturas de pantalla, correos, fotos o videos) para facilitar su análisis y resolución. 2. Una vez recibido un reporte de seguridad, el analista en la Mesa de Servicio emplea la herramienta Aranda para categorizar el incidente. Se considera un incidente de seguridad si se evidencia alguno de los siguientes criterios: daño o pérdida de información, fuga o robo de datos, robos de credenciales, modificaciones no autorizadas, suplantación de identidad, accesos no autorizados, pérdida o alteración en bases de datos, presencia de malware o ransomware, denegaciones de servicio, ciberataques, uso indebido de la imagen institucional o interrupción de servicios tecnológicos. De no cumplirse estos criterios, se manejará como un evento o incidente tecnológico. 3. Todos los incidentes de seguridad deberán estar registrados en la herramienta de gestión Aranda y en el formato GTI-F-19 Formato de Incidentes de Seguridad. 4.Una vez clasificado el incidente de seguridad este deberá ser categorizado en su impacto de acuerdo con el Impacto vs Valoración: **Catastrófico (Valoracion ALTA)**: Un incidente se considera catastrófico cuando las pérdidas económicas superan los 2000 SMLV, hay una afectación significativa a la imagen del Ministerio a nivel nacional e internacional, se incurre en sanciones de entidades como la Contraloría, Procuraduría y Fiscalía, se producen daños totales en la infraestructura del Ministerio, afecta sistemas críticos, compromete directamente el cumplimiento de los objetivos misionales del Ministerio, o impacta activos de información clasificados como de muy alto o alto impacto. **Mayor (Valoracion ALTA)**: Un incidente es clasificado como mayor si ocasiona pérdidas económicas entre 1501 a 2000 SMLV, afecta la imagen del Ministerio a nivel nacional, resulta en sanciones de entidades reguladoras, causa daños parciales a la infraestructura del Ministerio, afecta sistemas de la Oficina TIC y estaciones de trabajo con funciones críticas, o impacta activos de información de alto impacto.

7. CONDICIONES GENERALES Y/O POLITICAS DE OPERACION:	Moderado (Valoracion Media): Se cataloga un incidente como moderado cuando las perdidas economicas estan entre 1001 a 1500 SMLV, afecta la imagen de un proceso o área específica dentro del Ministerio, conlleva sanciones a nivel de la Oficina Jurídica o Control Interno, produce daños parciales en la infraestructura, afecta sistemas que dan soporte a más de una dependencia o proceso del Ministerio, provoca llamados de atención a nivel organizacional, o afecta activos de información de impacto medio. Menor (Valoracion Baja): Un incidente se considera menor si genera pérdidas económicas entre 501 a 1000 SMLV, afecta la imagen de un grupo o área a nivel del proceso, resulta en sanciones a nivel de procesos, causa daños menores en la infraestructura, afecta sistemas que apoyan a una única dependencia o proceso del Ministerio, conlleva llamados de atención a nivel de proceso, o impacta activos de información de bajo impacto. Insignificante (Valoracion Baja): Un incidente es insignificante si las pérdidas económicas son menores a 500 SMLV, afecta la imagen de un grupo a nivel de área o proceso, acarrea sanciones a nivel de grupo, causa daños pequeños en la infraestructura, afecta sistemas no críticos, provoca llamados de atención a nivel de grupo, o impacta activos de información de impacto bajo. Para el caso de la atención de incidentes de seguridad se han establecido unos tiempos máximos de atención de los mismos, con el fin de atender adecuadamente los incidentes de acuerdo con su impacto y valoración de impacto. Los tiempos expresados de acuerdo a la Urgencia, son un acercamiento al tiempo máximo en que el incidente debe ser atendido, y no al tiempo en el cual el incidente debe ser solucionado. Esto se debe a que la solución de los incidentes puede variar dependiendo del caso. URGENCIA□ **Alto**□El incidente de seguridad debe atenderse en un periodo máximo de 2 horas **Medio**□El incidente de seguridad debe atenderse en un periodo máximo de 4 horas **Bajo**□El incidente de seguridad puede atenderse en un periodo mayor a 4 horas 5. Equipos de Respuesta a Incidentes: Formados por el propietario del activo y miembros de la oficina TIC. En incidentes graves, informar a la alta gerencia y considerar la instalación de una mesa de crisis. 6. Gestión de Soluciones: Documentar soluciones efectivas en la base de datos de conocimiento de Aranda. 7. Documentación de Incidentes Graves: Los incidentes graves deben ser documentados en Aranda y reportados mediante un formato especial conforme al CSIRT de Gobierno. 8. Comunicación en Incidentes: En caso de que se requiera apoyo o se deba comunicar el incidente a entres externos, se debe consultar el documento Contacto con autoridades y grupos de interes.xlsx que se encuentra publicado en Nuestra Net en el micrositio del SGSI, en la siguiente dirección url : https://minviviendagovco.sharepoint.com/sites/SPO_NuestraNet/Dependencias/OficinaTICS/Paginas/SGSI.aspx; Lo anterior para contar con el apoyo de entes externos y así contener o dar solución al incidente presentado o en caso de que se deba informar a la autoridad competente para conocimiento de las mismas. 9. Revisión Post-Incidente: Actualizar la matriz de activos y riesgos para incorporar aprendizajes y ajustes necesarios.10 Lecciones Aprendidas: Comunicar lecciones aprendidas a todo el personal del MVCT para fortalecer la cultura de seguridad. 10. Notificación a Afectados: Informar a los afectados sobre incidentes que comprometan su información, incluyendo las medidas tomadas para su remediación. Procedimientos de Mejora:

8. DESARROLLO DEL PROCEDIMIENTO.

FLUJOGRAMA	DESCRIPCIÓN ACTIVIDAD	PUNTO DE CONTROL	RESPONSABLE / DEPENDENCIA	EVIDENCIA/ REGISTRO GENERADO
	**Actividad 1. Reportar el posible incidente de seguridad:** Identificar y reportar cualquier situación sospechosa que pueda comprometer la seguridad de la información por medio de la herramienta de gestion de servicios (Aranda).	x	Servidor Público Contratista Todas las dependencias	Correo electrónico / Tiquet Aranda
	**Actividad 2. Categorizar el Incidente de seguridad:** Evaluarlo y clasificarlo para determinar si corresponde a un incidente de seguridad o a otro tipo de incidente. SI: Es un incidente de seguridad, pasa a actividad 3 No: Pasa al procedimiento de gestion de incidentes.	x	Analistas de mesa de Servicio Coordinador GAT	Herramienta de gestión de servicios
	**Actividad 3. Escalar el incidente de seguridad**: Elevar el caso a un profesional especializado para su análisis detallado y clasificación según las políticas de seguridad. **(Politica 4) y si se clasifica como ALTO, se debe ejecutar las politicas 5 , 7 y 8**		Analistas de mesa de Servicio Oficina TIC Oficial de Seguridad de la Información	Herramienta de gestión de servicios GTI-F-19 Informe Incidentes de Seguridad de la Informacion
	**Actividad 4. Analizar causa raiz:** Investigar el origen del incidente para identificar los factores que lo causaron y decidir si es necesario implementar un plan de mejoramiento. **SI: Se requiere implementar plan de mejoramiento pasa a la actividad 13** **No: pasa a la actividad 5**	x	Oficial de Seguridad de la Información Equipo de atención del incidente Facilitador del proceso	Herramienta de gestión de servicios GTI-F-19 Informe Incidentes de Seguridad de la Informacion
	**Actividad 5. Contener el Incidente:** Implementar acciones inmediatas para controlar y minimizar el impacto del incidente mientras se trabaja en su resolución definitiva. **¿Se logró contener el incidente de seguridad?** **Si: Pasa a la actividad 6** **NO: Pasa a la actividad 4**	x	Oficial de Seguridad de la Información Equipo de atención del incidente	Herramienta de gestión de servicios GTI-F-19 Informe Incidentes de Seguridad de la Informacion
	**Actividad 6. Solucionar el Incidente de seguridad:** Realizar las acciones necesarias para erradicar las causas del incidente y restaurar la seguridad de la información afectada. **¿Se logró Solucionar el incidente de seguridad?** **Si: Pasa a la actividad 7** **NO: Pasa a la actividad 4**	x	Oficial de Seguridad de la Información Equipo de atención del incidente	Herramienta de gestión de servicios GTI-F-19 Informe Incidentes de Seguridad de la Informacion

	**Actividad 7. Documentar evidencias del inicidente de seguridad:** Recopilar y organizar todas las evidencias obtenidas durante la investigación para respaldar las acciones realizadas y facilitar auditorías futuras.		Oficial de Seguridad de la Información Equipo de atención del incidente	Herramienta de gestión de servicios GTI-F-19 Informe Incidentes de Seguridad de la Informacion
	**Actividad 8: Proteger Evidencias:** Asegurar el almacenamiento adecuado de las evidencias recopiladas para preservar su integridad y autenticidad.		Oficial de Seguridad de la Información Equipo de atención del incidente	Herramienta de gestión de servicios GTI-F-19 Informe Incidentes de Seguridad de la Informacion
	**Actividad 9. Cerrar incidente y documentar resultados:** Formalizar el cierre del incidente registrando los resultados obtenidos y las acciones implementadas en un acta de reunión.		Oficial de Seguridad de la Información Equipo de atención del incidente	Herramienta de gestión de servicios GTI-F-19 Informe Incidentes de Seguridad de la Informacion
	**Actividad 10. Revisar lecciones aprendidas:** Evaluar las acciones realizadas durante la gestión del incidente para identificar mejoras y decidir si incluirlas en la base de conocimiento organizacional.		Oficial de Seguridad de la Información Equipo de atención del incidente	Herramienta de gestión de servicios GTI-F-19 Informe Incidentes de Seguridad de la Informacion
	**Actividad 11. Notificar a afectados:** Informar a las partes interesadas sobre el impacto del incidente y las medidas tomadas para garantizar la transparencia y la confianza.	x	Oficial de Seguridad de la Información Equipo de atención del incidente	Herramienta de gestión de servicios GTI-F-19 Informe Incidentes de Seguridad de la Informacion
	**Actividad 12. Definir plan de mejoramiento:** Diseñar un plan con acciones específicas para prevenir futuros incidentes similares y fortalecer la postura de seguridad de la organización.	x	Oficial de Seguridad de la Información Facilitador del Proceso	SIG-F-14 Plan de Mejoramiento
				

8. CONTROL DE CAMBIOS

VERSIÓN	FECHA	MOTIVO DE LA MODIFICACIÓN	RESPONSABLE
1	23/08/2021	Creación del procedimiento	Lider del proceso
2	16/02/2022	Se reemplaza el logo de MINVIVIENDA 10 años	Lider del proceso
3	26/04/2022	Actualización política de operación No. 5.8	Lider del proceso
4	17/12/2024	Se aplica el flujo al procedimiento de acuerdo a los lineamientos documentales actuales y la imagen de la Entidad actual.	Lider del proceso