1. OBJETIVO:

Gestionar incidentes de ciberseguridad, seguridad de la información o continuidad tecnológica (lo que en el documento se denominará **incidentes de seguridad**), teniendo en cuenta los lineamientos y estándares definidos, a través de una oportuna identificación, atención y respuesta con el fin de mitigar el impacto asociado a la pérdida de la confidencialidad, integridad y disponibilidad de la información del Ministerio de Vivienda, Ciudad y Territorio.

2. ALCANCE:

La gestión de incidentes de seguridad inicia desde la identificación de un incidente, detección, contención y solución de este, finalizando con la documentación y lecciones aprendidas. El documento aplica a nivel de todas las sedes del MVCT.

3. DEFINICIONES:

- **Activo de Información:** En el contexto de la norma ISO/IEC 27001 es: “algo que una organización valora y por lo tanto debe proteger”. Se puede considerar como un activo de información a: Los datos creados o utilizados por un proceso de la organización en medio digital, en papel o en otros medios.
- **Amenaza:** se refiere a cualquier cosa que tenga el potencial de causar daño grave a un sistema o activo de información, una amenaza es algo que puede suceder o no, pero tiene el potencial de causar daño grave.
- **Analista de Mesa de Servicio:** Recibe la información de los Colaboradores del MVCT, registra los casos en la herramienta de mesa de servicio y es el primer contacto para la gestión de los incidentes de seguridad.
- **Ataque informático:** Conjunto de actividades realizadas por atacantes para vulnerar la seguridad informática de un sistema.
- **CCOCI:** Comando Conjunto Cibernético, Unidad Militar Conjunta (Ejército, Armada y Fuerza Aérea), que tiene como función principal prevenir, detectar, orientar, contener, decidir, responder y recuperar ante amenazas cibernéticas que afecten la sociedad, la soberanía nacional, independencia, integridad territorial, el orden constitucional y los intereses nacionales, todo esto, soportado en un marco jurídico y/o la Constitución Nacional.
- **Ciberataque:** es cualquier tipo de maniobra ofensiva hecha por individuos u organizaciones que ataquen a sistemas de información como lo son infraestructuras, redes computacionales, o bases de datos que están albergadas en servidores remotos. Estas maniobras son realizadas por medio de actos maliciosos usualmente originados de fuentes anónimas y direcciones que no pueden ser rastreadas.
- **Ciberseguridad:** ISACA: Es el proceso de proteger activos de información por medio del tratamiento de amenazas para información que es procesada, almacenada y/o transportada a través de sistemas de información interconectados.
- **Código malicioso:** Conjunto de instrucciones o códigos informáticos que se inserta en los programas de computador, tiene la capacidad de auto replicarse y usualmente porta una carga útil que afecta el funcionamiento del computador, destruye datos, altera y pone en riesgo la información.
- **COLCERT:** Por las siglas en inglés de Computer Emergency Response Team, es el Grupo de Respuesta a Emergencias Cibernéticas de Colombia, y tiene como responsabilidad central la coordinación de la Ciberseguridad y Ciberdefensa Nacional, la cual estará enmarcada dentro del Proceso Misional de Gestión de la Seguridad y Defensa del Ministerio de Defensa Nacional. Su propósito principal será la coordinación de las acciones necesarias para la protección de la infraestructura crítica del Estado colombiano frente a emergencias de Ciberseguridad que atenten o comprometan la seguridad y defensa nacional.
- **Contención de un incidente:** Son todas aquellas actividades encaminadas a reducir el impacto inmediato de un incidente de seguridad.

- **CSIRT:** Por las siglas en inglés de Computer Security Incident Response Team, es el equipo de Respuesta a Incidentes de Seguridad Informática de la Policía Nacional CSIRT-PONAL, 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.
- **Denegación del servicio:** Conjunto de actividades desarrolladas por atacantes informáticos para degradar o interrumpir el normal funcionamiento de un sistema o servicio informático.
- **Equipo de Respuesta a incidentes:** Equipo conformado por Colaboradores del MVCT y/o terceros asociados (operadores estratégicos) que cuentan con las habilidades y competencias para tratar los incidentes de seguridad durante el ciclo de vida de éstos.
- **Evento:** Ocurrencia o cambio de un conjunto particular de circunstancias. [ISO/IEC 27000:2009].
- **Evento de seguridad de la información:** Ocurrencia identificada de un sistema, servicio o estado de red que indica un posible incumplimiento de la política de seguridad de la información o falla de los controles, o una situación desconocida que puede ser relevante para la seguridad. [ISO/IEC 27000:2009].
- **Incidente de seguridad informática:** Una violación o amenaza inminente de violación de las políticas de seguridad informática, políticas de uso aceptable o políticas de seguridad y privacidad de la información. [NIST 800-61].
- **Incidente de seguridad de la información:** Es un acceso, intento de acceso, uso, divulgación, modificación o destrucción de información no autorizada; además de un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a una Política de Seguridad de la Información que atente contra la misionalidad del Ministerio.
- **Incidente de continuidad tecnológica**: Evento intencionado o no intencionado que puede afectar los servicios que presta el proceso de Tecnología de la información y de las comunicaciones.
- **Infraestructura Crítica (IC)**: Son las infraestructuras estratégicas cuyo funcionamiento es indispensable, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales. Adaptación Ley 8/2011-Gobierno de España.
- **Phishing**: Es un método que los ciberdelincuentes utilizan para engañar y conseguir que revele información personal, como contraseñas o datos de tarjetas de crédito, de la seguridad social y números de cuentas bancarias. Lo hacen mediante el envío de correos electrónicos fraudulentos o dirigiéndole a un sitio web falso.
- **Plan de continuidad de la operación (BCP. Business Continuity Plan):** Actividades documentadas que guían a la Entidad en la respuesta, recuperación, reanudación y restauración de las operaciones a los niveles predefinidos después de un incidente que afecte la continuidad de las operaciones.
- **Ransomware:** Piezas de código desarrolladas por atacantes informáticos para secuestrar información de los equipos infectados a través de técnicas criptográficas y posteriormente solicitar el pago de rescate para la recuperación de información.
- **Seguridad Digital:** Es la situación de normalidad y de tranquilidad en el entorno digital (ciberespacio), derivada de la realización de los fines esenciales del Estado mediante (i) la gestión del riesgo de seguridad digital; (ii) la implementación efectiva de medidas de ciberseguridad; y (iii) el uso efectivo de las capacidades de Ciberdefensa que demanda la voluntad social y política de las múltiples partes interesadas y de los ciudadanos del país.
- **Suplantación de identidad:** Todas aquellas actividades realizadas por la que una persona se hace pasar por otra para llevar a cabo actividades de carácter ilegal.
- **Vulnerabilidad:** Es una debilidad, atributo o falta de control que permitiría o facilitaría la actuación de una amenaza contra información clasificada, los servicios y recursos que la soportan. (CONPES 3854, pág. 87).

4. ABREVIATURAS:

- ColCERT (Grupo de Respuesta a Emergencias Cibernéticas de Colombia).
- CSIRT Gobierno (Equipo de Respuesta ante Incidencias de Seguridad Informáticas).
- CCP (Centro cibernético Policial).

5. POLÍTICAS DE OPERACIÓN:

5.1 Los posibles incidentes de seguridad y/o eventos se reportarán a la Mesa de Servicio a través de los siguientes canales:

i. A través del módulo de auto servicio de la herramienta Aranda http://aranda/usdkv8
ii. Enviando un mensaje de correo electrónico con la solicitud a la dirección soportearanda@minvivienda.gov.co
iii. Llamando a la Mesa de Servicio a las extensiones 3522, 3405, 2200.

El colaborador que identifique el posible incidente y/o evento de seguridad debe reunir la información que llevó a determinar que es un posible incidente, la cual podrá ser utilizada en la atención de este, Ejemplo: capturas de pantalla, correos electrónicos, fotografías, videos entre otros.

5.2 Una vez se reciba el reporte del posible Incidente o del evento de seguridad, el analista de la mesa de servicio debe realizar la primera categorización en la herramienta Aranda, para iniciar con la atención del mismo, si cumple con algunos de los siguientes criterios puede ser considerado como un incidente de seguridad, de lo contrario se tratará como un evento o como un incidente de tecnología.

- Hubo daño o pérdida de información física o digital.
- Hubo fuga y/o robo de información física o digital.
- Hubo robo de credencias o información mediante Phishing.
- Se presentó modificación no autorizada de la información.
- Se presentó suplantación de identidad.
- Se presentó un acceso no autorizado.
- Se presentó pérdida o alteración de registros de base de datos.
- Se presentó una pérdida de un activo de información.
- Hubo presencia de código malicioso “malware, Ransomware”.
- Se presentó una denegación del servicio.
- Se presentó algún ciberataque.
- Uso indebido de imagen institucional.
- Se presentó la suspensión de algún servicio de tecnología.

5.3 Todos los incidentes de seguridad deberán estar registrados en la herramienta de gestión Aranda.

5.4 Una vez clasificado el incidente de seguridad este deberá ser categorizado en su impacto de acuerdo con la “Tabla 1 Impacto vs Valoración”, y en su urgencia de acuerdo con la “Tabla 2 urgencia” en la herramienta de gestión Aranda.

IMPACTO	Descripción	Valoración
Catastrófico	Si el incidente que se está reportando puede generar consecuencias graves o efectos sobre la entidad a nivel de:	**ALTO**

	• Pérdidas Económicas superiores a 2000 SMLV. • Afectación de la imagen a Nivel Nacional e Internacional. • Sanciones de Contraloría, Procuraduría y Fiscalía. • Daños totales de la infraestructura del Ministerio. • Afecta a sistemas críticos. • Afecta directamente el cumplimiento de los objetivos misionales del Ministerio. • El incidente afecta activos de información considerados de impacto muy alto y alto.	
Mayor	Si el incidente que se está reportando puede generar consecuencias o efectos sobre la entidad: • Pérdidas Económicas entre 1501 a 2000 SMLV. • Afectación de la imagen a Nivel Nacional. • Sanciones de Contraloría, Procuraduría y Fiscalía. • Daños parciales de la infraestructura del Ministerio. • Afecta Sistemas de la Oficina TIC, y estaciones de trabajo con funciones críticas. • El incidente afecta activos de información considerados de impacto muy alto y alto.	
Moderado	Si el incidente que se está reportando puede generar consecuencias moderadas o efectos sobre la entidad: • Pérdidas Económicas entre 1001 a 1500 SMLV. • Afectación de la imagen del proceso o área a Nivel del Ministerio. • Sanciones a nivel de Oficina Jurídica o Control Interno. • Daños parciales de la infraestructura del Ministerio. • Afecta sistemas que apoyan más de una dependencia o proceso en el Ministerio. • Llamados de atención a nivel Organizacional. • El incidente afecta activos de información considerados de impacto medio.	**MEDIO**
Menor	Si el incidente que se está reportando puede generar consecuencias menores o efectos sobre la entidad: • Pérdidas Económicas entre 501 a 1000 SMLV. • Afectación Imagen grupo o área a nivel del proceso. • Sanciones a nivel procesos. • Daños pequeños de la infraestructura del Ministerio. • Afecta sistemas que apoyan a una sola dependencia o proceso en el Ministerio • Llamados de atención a nivel proceso. • El incidente afecta activos de información considerados de impacto bajo. Estos incidentes deben ser monitoreados con el fin de evitar un cambio en el impacto.	**BAJA**
Insignificante	Si el incidente que se está reportando puede generar consecuencias menores o efectos sobre la entidad. • Pérdidas Económicas menores a 500 SMLV. • Afectación Imagen grupo a nivel área o proceso. • Sanciones a nivel grupo. • Daños pequeños de la infraestructura del Ministerio. • Afecta sistemas no críticos, como estaciones de trabajo de usuarios con funciones no críticas. • Llamados de atención a nivel grupo. • El incidente afecta activos de información considerados de impacto bajo. Estos incidentes deben ser monitoreados con el fin de evitar un cambio en el impacto.	

Tabla 1 Impacto vs Valoración

En la anterior tabla, se muestra el impacto vs valoración del mismo, estas se entienden como las consecuencias que puede ocasionar en el Ministerio la materialización de un incidente de seguridad.

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 en la en la "Tabla No. 2 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	Descripción
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

Tabla 2 Urgencia

5.5 Los equipos de respuesta que atiendan el incidente de seguridad, estarán conformados como mínimo por el propietario y/o custodio del activo de información afectado por el incidente, y los colaboradores de la oficina TIC encargados de: Oficial de Seguridad de la Información, de la gestión de incidentes de seguridad de la información, de la Coordinación del Grupo de Apoyo Tecnológico y demás profesionales de la Oficina TIC o del proveedor de servicios tecnológicos que tengan a cargo activos o servicios que se vean afectados por el mismo.

Los equipos que se conformen podrán solicitar información o la participación de otros colaboradores de otros procesos requeridos para la atención del incidente de seguridad.

En caso que un incidente de seguridad tenga una valoración ALTO, el Oficial de Seguridad de la Información deberá informar al Líder del Sistema de Gestión de Seguridad de la Información (Jefe de la Oficina TIC), la ocurrencia de dicho evento, quien deberá informar a la Alta Gerencia, para determinar si se instala una mesa de crisis, en donde se analizará los recursos financieros, humanos y tecnológicos correspondientes a la atención del incidente, al igual evaluar las alternativas para la contención, erradicación y solución del mismo.

Es responsabilidad del Oficial de Seguridad mantener la trazabilidad del incidente desde el inicio hasta el fin.

5.6 El equipo de respuesta a incidentes identificará cuales soluciones de los incidentes deben postularse a la base de datos de conocimiento según lo establecido por la Oficina TIC.

5.7 Los incidentes de seguridad con valoración ALTO deben ser documentados en la herramienta de gestión de servicios y adicionalmente el Oficial de Seguridad de la información debe generar un reporte independiente en el formato establecido por el CSIRT de Gobierno, donde se evidencie las actividades realizadas de contención y solución. Dicho reporte debe ser enviado al Señor(a) Ministro(a) o a quien este delegue para que se determine si se da el conocer el incidente a entes externos.

5.8 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.

Se debe solicitar la atención del incidente y pedir la recolección de las evidencias digitales necesarias, con el fin de reducir la probabilidad de que estas se modifiquen después y sean consideradas no admisibles ante un ente judicial.

Dependiendo de la evidencia que se genere en el tratamiento del incidente, se determinará el lugar en donde se conservaran, por ejemplo: las evidencias producto de un incidente de seguridad de la información asociado a un ataque informático (Logs de auditoría) se almacenarán en un repositorio, el cual deberá cumplir unos requisitos mínimos de seguridad (Se determinarán de acuerdo con la clasificación de la información) para garantizar la integridad, disponibilidad y confidencialidad de esta.

5.9 Una vez se finalice el incidente se deben revisar la matriz de activos y la matriz de riesgos del proceso, con el fin de que se actualicen en caso de ser necesario.

5.10 El colaborador de la Oficina TIC que apoya la gestión de incidentes de seguridad de la información informará las lecciones aprendidas al profesional de la Oficina TIC que apoya el plan de uso y apropiación con el fin de que se comuniquen a los colaboradores del MVCT con el fin de generar conciencia entre los mismos.

5.11 Informar o notificar a los afectados sobre incidentes que afecten la confidencialidad, integridad y disponibilidad de su información, así como de las medidas adoptadas para la remediación del incidente.

5.12 Ejecutar el procedimiento SMC-P-05 Acciones Preventivas, Correctivas y de Mejora.

6. CONTENIDO:

No	Descripción	Responsable / dependencia	Evidencia	Observaciones
	Inicio			
1	Reportar el posible incidente de seguridad según Política de operación 5.1	− Todas las dependencias − Servidor Público − Contratistas	− Correo electrónico − Tiquete generado en el módulo de autoservicio de la herramienta de gestión de servicios.	Aplica política de operación 5.1
2 **P.C.**	Realizar el registro del posible incidente de seguridad y la categorización según Política de operación 5.2 ¿Es un incidente de seguridad? **SÍ:** pasa a la actividad 3 . **NO:** activar el Procedimiento de gestión de incidentes de tecnologías y finalizar el procedimiento	Analistas de mesa de Servicio / Oficina TIC	Herramienta de gestión de servicios	Aplica política de operación 5.2 sino se trata de un incidente de seguridad se debe activar el procedimiento GTI-P04 Gestión de incidentes yo requerimientos técnicos para disponibilidad de servicio.
3	Realizar el escalamiento del incidente de seguridad al Profesional de la Oficina TIC que apoya la gestión de incidentes de seguridad de la información para su análisis y clasificación.	Analistas de mesa de Servicio / Oficina TIC	Herramienta de gestión de servicios	Aplicar el Instructivo para la administración Aranda
4	Gestionar el incidente de seguridad recibido analizando y categorizando el incidente de seguridad reportado según con las políticas de operación 5.3 y 5.4. En caso de que el incidente tenga una valoración **ALTO** se deben aplicar	Oficial de Seguridad de la Información Colaborador / Oficina TIC.	Herramienta de gestión de servicios	Aplica políticas de operación 5.3, 5.4, 5.7, 5.8 y 5.9 Aplicar el Instructivo para la administración Aranda Consultar documento “Contacto con autoridades y grupos de interés”

	según políticas de operación 5.5, 5.7 y 5.8.			
5	Seleccionar el equipo de atención del incidente de seguridad. Informar a los implicados para la solución del incidente de seguridad y conformar el equipo según política de operación 5.5.	Oficial de Seguridad de la Información Colaboradores / Oficina TIC. Colaboradores del MVCT.	- Correo electrónico - Memorando - verbal con posterior documentación.	En caso de que la notificación se haga de manera verbal esa comunicación debe formalizarse a través de correo electrónico o de manera escrita Aplica política de operación 5.5
6	Analizar el incidente de seguridad. El equipo de respuesta a incidentes de seguridad realizará el análisis pertinente con el fin de identificar la causa raíz que dieron origen al incidente de seguridad. ¿se requiere definir plan de mejoramiento? **Si**: pasa a la actividad 16 **No**: pasa a la actividad 7	Oficial de Seguridad de la Información Equipo de atención del incidente Facilitador del proceso	- Formato Informe Incidente de Seguridad	Aplica política de operación 5.12
7 **P.C.**	Contener incidente de seguridad. Equipo de respuesta a incidentes de seguridad realizará todas aquellas tareas necesarias con el fin de contener el incidente de seguridad y así minimizar su impacto. ¿Se logró contener el incidente de seguridad? **Si**: pasa a la actividad 8 **No**: pasa a la actividad 6	Oficial de Seguridad de la Información Equipo de atención del incidente	- Formato Informe Incidente de Seguridad	
8 **P.C.**	Solucionar el incidente de seguridad. Equipo de atención del incidente realizará todas aquellas tareas necesarias con el fin de erradicar la cusa raíz detectada. ¿Se logró solucionar el incidente? **Si**: pasa a la actividad 9. **No: pasa a la actividad 6.**	Oficial de Seguridad de la Información Equipo de atención del incidente	- Herramienta de gestión de servicios - Formato Informe Incidente de Seguridad	
9	Documentar las evidencias del incidente de seguridad. Recopilar y organizar las evidencias producto de la investigación del incidente de seguridad.	Oficial de Seguridad de la Información Equipo de atención del incidente	- Formato Informe Incidente de Seguridad - Herramienta de gestión de servicios.	
10	Proteger las evidencias. Guardar la información recolectada	Oficial de Seguridad de la Información Equipo de atención del incidente	- Formato Informe Incidente de Seguridad	

11	Documentar el incidente de seguridad presentado.	Oficial de Seguridad de la Información Equipo de atención del incidente	- Acta de reunión cierre de incidente. - Formato Informe Incidente de Seguridad	
12	Revisar respuesta del incidente para identificar las lecciones aprendidas que serán incluidas en la base de datos de conocimiento. **¿Se postula el incidente a la base de datos de conocimiento?** **Si**: Inclusión de las lecciones aprendidas por la Oficina TIC, y continuar con la actividad 15. **No**: pasa a la actividad 15	Oficial de Seguridad de la Información Equipo de atención del incidente	- Formato acta de reunión - Correo electrónico	Aplica política de operación 5.6 y 5.10
13	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. Aplicar políticas de operación 5.9, 5.10 y 5.11	Oficial de Seguridad de la Información Colaboradores / Oficina TIC.	Acta de reunión cierre de incidente	
14	Definir plan de mejoramiento	Oficial de Seguridad de la Información Facilitador del Proceso	SIG-F-14 Plan de Mejoramiento	Aplica política de operación 5.12
	Fin			

P.C. Punto de control

7. CONTROL DE CAMBIOS:

FECHA	VERSIÓN DEL DOCUMENTO QUE MODIFICA	VERSIÓN ACTUAL DEL DOCUMENTO	MOTIVO DE LA MODIFICACIÓN
23/08/2021		1.0	Creación del procedimiento
16/02/2022	1.0	2.0	Se reemplaza el logo de MINVIVIENDA 10 años
26/04/2022	2.0	3.0	Actualización política de operación No. 5.8