	<b>GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN</b>	Código: 208-TIC-Pr-13	
		Versión: 1	Pág. 1 de 12
		Vigente desde: 23/12/2019	

## 1. OBJETIVO

Gestionar los incidentes de seguridad de la información que se materialicen al interior de la Entidad, a través de la identificación, atención y respuesta a los mismos con el fin de mitigar el impacto asociado a la pérdida de la confidencialidad, integridad y disponibilidad de la información de la Caja de la Vivienda Popular-CVP.

## 2. ALCANCE


La gestión de incidentes de seguridad de la información inicia desde la identificación de un posible incidente, detección, contención y solución del mismo, finalizando con la documentación. El procedimiento aplica a todos(as) los(as) funcionarios(as) y contratistas que tengan algún vínculo con la Entidad.

## 3. RESPONSABLES

La responsabilidad de la modificación o actualización de este procedimiento está en cabeza del Jefe de la Oficina de Tecnología de la Información y las Comunicaciones - TIC.

La responsabilidad en la gestión que se realice de los reportes de posibles incidentes de seguridad de la información que se materialicen en la Entidad, es del profesional de seguridad de la información o quien haga sus veces de la Oficina de Tecnología de la Información y las comunicaciones.

Elaboró	Revisó	Aprobó
Maryury Forero Bohorquez  Profesional Contratista Oficina TIC	Andrés Orlando Briceño Jefe de Oficina TIC	Andrés Orlando Briceño Jefe de Oficina TIC – Oficina TIC
Fecha: 23-12-2019	Fecha: 23-12-2019	Fecha: 23-12-2019

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. HÁBITAT Caja de Vivienda Popular</p>	<b>GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN</b>	Código: 208-TIC-Pr-13	
		Versión: 1	Pág. 1 de 12
		Vigente desde: 23/12/2019	

#### 4. NORMATIVIDAD

TIPO	No.	TEMA	FECHA	ORIGEN		
				Nacional	Distrital	Interna
Decreto	1008	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones	14-JUNIO-2018	X		
Resolución	3332	Actualización de la política de seguridad de la información.	16-AGO-2019			X



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
HÁBITAT  
Caja de Vivienda Popular

## GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Código: 208-TIC-Pr-13

Versión: 1

Pág. 1 de 12

Vigente desde: 23-12-2019

TIPO	No.	TEMA	FECHA	ORIGEN		
				Nacional	Distrital	Interna
Norma Técnica Colombiana	NTC/ISO-27001	Sistema De Gestión La Seguridad De La Información-SGSI es una norma colombiana que hace posible que las organizaciones aseguren la confidencialidad, integridad y disponibilidad.	11-DIC-2019	X		
Guía Técnica Colombiana	NTC-ISO/27035	Guía que brinda un enfoque estructurado y planificado para: detectar, reportar y evaluar incidentes de seguridad de la información; responder a incidentes de seguridad de la información y hacer su gestión.	12-DIC-2012	X		
Guía Técnica Colombiana	NTC-ISO/27001	Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos.	11-DIC-2013	X		



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
HÁBITAT  
Caja de Vivienda Popular

**GESTIÓN DE INCIDENTES DE  
SEGURIDAD DE LA INFORMACIÓN**


Código: 208-TIC-Pr-13

Versión: 1

Pág. 1 de 12

Vigente desde: 23/12/2019

TIPO	No.	TEMA	FECHA	ORIGEN		
				Nacional	Distrital	Interna
Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información	No.21	Esta guía entrega los lineamientos básicos para poner en marcha un Sistema de Gestión de Incidentes de Seguridad de la información, a través de un modelo propuesto, el cual está concebido para que se puedan integrar los incidentes de seguridad sobre los activos de información, independiente del medio en el que se encuentren.	06-NOV-2016	X		
CONPES	3854	Se establecen los lineamientos y directrices de seguridad digital.	07-MARZO-2017	X		

	<b>GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN</b>	Código: 208-TIC-Pr-13	
		Versión: 1	Pág. 1 de 12
		Vigente desde: 23-12-2019	

TIPO	No.	TEMA	FECHA	ORIGEN		
				Nacional	Distrital	Interna
INVENTARIO Y CLASIFICACIÓN ACTIVOS DE INFORMACIÓN	208-TIC-Ft-21	Consolidado del inventario de activos de información.	20-JUNIO-2019			X

5. DOCUMENTOS DE REFERENCIA				
Tipo de documento	Título del documento	Código	Origen	
			Externo	Interno
Política	Política de Seguridad de la Información	208-TIC-Mn-07		X

## 6. DEFINICIONES


**Activo:** Cualquier cosa que tiene valor para la organización.

**Activo de información:** Elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo. En su sentido más amplio, éstos hacen referencia a la información que se recibe, transforma y produce en la entidad u organismo distrital en el cumplimiento de sus funciones.

**Clasificación:** es la identificación y agrupamiento de características que presentan los incidentes de seguridad de la información para determinar el tratamiento de este.

**Confidencialidad:** Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

**Disponibilidad:** Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada. Un documento disponible es aquel que puede

	<b>GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN</b>	Código: 208-TIC-Pr-13	
		Versión: 1	Pág. 1 de 12
		Vigente desde: 23/12/2019	

ser localizado, recuperado, presentado e interpretado. Su presentación debe mostrar la actividad u operación que lo produjo.

**Información:** Conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

**Integridad:** Propiedad de salvaguardar la exactitud y estado completo de los activos. La integridad de un documento hace referencia a su carácter completo e inalterado. Es necesario que un documento este protegido contra modificaciones no autorizadas

**Registro:** Documento que presenta resultados obtenidos o proporciona evidencia de actividades ejecutadas.


**Seguridad de la información:** Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además puede involucrar otras propiedades tales como: autenticidad, trazabilidad (accountability), no repudio y fiabilidad.

**Evento de seguridad de la información:** presencia identificada de una condición en un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad<sup>1</sup>.

**Incidente de seguridad de la información:** evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa comprometer las operaciones del negocio y amenazar la seguridad de la información<sup>2</sup>.

<sup>1</sup> Norma Técnica Colombiana NTC-ISO-IEC 27001

<sup>2</sup> Guía Técnica Colombiana NTC-ISO-IEC 27035

 <b>ALCALDÍA MAYOR DE BOGOTÁ D.C. HÁBITAT</b> Caja de Vivienda Popular	<b>GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN</b>	Código: 208-TIC-Pr-13	
		Versión: 1	Pág. 1 de 12
		Vigente desde: 23-12-2019	

## 7. CONDICIONES GENERALES


### a) Identificación de un incidente de seguridad de la información

Es todo evento que tienen probabilidad significativa comprometer la operación normal y/o los servicios misionales prestados por la Caja de la Vivienda Popular, amenazando la triada de la información (confidencialidad, integridad y disponibilidad), por ejemplo:

- Ocurrió daño o pérdida y robo de información.
- Ocurrió hurto de credenciales o información mediante Phishing.
- Se presentó modificación no autorizada de la información.
- Se presenta un comportamiento anormal del equipo de cómputo y/o sistema de 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 de servicio.
- Se presentó algún ciber-ataque


### b) Responsabilidades

- ✓ Es responsabilidad de todos los servidores y demás partes interesadas que tengan acceso a los activos de información de la Caja de la Vivienda Popular y evidencien un posible incidente de seguridad de la información, y/o es conocedor de que alguna persona que está violando las políticas de seguridad de la información y/o conoce de riesgos asociados a la información, deberá reportar esta situación, a través del correo electrónico [soporte@cajaviviendapopular.gov.co](mailto:soporte@cajaviviendapopular.gov.co) con copia a la cuenta de correo electrónico del jefe de la Oficina de las Tecnologías de la Información y las Comunicaciones.
- ✓ Todo reporte de un posible incidente de seguridad de la información debe contener como mínimo los siguientes datos:

	<b>GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN</b>	Código: 208-TIC-Pr-13	
		Versión: 1	Pág. 1 de 12
		Vigente desde: 23/12/2019	

- Nombre del servidor o tercero que reporta
  - Teléfono de contacto
  - Correo electrónico
  - Descripción del posible incidente de seguridad, esta descripción debe reunir la información que llevó a determinar que es un posible incidente, la cual podrá ser utilizada en la atención del mismo, Ejemplo: capturas de pantalla, correos electrónicos, fotografías, videos entre otros.
- ✓ Todo reporte de un posible incidente de seguridad de la información será valorado por la mesa de ayuda, teniendo en cuenta las siguientes consideraciones al momento de realizar la asignación del caso:
- Relacionar el posible incidente con una afectación en la confidencialidad, integridad y disponibilidad de la información.
  - Reunir información básica (lugar, tipo de información, datos de contacto de la persona que reporta) que llevó a determinar que es un posible incidente de seguridad de la información, información que podrá ser utilizada en la investigación y/o para empezar a contener los daños y minimizar el riesgo.
  - Esta información se usará más adelante para documentar el incidente (ya sea real o un falso incidente).
- ✓ Todos los incidentes de seguridad de la información deben estar registrados y clasificados en la herramienta de gestión de tickets.
- ✓ El Profesional de Seguridad de la Información o quien haga sus veces documentará las acciones adelantadas para tratar el incidente. Se debe diligenciar el formato de registro de incidentes de seguridad de la información que se encuentra en la carpeta de calidad, en el cual se realiza una descripción del incidente, y detalles de cada acción tomada (quién llevó a cabo la acción, cuándo lo hizo y por qué).
- ✓ El jefe de la Oficina TIC notificará a la Dirección Jurídica los incidentes de seguridad de la información que tengan consecuencias mayores o catastróficas y que requieran trámites jurídicos.
- ✓ Para los incidentes que se presenten con documentos de archivo físico, se debe tener en cuenta las condiciones de operación y gestión definidas por la



 <b>ALCALDÍA MAYOR DE BOGOTÁ D.C. HÁBITAT</b> Caja de Vivienda Popular	<b>GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN</b>	Código: 208-TIC-Pr-13	
		Versión: 1	Pág. 1 de 12
		Vigente desde: 23-12-2019	

Subdirección Administrativa en los documentos (208-SADM-Mn-05 PROGRAMA DE GESTIÓN DOCUMENTAL -PGD V4, 208-SADM-Pr-19 CONSULTA DE DOCUMENTOS V4 y 208-SADM-Pr-33 RECONSTRUCCION EXPEDIENTES V1).

### c) Clasificación de los incidentes de seguridad de la información

Los incidentes de seguridad de la información en la CVP se clasifican, así:

Clases de incidentes de seguridad de la información	Descripción de la causa raíz	Ejemplo
Incidente de desastre natural	Por desastres naturales fuera del control humano.	Terremotos, erupciones volcánicas, inundaciones, huracanes, tormentas eléctricas, incendio forestal, tsunamis, derrumbes, etc.
Incidente de daño físico	Debido a acciones físicas accidentadas en las instalaciones de la CVP.	Incendio, agua, ambiente nefasto (contaminación, polvo, corrosión, congelamiento), destrucción de equipos, destrucción de medios, robo de equipos, robo de medios, etc.
Incidente de fallas de infraestructura tecnológica	Generado por fallas en los sistemas y servicios básicos que apoyan el funcionamiento de los sistemas de información y servicios de TI en la CVP.	Fallas en la alimentación eléctrica, en las redes, en el aire acondicionado, fallas de hardware, etc.
Incidente de código malicioso	Causas asociadas de programas maliciosos creados y divulgados en forma intencional.	Virus informáticos, gusanos de red, troyanos, malware, botnet (red de robots), ataques combinados, páginas web con códigos maliciosos, sitio hosting con códigos maliciosos, etc.



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
HÁBITAT  
Caja de Vivienda Popular

## GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN


Código: 208-TIC-Pr-13

Versión: 1

Pág. 1 de 12

Vigente desde: 23/12/2019

Clases de incidentes de seguridad de la información	Descripción de la causa raíz	Ejemplo
Incidente de ataque técnico	Resultado de ataques a sistemas de información, a través de redes u otros medios técnicos, mediante el aprovechamiento de las vulnerabilidades de los sistemas de información en cuanto a configuraciones, protocolos o programas, o por la fuerza, que genera un estado anormal de los sistemas de información.	Aprovechamiento de puertas traseras, aprovechamiento de vulnerabilidades informáticas, denegación de servicios, escaneo de redes, intentos de ingreso, interferencia, etc.
Incidente relacionado con contenidos peligrosos	Por causas asociadas de propagación de contenido indeseable a través de redes de información, lo que pone en peligro la seguridad nacional, la estabilidad social y/o la seguridad y beneficios públicos.	Contenido ilegal, contenido que provoca pánico, contenido malicioso, contenido abusivo, etc.
Incidente de puesta en riesgo de la información	La pérdida de seguridad de la información es causada al poner en riesgo en forma accidental o intencional la confidencialidad, integridad y disponibilidad de la información.	Interceptación, espionaje, "chuzada" de teléfonos, divulgación, enmascaramiento, ingeniería social, phishing de redes (Suplantación de identidad), robo de datos, alteración de datos, errores de datos, etc.

 <b>ALCALDÍA MAYOR DE BOGOTÁ D.C. HÁBITAT</b> Caja de Vivienda Popular	<b>GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN</b>	Código: 208-TIC-Pr-13	
		Versión: 1	Pág. 1 de 12
		Vigente desde: 23-12-2019	

Clases de incidentes de seguridad de la información	Descripción de la causa raíz	Ejemplo
Incidente de violación de reglas	Debido al uso no autorizado de recursos y violación de derechos de autor.	Uso de recursos de acceso para propósito no autorizado, por ejemplo, el uso del correo para participar en cadenas ilegales, pirámides, etc. Causada por la venta e instalación de copias de software sin licencia, u otros materiales protegidos por derechos de autor.


Basado en la NTC/ISO: 27035:2012

#### d) Niveles de criticidad

Se definen niveles de criticidad de acuerdo con niveles de afectación de activos de información y posibles interrupciones en la normal operación de la entidad.

Nivel	Descripción
<b>Alto</b>	Afecta la operación de la entidad, el incidente puede tener celeridad significativa/rápida en su propagación y ocasionar daños de activos. Podría llegar a afectar más de un tipo de activo.
<b>Medio</b>	Afecta por poco tiempo los procesos generales de la entidad, el incidente/evento compromete un activo importante.
<b>Bajo</b>	No afecta el normal funcionamiento de la entidad; el incidente/evento se detecta y puede controlar fácilmente con recursos existentes en la entidad.

En caso de que el incidente de seguridad de la información se considere de prioridad alto, el Profesional de Seguridad de la Información o quien haga sus veces de la

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. HÁBITAT Caja de Vivienda Popular</p>	<b>GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN</b>	Código: 208-TIC-Pr-13	
		Versión: 1	Pág. 1 de 12
		Vigente desde: 23/12/2019	

CVP deberá proponer el equipo que participará en el tratamiento del incidente y este será aprobado por el jefe de la Oficina TIC.


Los incidentes de seguridad de la información que no se consideren prioridad alto estarán liderados por el Profesional de Seguridad de la Información o quien haga sus veces.

#### e) Niveles de escalamiento

De acuerdo con el análisis, evaluación y valoración del incidente reportado, su criticidad o afectación, se prevén niveles de escalamiento tanto internos como externos.

Prioridad	Escalamiento
<b>Alto</b>	Se escala a los proveedores pertinentes y si es el caso a las autoridades externas competentes.
<b>Medio</b>	Se escala al equipo de la Oficina TIC y/o a las dependencias involucradas.
<b>Bajo</b>	Se documenta el incidente/evento en la herramienta de mesa de ayuda, o se escala al responsable del activo de información involucrado en caso de ser necesario.

DESCRIPCIÓN DEL PROCEDIMIENTO			
No.	Actividad	Responsable	Documentos/Registros
1	Los funcionarios, contratistas y demás partes interesadas, que tengan acceso a información de la entidad y evidencien un ataque a los activos de información de la entidad, y/o es conocedor de que alguna persona está violando las políticas de	Usuarios	Herramienta mesa de ayuda y/o correo electrónico.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. HÁBITAT Caja de Vivienda Popular	<b>GESTIÓN DE INCIDENTES DE  SEGURIDAD DE LA INFORMACIÓN</b>	Código: 208-TIC-Pr-13	
		Versión: 1	Pág. 1 de 12
		Vigente desde: 23-12-2019	

	seguridad de la información y/o conoce de riesgos asociados a la información, deberá reportar esta situación como un evento o incidente de seguridad de la información a través del correo de <a href="mailto:soporte@cajaviviendapopular.gov.co">soporte@cajaviviendapopular.gov.co</a>		
2	Registrar evento y/o incidente de seguridad de la información.  La mesa de ayuda registrará en la herramienta de mesa de ayuda el evento y/o incidente de acuerdo con la información suministrada; en caso de solucionar, de inmediato se documenta en una bitácora interna de gestión la solución aplicada.	Profesional mesa de ayuda	Herramienta mesa de ayuda  208-TIC-Ft-34 Registro de Incidentes de Seguridad de la Información
<b>¿Es un incidente de seguridad de la información?</b> <b>SI:</b> Continuar con la actividad 3 <b>NO:</b> Solucionar por parte de soporte técnico			
3	Escalar el incidente de seguridad de la información.  En dado caso que no se pueda resolver el incidente, se asignará el ticket al profesional de Seguridad de la Información correspondiente al segundo nivel, quien evaluará que tipo de evento y/o incidente corresponde; es el quien determina la afectación de activos, cual es alcance, que probabilidad de expansión tiene, así como los daños potenciales o reales que se generen.	Oficina TIC	Herramienta mesa de ayuda



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
HÁBITAT  
Caja de Vivienda Popular

**GESTIÓN DE INCIDENTES DE  
SEGURIDAD DE LA INFORMACIÓN**


Código: 208-TIC-Pr-13

Versión: 1


Pág. 1 de 12

Vigente desde: 23/12/2019

4	<p>Clasificar y priorizar el incidente de seguridad de la información.</p> <p>El profesional de seguridad de la información clasificará y priorizará el incidente de acuerdo con las condiciones generales de este procedimiento, para así iniciar con la evaluación y posible solución al mismo.</p>	Oficina TIC	Herramienta mesa de ayuda
5	<p>Aplicar la estrategia establecida por MINTIC para la contención, erradicación y recuperación.</p> <p>Luego del análisis y evaluación del incidente de SI, el profesional de seguridad de la información debe establecer el cómo será la contención (consiste en evitar que el incidente de seguridad de la información siga produciendo más daños a la información y/o a la plataforma tecnológica), erradicación (se debe determinar la causa raíz del incidente y eliminarla) y recuperación (luego se procede a la recuperación a través de la restauración de los sistemas y/o servicios afectados).</p>	Oficina TIC	Herramienta mesa de ayuda.
6	<p>Si al implementar la estrategia de solución implica realizar un cambio en las tecnologías de la información (actualizaciones, nuevas herramientas informáticas, etc.) se debe llevar a cabo la ejecución del mismo.</p>	Oficina TIC	Herramienta mesa de ayuda.

 <b>ALCALDÍA MAYOR DE BOGOTÁ D.C. HÁBITAT</b> Caja de Vivienda Popular	<b>GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN</b>	Código: 208-TIC-Pr-13	
		Versión: 1	Pág. 1 de 12
		Vigente desde: 23-12-2019	


7	<p>Recopilar y documentar evidencias.</p> <p>El profesional de seguridad de la información debe recopilar y documentar las evidencias producto de la investigación del incidente, las cuales son registradas en el formato de registro de incidentes de seguridad de la información.</p>	Oficina TIC	208-TIC-Ft-34 Registro de Incidentes de Seguridad de la Información
8	<p>Resolver y documentar el incidente de seguridad de la información.</p>	Oficina TIC	Herramienta mesa de ayuda 208-TIC-Ft-34 Registro de Incidentes de Seguridad de la Información
9	<p>Diligenciar el formato de registro de incidentes de seguridad de la información para actividades de lecciones aprendidas.</p>	Oficina TIC	208-TIC-Ft-34 Registro de Incidentes de Seguridad de la Información
<b>FIN DEL PROCEDIMIENTO</b>			

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. HÁBITAT Caja de Vivienda Popular</p>	<b>GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN</b>	Código: 208-TIC-Pr-13	
		Versión: 1	Pág. 1 de 12
		Vigente desde: 23/12/2019	

## 9. PUNTOS DE CONTROL

N°	Actividad	¿Qué se controla?	¿Con qué frecuencia?	¿Quién lo controla?	Riesgos Asociados
2	<p>Registrar evento y/o incidente de seguridad de la información.</p> <p>La mesa de ayuda registrará en la herramienta de mesa de ayuda el evento y/o incidente de acuerdo con la información suministrada; en caso de solucionar, de inmediato se documenta en una bitácora interna de gestión la solución aplicada.</p>	El tratamiento que se le debe dar a los incidentes de seguridad de la información es totalmente diferente a los incidentes tecnológicos.	N/A	Profesional mesa de ayuda.	Incumplimientos legales, continuidad de la operación. Pérdida de confidencialidad, integridad y disponibilidad.
3	<p>Escalar el incidente de seguridad de la información.</p> <p>En dado caso que no se pueda resolver el incidente, se asignará el ticket al profesional de Seguridad de la Información correspondiente al segundo nivel, quien evaluará que tipo de evento y/o incidente corresponde; es el quien determina la afectación de activos, cual es alcance,</p>	Que los incidentes de seguridad de la información tengan la clasificación adecuada para la documentación correspondiente.	N/A	Profesional de seguridad de la información.	



 <b>ALCALDÍA MAYOR DE BOGOTÁ D.C. HÁBITAT</b> Caja de Vivienda Popular	<b>GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN</b>	Código: 208-TIC-Pr-13	
		Versión: 1	Pág. 1 de 12
		Vigente desde: 23-12-2019	

	que probabilidad de expansión tiene, así como los daños potenciales o reales que se generen.				
--	--	--	--	--	--

**11. ANEXOS**

208-PLA-Ft-34 Registro de Incidentes de Seguridad de la Información.

<b>12. CONTROL DE CAMBIOS</b>			
<b>Versión</b>	<b>Fecha Aprobación (dd-mm-aaaa)</b>	<b>Cambios</b>	<b>Revisó Nombre(s) y apellido(s) del líder del proceso</b>
01	23-12-2019	Creación del Procedimiento	Andrés Orlando Briceño Díaz Jefe Oficina TIC