acueducto
AGUA Y ALCANTARILLADO DE BOGOTÁ

PROCEDIMIENTO	
Macro Proceso - Proceso: Gestión Técnica y Tecnológica – Gestión de Seguridad de la información	**Pagina:** 1 **de** 10
Procedimiento: Detección y atención de Incidentes de Seguridad Informática.	**Código:** FT0403P

Objetivo del Procedimiento

Determinar las actividades y responsabilidades en la atención de incidentes de seguridad informática sobre los sistemas de información de la Empresa y demás elementos de infraestructura de la red de datos de Acueducto.

Normas que Rigen el Procedimiento

- Políticas Generales de Seguridad de la Información de la Empresa de Acueducto y Alcantarillado de Bogotá.
- Resolución 305 de 2008 de la Comisión Distrital de Sistemas (CDS) de Bogotá D.C

Políticas Generales

1. El dueño del procedimiento es el Líder / Dirección de Servicios de Informática / Gerencia Tecnología, quien es el responsable de garantizar el mejoramiento continuo del procedimiento y autorizar cualquier cambio que se realice sobre este.

2. Para Acueducto se considera un evento de seguridad informática a cualquier acción o suceso observable sobre cualquiera de los recursos y/o servicios informáticos y/o sobre los sistemas de información y que se relacione con la seguridad de los mismos. Estos eventos se pueden generar a partir de acciones manuales o automatizadas, remotas o locales, ya sean intencionadas o no.

3. Para Acueducto se considera un incidente de seguridad informática a cualquier evento de seguridad informática que represente una violación a las Políticas Generales de Seguridad de la Información de la Empresa, al Acuerdo de Uso de los Recursos o a cualquier procedimiento o directiva de seguridad informática de aplicación vigente en Acueducto o que represente una amenaza inminente de afectación de la seguridad de la información y/o de la plataforma informática de la Empresa.

4. En Acueducto se establecen 10 categorías de incidentes de seguridad informática las cuales se listan a continuación. Las definiciones de estas categorías junto con los parámetros de clasificación de los eventos en cada categoría, se encuentran consignados en cada uno de los manuales de atención de incidentes de seguridad por categoría, anexos a este procedimiento. Categorías de atención de incidentes de seguridad informática:

   - FT0403M06 - Denegación de servicios.
   - FT0403M04 - Detección de exploits.
   - FT0403M07 - Violación a la propiedad intelectual.
   - FT0403M03 - Interceptación, monitoreo o análisis de tráfico.
   - FT0403M08 - Detección de intrusiones.
   - FT0403M01 - Detección de código malicioso.
   - FT0403M09 - Detección de pruebas sobre la red.
   - FT0403M02 - Violación a las políticas de seguridad.

Elaboró: William Andrés Cifuentes	**Revisó:** Álvaro Pinzón	**F. Revisión:** 25/11/2009
Dueño del Procedimiento: Líder Dirección Servicios de Informática	**Aprobó**: Elba Lucia Corredor	**F. Aprobación:** 12/02/2010

- FT0403M05 - Detección de vulnerabilidades.
- FT0403M10 - Detección de acceso no autorizado.

5. El Usuario de la Información es responsable de reportar los cambios no autorizados que detecte en la información que tenga a cargo (por ejemplo eliminación o aparición de nuevos archivos), los comportamientos anómalos o problemas en los recursos, servicios o sistemas de información que usa, así como todo posible intento o violación a la seguridad informática. Esta notificación se debe realizar al Centro de Servicio - CS / Dirección Servicios de Informática, a través de la línea 7777.

6. Para automatizar la detección y atención de incidentes de seguridad, Acueducto cuenta con la herramienta de monitoreo "Sentinel", administrada por el Grupo de Seguridad Informática / Dirección de Servicios de Informática (GSI). El objetivo de contar con la herramienta es el de poder detectar de forma automática la ocurrencia de eventos de seguridad sobre elementos de la plataforma informática considerados críticos y el de apoyar las gestión del proceso de atención de incidentes de seguridad para obtener una ejecución clara y consistente del proceso.

7. Terminología:
   - iTrac: WorkFlow de atención de incidentes generado por la herramienta Sentinel.
   - CS: Centro de Servicio / Dirección Servicios de Informática
   - ServiceCenter: Herramienta de gestión de servicios IT usada por la Dirección Servicios de Informática.
   - Exploits: Programa de computador que aprovecha las vulnerabilidades de otro programa.

Políticas Específicas (Actividad 1): Detecta Eventos.

1. El responsable de esta actividad son los Administradores de Infraestructura / Operador de Servicios de Informática y el Grupo de Seguridad de la Información - GSI.

2. Los eventos de seguridad informática en Acueducto los pueden detectar los administradores de infraestructura por cualquiera de los siguientes medios:
   - Reporte directo de los usuarios finales a través del CS.
   - Inspección manual de los registros de auditoria y seguridad.
   - Inspección manual de los registros de operación de un sistema, aplicación o elemento de infraestructura, como consumos de disco, de procesador, de memoria, de ancho de banda, etc.
   - Por alarma directa de las herramienta de monitoreo de la plataforma informática con que cuenta Acueducto (Patrol, DashBoard, Sentinel, FoundStone, IDS).

3. Los eventos reportados por los usuarios al CS, por cualquiera de los canales de comunicación, y que se categorizan como posibles eventos de seguridad, se ingresan como llamadas (requerimientos de servicio) con la categoría de incidentes de seguridad y se escalan al Administrador de Incidentes de Seguridad / Operador de Servicios de Informática para su evaluación.

4. Es responsabilidad de los administradores de la plataforma informática
   - Revisar los registros de eventos de seguridad de cada uno de los sistemas a su cargo, ya sea por inspección directa o a través de las herramientas dispuestas por Acueducto para la automatización de monitoreo de eventos.
   - Reportar los eventos que puedan representar un incidente de seguridad.
5. El grupo de seguridad de la información es responsable por detectar y reportar eventos de seguridad a través de las actividades que desarrolla y las herramientas que administra:
   - Auditorias.
   - Herramienta de atención e incidentes de seguridad – Sentinel.
   - Sistemas de Detección de intrusiones – IDS.
   - Sistemas de Prevención de Intrusiones – IPS.
   - Herramienta de identificación de vulnerabilidades – FoundStone.
6. En la clasificación de los eventos de seguridad se deben tener en cuenta los parámetros de clasificación definidos en cada unos de los manuales de atención de incidentes por categoría.

Políticas Específicas (Actividad 2): Registra Eventos.

1. El responsable de esta actividad es el Administrador de Incidentes de Seguridad / Operador de Servicios de Informática y el Grupo de Seguridad de la Información - GSI.
2. El Administrador de Incidentes de Seguridad recibe los eventos que han sido tipificados como posibles incidentes de seguridad, para investigación y evaluación de los mismos.
3. El Administrador de Incidentes de Seguridad realiza una evaluación previa y descarta los eventos que por inspección no correspondan a incidentes de seguridad. Si el evento se registró previamente en ServiceCenter se debe reclasificar como un incidente de infraestructura.
4. Si el evento escalado se considera un posible incidente de seguridad, el Administrador de Incidentes de Seguridad registra en la herramienta Sentinel el evento como un incidente en estado de "Investigación", con la descripción suministrada del evento. Si el evento se registró previamente en ServiceCenter, se cierra el caso colocando como respuesta el número del incidente generado en Sentinel.
5. El GSI tiene la potestad de registrar directamente eventos que detecte y clasifique como incidentes de seguridad. Estos eventos los debe registrar en la herramienta Sentinel como incidentes en estado de "Asignado", se les debe asignar el iTrack "Incidente de Seguridad" y deben ser asignados al Administrador de Incidentes de Seguridad para su atención.

Políticas Específicas (Actividad 3): Recolecta Información.

1. El responsable de esta actividad es el Administrador de Incidentes de Seguridad / Operador de Servicios de Informática.
2. El Administrador de Incidentes de Seguridad debe recolectar la información necesaria para poder evaluar el posible incidente de seguridad, ya sea por vía propia o solicitando directamente la información requerida para la evaluación a los Administradores de Infraestructura o a los responsables técnicos de las redes de terceros unidas a la red de Acueducto.
3. El Administrador de Incidentes de Seguridad tiene la potestad de asignar tareas específicas de recolección de información a los Administradores de Infraestructura o a los responsables técnicos de las redes de terceros unidas a la red de Acueducto.
4. La recolección de información se debe realizar de forma diligente a través de los canales de comunicación en línea como teléfono o chat, directamente con los Administradores de Infraestructura o con los responsables técnicos de las redes de terceros unidas a la red de Acueducto. Adicionalmente, se debe dejar constancia, vía correo electrónico, de la información solicitada; esta constancia se debe anexar a la documentación del incidente en la herramienta Sentinel.
5. La información que se requiera colectar en diferentes áreas al interior de la Empresa, se solicita a través del Líder de Seguridad / Dirección Servicios de Informática o de uno de los Lideres de Proceso / Dirección Servicios de Informática presente.
6. Toda la información colectada junto con los datos de la persona que reporta la información se deben adjuntar a la documentación del incidente en la herramienta Sentinel.

Políticas Específicas (Actividad 4): Evalúa Evento.

1. El responsable de esta actividad es el Administrador de Incidentes de Seguridad / Operador de Servicios de Informática.
2. Con la información colectada, el Administrador de Incidentes de Seguridad determina si el evento corresponde a un incidente de seguridad, a un falso positivo o si es un incidente de infraestructura y propone las acciones de contención y atención del incidente o invoca el manual de atención de incidentes de seguridad de la categoría correspondiente.
3. Si un evento evaluado corresponde a un incidente de seguridad, se debe actualizar el estado en la herramienta Sentinel a incidente de seguridad "Reconocido" y se deben documentar las acciones de atención o hacer referencia al manual de atención de incidentes de seguridad por categoría, si es un caso de falso positivo se actualiza el estado a incidente de seguridad "falso positivo" y se descarta el caso. Si por lo contrario el incidente es de infraestructura, se debe escalar al procedimiento "FT0302P – Gestión

de incidentes tecnologías de información y comunicación" para que sea atendido.

4. Una vez se ha reconocido un evento como incidente de seguridad informática, se debe evaluar y asignar su "Severidad" y "Prioridad" de atención en la herramienta Sentinel sobre el incidente registrado, la severidad del incidente se evalúa en función del impacto sobre los recursos afectados y la prioridad hace referencia a la celeridad con que se debe atender el incidente dados los efectos técnicos potenciales del incidente. Esta clasificación se realiza de acuerdo a las siguientes tablas:

Severidad	
Valor	**Descripción.**
None	Corresponden a eventos aislados sobre equipos de trabajo no críticos y que son de fácil atención por soporte de primer nivel. • No se afecta ningún elemento crítico de la infraestructura. • No se ven afectados los niveles de seguridad. • No se viola ninguno de los procedimientos o directivas de seguridad existentes.
Trivial	Corresponden a eventos aislados sobre equipos de trabajo no críticos y que son de fácil atención por el soporte de segundo nivel. • No se afecta ningún elemento crítico de la infraestructura. • No se ven afectados los niveles de seguridad. • No se viola ninguno de los procedimientos o directivas de seguridad existentes.
Low	• Violación menor a los procedimientos y directivas de seguridad que pueden ser fácilmente subsanados. • Se afectan elementos de la infraestructura que puedan llegar a afectar la disponibilidad de los servicios informáticos en un número reducido de usuarios. • Se ven afectados equipos de trabajo que pueden ser atendidos en sitio por soporte de segundo nivel. • No se ven afectados los niveles de seguridad.
Medium	• Violación media a los procedimientos y directivas de seguridad que requieren la intervención de usuarios para ser subsanados. • Se afecta algún elemento de la infraestructura que puede llegar a afectar la disponibilidad de los servicios informáticos a un piso o sede especifica. • Se ven afectados equipos de trabajo que requieren atención en laboratorio por soporte de segundo nivel. • No se ven afectados los niveles de seguridad informática.
High	• Violación directa a los procedimientos y directivas de seguridad. • Violación directa a los niveles de seguridad de la empresa. • Afectación parcial de la disponibilidad de los servicios informáticos críticos. • Se afectan varios equipos de trabajo que requieren la intervención de soporte de tercer nivel.
Severe	• Violación directa a las Políticas Generales de Seguridad informática. • Violación directa a los niveles de seguridad de la información critica de la empresa

	• Afectación total de la disponibilidad de los servicios informáticos críticos. • Se ven afectados masivamente equipos de trabajo.

Prioridad	
Valor	**Descripción.**
None	Se ve afectado un equipo de trabajo no crítico de forma aislada sin que represente un foco para masificación del incidente.
Low	El incidente se detecta en focos mínimos aislados y se encuentra contenido por los controles existentes.
Medium	El incidente se encuentra en múltiples focos pero está contenido por los controles existentes.
High	El incidente se encuentra en focos aislados y se requiere para la contención del incidente controles adicionales a los existentes en la plataforma y la severidad del incidente se clasificó como "Medium".
Urgent	La tasa de masificación del incidente es baja y se requiere para la contención del incidente controles adicionales a los existentes en la plataforma y la severidad del incidente se clasificó como "High".
Top	La tasa de masificación del incidente es alta y se requiere para la contención del incidente controles adicionales a los existentes en la plataforma y la severidad del incidente se clasificó como "Severe".

Políticas Específicas (Actividad 5): Informa a GSI.

1. El responsable de esta actividad es el Administrador de Incidentes de Seguridad / Operador de Servicios de Informática.
2. Todos los incidentes que se clasifiquen con severidad, "Medium", "High" o "Severe" deben ser notificados al momento de sus evaluación a los lideres del GSI, vía correo y personalmente o por vía telefónica. La no notificación es causal para declarar la atención de un incidente como no conforme.
3. El GSI tiene la potestad de intervenir en la evaluación de todos los incidentes de seguridad que se detecten o registren, así como en la asignación, definición de actividades de atención o toma de control de la coordinación de atención del mismo.

Políticas Específicas (Actividad 6): Convoca mesa de control

1. El responsable de esta actividad es el Administrador de Incidentes de Seguridad / Operador de Servicios de Informática y el Grupo de Seguridad de la Información - GSI.

2. Para todos los incidentes que se clasifiquen con severidad "High" o "Severe", el Administrador de Incidentes de Seguridad debe convocar a comité de seguridad extraordinario conformado por los Administradores de Infraestructura impactados, por el Líder y Gestor de Infraestructura y por el GSI. Este comité de seguridad ejerce el rol de "Mesa de Control" en la coordinación de atención del incídete y tiene plena potestad para asignar y ordenar las medidas de contención y atención necesarias.

3. El comité de seguridad tiene la potestad de convocar "Mesa de Control" e intervenir en el control de la coordinación de atención de todos los incidentes de seguridad activos, cuando así lo considere necesario.

Políticas Específicas (Actividad 7): Asigna Incidente.

1. El responsable de esta actividad es el Administrador de Incidentes de Seguridad / Operador de Servicios de Informática.

2. A los incidentes de seguridad confirmados el Administrador de Incidentes de Seguridad les asigna un responsable de atención en la herramienta Sentinel, quien será el encargado de ejecutar o coordinar las acciones de contención y atención del incidente. Adicionalmente debe actualizar el estado del incidente a incidente de seguridad "Asignado" y se asigna el iTrac que corresponda a la categoría del incidente para seguimiento de la atención del mismo.

3. El iTrac activado notifica al responsable de la atención del incidente que tiene un incidente nuevo para ser atendido, además que permite la actualización de información del incidente y registra el tiempo de atención del mismo.

Políticas Específicas (Actividad 8): Solicita Acciones de Contención.

1. El responsable de esta actividad es el Administrador de Incidentes de Seguridad / Operador de Servicios de Informática.

2. Si un incidente requiere la ejecución de acciones de contención para controlar su acción y propagación, estas se deben solicitar al Gestor\Líder de Infraestructura para su aplicación inmediata.

3. Se deben observar para aplicación, las acciones de contención propuestas en los manuales de atención de incidentes por categoría y las determinadas en comité de seguridad.

Políticas Específicas (Actividad 9): Ejecuta Acciones de Contención.

1. El responsable de esta actividad son los Administradores de Infraestructura / Operador de Servicios de Informática.
2. Las acciones que se aprueben para contención de la ocurrencia del incidente se deben ejecutar de forma inmediata teniendo en cuenta el impacto de las mismas en la prestación y disponibilidad del servicio.
3. La verificación de la efectividad de las acciones de contención aplicadas la realiza el Administrador de Incidentes de Seguridad en compañía del administrador(es) de plataforma que ejecuto las acciones.

Políticas Específicas (Actividad 10): Atiende Incidente.

1. El responsable de esta actividad son los Administradores de Infraestructura / Operador de Servicios de Informática.
2. Una vez contenido el incidente de seguridad se debe proceder a su atención definitiva. En la atención de los incidentes se debe seguir los manuales y planes de atención de incidentes de seguridad por categoría y las acciones solicitadas por el Administrador de Incidentes de Seguridad o por el Comité de Seguridad.
3. Las acciones de atención de incidentes que requieran cambios en la infraestructura se deben solicitar como RFCs urgentes de acuerdo al procedimiento de Gestión de Cambios de la Dirección Servicios de Informática.

Políticas Específicas (Actividad 11): Recupera Sistemas.

1. El responsable de esta actividad son los Administradores de Infraestructura / Operador de Servicios de Informática.
2. Si el incidente de seguridad causa algún tipo de alteración en los sistemas impactados, como perdida de información, daños en la configuración o caída total del sistema, se deben ejecutar los procedimientos de restauración de sistemas y restauración de backups existentes, o invocar el plan de DRP para reanudar la prestación del servicio.
3. Una vez restaurado el servicio o sistema impactado se debe verificar que el incidente de seguridad no persiste.

Políticas Específicas (Actividad 12): Informa a CS.

1. El responsable de esta actividad son los Administradores de Infraestructura / Operador de Servicios de Informática.
2. Si las acciones de contención, atención o recuperación ejecutadas generan impacto en el usuario final, el administrador(es) de infraestructura que ejecuta la acción debe informar al CS para que este pueda responder correctamente a las reclamaciones que se generen y se cuantifique el número de usuarios afectados.

Políticas Específicas (Actividad 13): Coordina Seguimiento del Incidente.

1. El responsable de esta actividad es el Administrador de Incidentes de Seguridad / Operador de Servicios de Informática.
2. Una vez atendido un incidente de seguridad, este se debe pasar al estado de "Verificado" en la herramienta Sentinel y se debe mantener monitoreo del mismo de forma que se garantice que las acciones aplicadas son definitivas y que no hay reincidencia del incidente.

Políticas Específicas (Actividad 14): Documenta Incidente.

1. El responsable de esta actividad es el Administrador de Incidentes de Seguridad / Operador de Servicios de Informática.
2. Todas las acciones que se ejecuten para contención, atención o recuperación del incidente presentado, así como el resultado de las mismas, se deben documentar en el incidente registrado en la herramienta Sentinel. La herramienta permite agregar notas o adjuntar documentos en cualquier formato.
3. Si el incidente ocurrido no está categorizado como un incidente conocido, se deben crear los planes de contención y atención para este tipo de incidente para uso en futuras ocurrencias del mismo.

Políticas Específicas (Actividad 15): Evalúa Atención.

1. El responsable de esta actividad es el grupo de Seguridad Informática / Dirección de Servicios de Informática (GSI).
2. El GSI evalúa que la documentación adjuntada como atención del incidente en la herramienta Sentinel corresponda a las acciones tomadas, que la aplicación de las actividades haya seguido el plan de trabajo acordado y que los procedimientos definidos para la realización de cambios y documentación de configuración de la infraestructura se hayan cumplido.

Políticas Específicas (Actividad 16): Reasigna Incidente.

1. El responsable de esta actividad es el grupo de Seguridad Informática / Dirección de Servicios de Informática (GSI).
2. Un incidente de seguridad podrá ser reasignado por el GSI, antes de ser cerrado, en el caso que la documentación o atención del incidente no cumpla con los estándares de atención, el incidente se reasigna al Administrador que lo atendió para cumplir con las observaciones faltantes.
3. Un incidente reasignado se mantiene en estado de incidente de seguridad "abierto" hasta tanto no se cumpla con su correcta atención y sea aprobado por el GSI.
4. Un incidente podrá ser reasignado varias veces hasta que se cumpla con su adecuada atención. Se debe mantener el indicador de las veces que se reasigno un incidente y se debe adjuntar este indicador en la documentación de atención del incidente.

Políticas Específicas (Actividad 17): Cierra Incidente.

1. El responsable de esta actividad es el grupo de Seguridad Informática / Dirección de Servicios de Informática (GSI).
2. Si el incidente cumple con los requerimientos de documentación y en la etapa de seguimiento no se presentaron reincidencias del mismo se declara como cerrado y se actualiza el estado en la herramienta Sentinel a incidente de seguridad "Cerrado".
3. Todos los incidentes generados en la herramienta Sentinel se almacenan y mantienen en la herramienta para seguimiento y futuras investigaciones y como parte de la base de datos de conocimiento.