PROCEDIMIENTO		
Proceso - Subproceso: Gestión de TIC – Gestión de Seguridad de la Información	**Página 1 de 16**	
Procedimiento: Conexión de equipos de cómputo a la red de datos de la Empresa	**Código: MPFT0203P**	**Versión: 01**

Objetivo.

Determinar las políticas y establecer las actividades a seguir para el ingreso de equipos de cómputo de la EAAB-ESP a la red de datos de la Empresa

Alcance.

Desde la solicitud de conexión de equipos a la red hasta la notificación de conexión. Abarca la conexión de equipos de cómputo, dispositivos móviles como teléfonos, PDAs, IPODs, tabletas tanto de la EAAB-ESP, como de terceros que requieran acceder a la red de la EAAB-ESP.

Términos y definiciones.

CMS: *Condiciones Mínimas de Seguridad.*
CS: *Centro de Servicio – Mesa de ayuda de* la EAAB-ESP*, línea 7777.*
GV: Grupo de control de vulnerabilidades
DA: Directorio Activo

GESTOR DE INFRAESTRUCTURA
Persona responsable por parte del contratista de gestionar todas las necesidades de relacionadas con la infraestructura informática

GRUPO DE CONTROL DE VULNERABILIDADES
Grupo de personas encargado de responder por las vulnerabilidades que se presenten en la infraestructura informática

OPERADOR SERVICIOS DE INFORMÁTICA
Grupo de personas encargadas de atender la operación sobre los equipos de cómputo de la EAAB-ESP

PERFIL DE USUARIO
Información a la que el usuario necesita acceder para el desarrollo de sus tareas, criticidad de la información, funciones del puesto, etc.

USERNAME (nombre de usuario):
Nombre único que identifica a un usuario, y es utilizado como medio de identificación ante un Sistema

USUARIO
Aquella persona natural o jurídica a la que, sin ser cliente, la entidad le presta un servicio**.**

PROCEDIMIENTO		
Proceso - Subproceso: Gestión de TIC – Gestión de Seguridad de la Información	**Página 2 de 16**	
Procedimiento: Conexión de equipos de cómputo a la red de datos de la Empresa	**Código: MPFT0203P**	**Versión: 01**

Normatividad.

- Políticas Generales de Seguridad de la Información de la EAAB-ESP.
- Resolución 305 de 2008 de la Comisión Distrital de Sistemas (CDS) de Bogotá D.C.

Políticas Generales y de Operación.

1. La Dirección de Servicios de Informática tiene entre sus funciones la de gobernar, administrar y operar la red de datos de la EAAB-ESP.

2. Los equipos de cómputo que requieran acceder a los sistemas de información de la EAAB-ESP, deben cumplir con los requisitos expuestos en el presente procedimiento, de lo contrario estos equipos no se pueden conectar a la red privada de la Empresa.

3. Este procedimiento reglamenta la conexión y desconexión de equipos de cómputo de la EAAB-ESP y Terceros a la red de datos de la EAAB-ESP.

4. Para fines de este procedimiento se consideran Terceros o Contratistas, Subcontratistas y en general toda persona natural o jurídica que tenga un vínculo contractual con la Empresa y requiera conectar un equipo de cómputo a la red de datos de la Empresa.

5. Cuando un usuario ingrese un equipo de cómputo a las instalaciones de la EAAB-ESP, la vigilancia de la Empresa debe informar lo siguiente:
   "El uso de computadores externos está permitido en las instalaciones de la Empresa de la EAAB-ESP, sin embargo, si usted requiere conectarse a la red corporativa o ingresar desde su equipo a los sistemas de información, contáctese con el Centro de Servicio en la línea 7777 donde le indicarán los pasos a seguir".

6. El usuario del equipo a conectar debe tener una razón justificada de negocio.

7. El usuario del equipo de cómputo es el directo responsable de la utilización de sus cuentas dentro de las instalaciones de la Empresa y de las actividades que desde este se generen.

8. El usuario del equipo a conectar, debe solicitar la creación de cuentas en el sistema.

9. El acceso del equipo a la red de datos será bloqueado sin previo aviso en cualquiera de los siguientes casos:
   - Detección de anomalías en la autorización de ingreso del equipo a la red.
   - Detección de uso indebido de datos y recursos informáticos a los cuales se tiene acceso a través de la red de datos.

- Detección del uso o intento de uso de recursos o datos a los cuales no tiene autorización de acceso a través de la red.
- Actividades sospechosas que violen la política de seguridad de la Empresa.

10. Antes de configurar el equipo para la conexión y uso de los servicios de red, el usuario responsable del equipo deberá permitir la revisión de las Condiciones Mínimas de Seguridad (CMS) en el equipo. del cumplimiento de estas condiciones depende la autorización de conexión del equipo.

11. Todos los responsables y usuarios de los equipos informáticos deben permitir ser incluidos en un plan de comprobación periódica de las CMS que tiene como objetivo el control del nivel de vulnerabilidades presentes en la plataforma informática de la Empresa.

12. Las desviaciones de las CMS que se detecten en los equipos de cómputo deben ser atendidas por los Terceros responsables de los equipos. La no atención de parte del Tercero de las desviaciones reportadas en el equipo, dentro de los plazos establecidos según la severidad de la vulnerabilidad, es causal de desconexión del equipo de la red de datos de la EAAB-ESP, previa notificación. Dicha medida exime de responsabilidad a la Dirección de Servicios de Informática de la EAAB-ESP ya que corresponde al Tercero.

13. A los equipos de Terceros que se conecten a la red privada de la EAAB-ESP, se les instalará el agente de la consola Antivirus de la EAAB-ESP. Otros antivirus que residan en el equipo del tercero debe ser eliminado. Esta es una condición necesaria para la autorización del ingreso a la red de datos.

    El usuario del Tercero responsable de la administración del equipo puede conservar los privilegios de administración del equipo con fines de adelantar actividades de soporte y actualización sobre el mismo, este permiso lo asigna el grupo de Soporte en Sitio afiliando la cuenta del usuario (USERNAME) del equipo al grupo “administradores” del equipo, por cuanto estos equipos de cómputo de Terceros no cuentan con soporte técnico a cargo de la EAAB-ESP.

14. Los puntos de red libres en la infraestructura de red de la EAAB-ESP se deben encontrar deshabilitados y su habilitación debe corresponder a la asignación de direcciones de red. La asignación de direcciones IP requiere de una autorización expresa de conexión de equipos y generada por el grupo de Control de Vulnerabilidades de seguridad. Es decir, el servicio no debe entregar direcciones de red libres a equipos que no se encuentren previamente y expresamente autorizados.

15. Los equipos de cómputo que se conecten a la red de datos de la EAAB-ESP, se deben afiliar observando lo descrito en el manual Manual de Directorio Activo.

16. Para efectos del presente procedimiento se entiende por equipos, cualquier elemento tecnológico: equipos de cómputo, dispositivos móviles como teléfonos, PDAs, IPODs, tabletas.

17. El Grupo de Control de Vulnerabilidades, podrá declarar incidente de seguridad las omisiones

detectadas para equipos en la red de datos.

18. Todos los equipos que se encuentren en la red de datos de la EAAB-ESP, deben estar registrados y serán objeto de vigilancia de control de vulnerabilidades.

19. Las cuentas de administración del equipo que ingresa, y las cuentas que sobre este se necesiten crear para su operación o que necesite para la integración con otros sistemas, se deben solicitar y registrar en el proceso SIMI, de acuerdo con el procedimiento MPFT0202P "Administración de Cuentas de Acceso y Autorizaciones".

20. El cambio de equipos se debe registrar como una eliminación y creación. El Responsable del PC del Tercero debe notificar al 7777 el retiro y en caso que no lo haga el equipo entrará en cuarentena durante un mes si no registra actividad en la red, luego de lo cual podrá ser desconectado sin notificación previa. Si el equipo requiere ingresar nuevamente después de este tiempo deberá ser considerado como un nuevo ingreso.

21. La conexión de equipos activos de comunicación tales como: Hubs, Switches, Access Point, Router, sin autorización no está permitida y corresponde a una falta grave a la política de seguridad de la información de la EAAB-ESP.

22. El retiro/desconexión de un equipo de la red de datos se considera un movimiento lógico y aplica para su gestión este procedimiento, con excepción de la actividad 3 y de los puntos donde se indique realizar la nueva conexión. Cuando sea un tercero quien realiza el retiro/desconexión del equipo, el interventor/gerente del proyecto debe informar al Centro de Servicios (CS) vía correo 7777@EAAB.com.co o llamada telefónica a la extensión 7777, el retiro del equipo.

23. Los equipos no pueden permanecen activos en la red mas allá de la fecha de vigencia del contrato del usuario titular de uso del equipo.

24. Cuando la cuenta de un equipo en Directorio Activo (DA) pase a estado de cuarentena (de acuerdo a los indicado en el documento "Manual de administración de Directorio Activo"), se debe eliminar la reserva de DHCP y se debe bloquear el punto de red en el cual se encontraba conectado el equipo.

25. Cuando se retire un equipo de la red de datos se debe eliminar la respectiva reserva de DCHP, de la consola EPo y se debe bloquear el punto de red en el cual se encontraba conectado el equipo. El administrador del DA debe informar periódicamente de estos cambios al Grupo de Control de Vulnerabilidades.

26. Para este procedimiento, se deben tener en cuenta los siguientes términos:
    - *CMS: Condiciones Mínimas de Seguridad.*
    - *CS: Centro de Servicio – Mesa de ayuda de* la EAAB-ESP*, línea 7777.*
    - GV: Grupo de control de vulnerabilidades

- DA: Directorio Activo

27. Si el equipo del Tercero no puede aceptar y acatar las medidas contempladas en este procedimiento entonces solo podrá acceder a los recursos y servicios informáticos de la EAAB-ESP de forma Web, es decir a través de los acceso vía Internet.

ACTIVIDADES	PUNTO DE CONTROL	RESPONSABLE (DEPENDENCIA Y CARGO)	DOCUMENTOS Y REGISTROS
1. SOLICITAR CONEXIÓN DEL EQUIPO			
1.1 Solicita a su respectivo interventor o al funcionario responsable, indicando los servicios que requiere junto con el tiempo durante el cual necesita hacer uso de estos servicios. 1.1.1 El funcionario de EAAB/interventor solicita al *Centro de Servicios* (CS) vía correo 7777@EAAB.com.co o llamada telefónica a la extensión 7777 la conexión del equipo de cómputo a la red privada. La solicitud será atendida dentro de los dos (2) días hábiles siguientes siempre y cuando el equipo se encuentre disponible para revisión en las instalaciones centrales de la EAAB-ESP y cumpla las condiciones de ingreso. 1.1.2 El operador del CS que tome la solicitud del servicio debe solicitar la siguiente información al funcionario solicitante del servicio (esta información se consigna en el formato "Formato de Ingreso/Retiro de Equipos de Terceros a la Red de Datos de la EAAB-ESP"): • Datos del funcionario solicitante/responsable o Nombre o Cargo o Registro o Teléfono o Correo • Datos del Tercero responsable o	Correo o Servicio Web Correo indicando los servicios que requiere	El Líder de proceso / Dirección de Servicios de Informática que requiera conectar un equipo de cómputo a la red privada. Interventor o responsable en la EAAB-ESP del Tercero que requiere conectar su equipo de cómputo a la red de datos de la Empresa.	Procedimiento "MPFT0202P Administración de Cuentas de Acceso y Autorizaciones". "Formato de Ingreso/Retiro de Equipos de Terceros a la Red de Datos de la EAAB-ESP

usuario del equipo o Nombre o Teléfono o Correo • Lugar de ubicación física del equipo. • Direcciones IP y MAC de las tarjetas red e Inalámbrica para equipo Portátiles de Terceros. • Nombre del equipo, el cuál debe cumplir con la nomenclatura establecida por la EAAB-ESP, de no ser así no se aprobará su conexión. • Actividad del equipo. • Servicios y aplicaciones de la EAAB-ESP a los cuales accede el equipo. • Fecha de inicio de la autorización. • Fecha de expiración de la autorización. • Observaciones. 1.1.3 El funcionario de la EAAB-ESP debe solicitar las cuentas necesarias para que el usuario del equipo de cómputo pueda acceder a los servicios informáticos de la Empresa. Esta solicitud se realiza de acuerdo al procedimiento MPFT0202P "Administración de Cuentas de Acceso y Autorizaciones". 1.1.4 Los usuarios con equipos de cómputo conectados a la red privada de la Empresa pueden solicitar de manera anticipada la desconexión del equipo (antes de finalizar el tiempo aprobado de uso de los servicios). La desconexión anticipada puede ser pedida por el funcionario que realizó la solicitud de ingreso del equipo, a través del CS vía correo 7777@EAAB.com.co o llamada telefónica a la extensión 7777. 1.1.5 La solicitud de extensión de tiempo de permanencia se debe pedir por lo menos dos (2) días hábiles antes a la fecha de terminación de la actividad o uso de los servicios indicados en el formato, para su debido trámite, registro y control. Debe ser pedida por el funcionario que realizó la solicitud de ingreso del equipo, a través del CS vía correo 7777@EAAB.com.co o llamada telefónica a la extensión 7777.			MPFT0202P "Administración de Cuentas de Acceso y Autorizaciones"

2. VALIDAR INFORMACIÓN SUMINISTRADA			
2.1 Valida que la información suministrada por el solicitante este completa, de no ser así debe informarle vía correo al solicitante para que la complete y vuelva a iniciar el procedimiento.	Correo	Grupo de Soporte en Sitio / Operador de Servicios de Informática.	
3. VERIFICAR LA EXISTENCIA DE CUENTAS DE USUARIO			
3.1 Antes de proceder con la conexión de un equipo de cómputo a la red de datos de la EAAB-ESP, El operador del CS verifica: • Que existan cuentas de usuario en algún sistema informático de la EAAB-ESP para el usuario objeto de la solicitud (usuario del equipo de cómputo a conectar). • O que exista una solicitud de cuentas de usuario aprobada para el usuario objeto de la solicitud.	Existencia de cuentas de usuario en algún sistema informático	El grupo de CS / Operador de Servicios de Informática.	
3.2 El operador del CS informa vía correo al funcionario de la EAAB-ESP que solicitó la conexión del equipo de cómputo la no existencia/solicitud de cuentas con el siguiente mensaje: "No se puede proceder con la conexión del equipo a la red de datos por cuanto no existen cuentas o solicitud de cuentas aprobadas que le permitan al usuario del equipo acceder a los servicios informáticos de la Empresa, sin la existencia de estos requisitos se considera injustificada la conexión del equipo a la red de datos. Se suspende el proceso de conexión del equipo a la red de datos hasta tanto se verifique	Correo		

que las cuentas han sido solicitadas y se encuentran en estado de aprobado."			
4. REVISAR CMS			
4.1 Revisa las Condiciones Mínimas de Seguridad (CMS) de los equipos de la EAAB-ESP cuando le es escalada la solicitud. 4.1.1 El Agente de Soporte en Sitio es responsable de remitir al correo aseguramiento@acueducto.com.co los reportes de revisiones de CMS para su evaluación. 4.1.2 Para los equipos diferentes a equipos de escritorio, el administrador del equipo es el responsable de coordinar con el Grupo de Control de Vulnerabilidades su debida revisión.	Correo con los reportes de revisiones de CMS para la evaluación.	Grupo de Soporte en Sitio / Operador de Servicios de Informática.	
5. EVALUAR CMS			
5.1 Evalúa el resultado de la comprobación de las CMS, quien califica el equipo de cómputo como "Apto" ó "No Apto" para el uso de los servicios informáticos de la EAAB-ESP. El Grupo de Control de Vulnerabilidades es responsable de la correcta evaluación de las CMS y de las condiciones en que se permita la conexión de los equipos de cómputo a la red de datos de la Empresa. Los aspectos de evaluación son los siguientes: • El sistema operativo del equipo debe estar actualizado en parches de seguridad. • No se debe encontrar en el equipo ningún	Respuesta Grupo de Control de Vulnerabilidades "*Apto*" ó "*No Apto*"	Grupo de Control de Vulnerabilidades/ Seguridad Informática / Dirección de Servicios Informáticos.	

tipo de software de código malicioso como virus, gusanos o troyanos.

- Las aplicaciones instaladas en el equipo se deben encontrar actualizadas en parches de seguridad.
- No se aceptan aplicaciones de uso prohibido en la red de datos de la EAAB-ESP, como aplicaciones de transferencia P2P, herramientas de hacking, entre otras.
- El equipo puede tener instalado un software antivirus; éste debe permanecer durante el análisis, pero no se debe considerar como un elemento de evaluación CMS. Lo anterior debido a que, una vez aceptado el equipo como apto para conectar a la red de la EAAB-ESP, éste software antivirus será eliminado y reemplazado con una licencia del software antivirus corporativo de la EAAB-ESP.

5.1.1 Un equipo de cómputo será considerado *Apto* si cumple todos los requerimientos de evaluación. Si alguno de los requerimientos no se cumple en su totalidad, se dará una calificación de *No Apto* y no se autoriza el acceso a la red de datos de la EAAB-ESP, hasta tanto no cumplan con las CMS requeridas.

5.1.2 El Grupo de Control de Vulnerabilidades notifica vía correo al grupo de Soporte en Sitio el resultado de la evaluación de seguridad del equipo, junto con el reporte de acciones de aseguramiento que se deben completar en los equipos evaluados como *No Apto* para que estos sean admitidos. El reporte debe contener:

- Nombre del equipo evaluado.
- Fecha de evaluación del equipo.
- Fallas de seguridad detectadas en la configuración del equipo:
  - Falta de actualizaciones en sistema operativo y aplicaciones.
  - Antivirus desactualizado o no instalado.
  - Software instalado con

restricción de uso en la red de datos de la EAAB-ESP. • Sobre cada una de las fallas detectadas se entrega la exigencia de solución y la descripción de aplicación de la solución. La calificación obtenida por el equipo junto con las CMS con que se aprueba la conexión de un equipo de Terceros se deben registrar en el formato "Formato de Ingreso/Retiro de Equipos de Terceros a la Red de Datos de la EAAB-ESP"			
6. NOTIFICAR RESULTADO DE EVALUACIÓN CMS			
6.1 Notifica el resultado de la evaluación del equipo de cómputo junto con el reporte de acciones de aseguramiento que se deben aplicar, en el caso de equipos calificados como "*No Apto*", las comunica el Agente de Soporte en Sitio en medio físico al responsable o al usuario del equipo. 6.1.1 Una vez solucionados los fallos, en el caso de equipos de cómputo calificados con "*No Apto"*, se podrá solicitar nuevamente la ejecución del procedimiento. 6.1.2 Para facilitarle al usuario la remediación de los fallos de seguridad, se le proporcionará un punto de conexión con acceso a Internet en la oficina del grupo de Soporte en Sitio. Se advierte que es responsabilidad del usuario el respaldo de su información, al igual que el impacto que la aplicación de la remediación pueda tener sobre la misma.	Resultado evaluación. Apto , No Apto	El grupo de Soporte en Sitio / Operador de Servicios de Informática.	
7. AJUSTAR LAS CMS			

7.1 Ajusta las CMS en los equipos calificados como "No Apto", de acuerdo a lo indicador en el reporte entregado por el Agente de Soporte en Sitio. Una vez ajustadas las CMS, el usuario podrá solicitar nuevamente la ejecución de este procedimiento.		Usuario de los equipos de cómputo cubiertos por este procedimiento, conectados a la red de datos de la EAAB-ESP.	
8. NOTIFICAR VULNERABILIDADES.			
8.1 Comunica vía correo a los usuarios solicitados por el Grupo de Control de Vulnerabilidades, el informe de estado de vulnerabilidades, con el siguiente mensaje: "Para cumplir con las condiciones mínimas de seguridad que le permitan mantener la conexión de su equipo de cómputo a la red de datos, es necesario que atienda los fallos de seguridad descritos en el documento adjunto. La no remediación de estos fallos en el tiempo asignado es causal para la desconexión del equipo."	Correo	Grupo de CS / Operador de Servicios de Informática.	
9. REMEDIAR VULNERABILIDADES			
9.1 Remedia las vulnerabilidades detectadas en su equipo y que fueron notificadas por el CS. El incumplimiento de esta actividad es causal de suspensión de la conexión del equipo a la red de datos de la Empresa.		Grupo de Soporte en Sitio / Operador de Servicios de Informática.	
10. IDENTIFICAR LUGAR Y TIPO DE CONEXIÓN			

10.1 Una vez realizada la comprobación de las CMS y con una evaluación de Apto, un Agente de Soporte en Sitio procede a identificar el tipo de conexión (físico o inalámbrico), el punto de red y la dirección MAC del equipo de cómputo, e informará al administrador de la red de datos/Operador de Servicios de Informática y al administrador del servicio DHCP/Operador de Servicios de Informática.		Grupo de Soporte en Sitio / Operador de Servicios de Informática.	
11. HABILITAR PUERTO EN EL SWITCH O ACCESS POINT			
11.1 Habilita, de acuerdo al tipo de conexión, el acceso correspondiente asociando la MAC del equipo en el dispositivo que permite el acceso.		Administrador de la infraestructura (red de datos) / Operador de Servicios de Informática.	
12. ASIGNAR RESERVA EN DHCP			
12.1 Crea la reserva en DHCP asociando la MAC del equipo de cómputo con la dirección IP asignada, de esta forma el equipo siempre toma la misma dirección IP. El servicio de DHCP no debe entregar direcciones IP libres a equipos que no se encuentren registrados.		Administrador de la infraestructura (DHCP) / Operador de Servicios de Informática.	
13. MATRICULAR EQUIPO EN EL DOMINIO			
13.1 Afilia todos los equipos de cómputo de EAAB/Terceros al dominio EAAB.RED y ubicar en la Unidad Organizacional (OU) correspondiente. Siguiendo las indicaciones del "Manual de administración de Directorio Activo" para la ubicación e identificación del equipo en el dominio.		Grupo de Soporte en Sitio / Operador de Servicios de Informática.	Manual de administración de Directorio Activo

13.2 Diligencia el registro de la realización del proceso, formato "Formato de Ingreso/Retiro de Equipos de Terceros a la Red de Datos de la EAAB-ESP", el cual se debe diligenciar por cada equipo de cómputo que ingrese a la red datos de la Empresa y se debe remitir al administrador de antivirus y al Grupo de Control de Vulnerabilidades al correo aseguramiento@acueducto.com.co. 13.3 Cualquier equipo que ingrese a la red debe ser detectado de manera automática por el sensor McAfee Rouge System(Consola EPo), instalado en el servidor DCHP.			"Formato de Ingreso/Retiro de Equipos de Terceros a la Red de Datos de la EAAB-ESP"
14. REALIZAR ESCANEOS PERIÓDICOS DE SEGURIDAD			
14.1 Realiza semanalmente una evaluación de las CMS a la totalidad de los equipos de EAAB/Terceros conectados a la red de datos de la EAAB-ESP. 14.2 El grupo de gestión de vulnerabilidades prepara un informe del estado de vulnerabilidades por cada equipo evaluado y lo remite al CS para que sea informado a los responsables de los equipos. El informe debe contener: • Equipos afectados. • Vulnerabilidades detectadas. • Descripción de las vulnerabilidades detectas en cada equipo. • Descripción de las acciones de solución por vulnerabilidad. • Tiempo máximo otorgado para la aplicación de la solución. • Fecha a partir de la cual se suspende la conexión si no han sido resueltas las vulnerabilidades. 14.3 Se considera también vulnerabilidad, cuando un equipo no tiene instalado el antivirus oficial y corporativo de la EAAB-ESP". Cuando se		El grupo de gestión de vulnerabilidades	"MPFT0201P – Atención de Vulnerabilidades Informáticas".

presente esta situación se debe incluir además de la información que contiene el informe de vulnerabilidades, la siguiente información: • Vulnerabilidad detectada (sin antivirus oficial y corporativo de la EAAB-ESP) • Descripción de la vulnerabilidad (agente y software antivirus oficial y corporativo de la EAAB-ESP son obligatorios para toda máquina conectada en la red). • Tiempo máximo otorgado para la aplicación de la solución (un día). • Fecha a partir de la cual se suspende la conexión si no han sido resuelta la vulnerabilidad (segundo día). **14.4** El Grupo de Control de Vulnerabilidades debe mantener un seguimiento continuo a la evolución del trabajo de remediación y debe notificar a los responsables de los equipos el estado de avance. La notificación se hará semanalmente, dos (2) días hábiles antes de la fecha de expiración, y el día de expiración de la ventana de tiempo de remediación y se realiza a través del CS.			
15. SOLICITAR DESCONEXIÓN DEL EQUIPO			
15.1 Solicita la desconexión de un equipo de cómputo de Terceros de la red privada de la Empresa en cualquiera de los siguientes casos: • Si transcurrido el tiempo máximo otorgado para la remediación de vulnerabilidades no se ha solucionado o argumentado la no solución de la misma. • Si en la realización periódica del escaneo de seguridad se detecta que hay equipos de cómputo con cuatro (8) semanas calendario de inactividad. • Ante incidentes de seguridad que tengan como foco los		Grupo de Control de Vulnerabilidades/ Seguridad Informática / Dirección de Servicios Informáticos	

equipos de cómputo de Terceros. • Si se detecta que la conexión del equipo de cómputo a la red de datos de la Empresa se dio sin la debida autorización. • Si dos días después, no se ha atendido la eliminación de antivirus e instalación del antivirus oficial y corporativo de la EAAB-ESP. 15.2 La desconexión de equipos debe incluir solicitud al *Centro de Servicios* (CS) vía correo 7777@acueducto.com.co. o Dirección IP, o Dirección MAC. o Nombre del equipo. 15.3La solicitud de una nueva conexión de equipos debe atenderse de acuerdo a la actividad 1 de este procedimiento.		Gerente del proyecto por parte del tercero / Interventor del contrato.	
16. DESCONECTAR EQUIPO			
16.1Para desconectar un equipo de la EAAB-ESP /Terceros de la red de datos de la Empresa es necesario: • Bloquear el puerto asignado en el Switch. • Eliminar la asociación en el dispositivo de conexión. • Liberar la reserva de IP-MAC en el DHCP. • Liberar la reserva en la consola EPo mediante correo por parte del administrador del DHCP al administrador de la consola EPo. • Notificar al CS y al Grupo de control de Vulnerabilidades de la ejecución. 16.2 Si se requiere conectar nuevamente un equipo a la red de datos deberá solicitar la ejecución de este procedimiento en su totalidad. 16.2.1 Para el caso de atención de solicitudes		Administrador de la infraestructura(Red de Datos) / Operador de Servicios de Informática.	

por novedades (vacaciones) de un funcionario. El Administrador de la Red de Datos deberá bloquear la reserva. 16.2.2 En caso que no haya una solicitud de desbloqueo y el equipo sume 8 semanas de inactividad y bloqueo el Administrador procederá según punto 16.1. 16.2.3 La desconexión de equipos de terceros por término de contrató (si no hay prorroga) se realizará automáticamente al finalizar el día que aparece como fecha de vencimiento en el carnet de ingreso del usuario.			
17. NOTIFICAR DESCONEXIÓN			
17.1 Notifica vía correo al grupo de Soporte en Sitio / Operador de Servicios de Informática y al funcionario responsable del equipo de cómputo la fecha a partir de la cual se suspende la conexión del equipo indicando el motivo por el cual se realiza la desconexión, con el siguiente mensaje: "El equipo <*nombre del equipo*> que se encuentra bajo su responsabilidad no cumple con las condiciones mínimas de seguridad necesarias para mantener la conexión a la red de datos de la Empresa, por tal motivo se suspende la prestación del servicio a partir del día <*fecha desconexión*>."	Correo	El grupo de CS / Operador de Servicios de Informática.	