PROCEDIMIENTO		
Proceso - Subproceso: Gestión de TIC - Gestión de Seguridad de la Información	**Página 1 de 5**	
Procedimiento: Atención de vulnerabilidades informáticas **Sello de protección** (Clasificación por transparencia: **público**)	**Código:** MPFT0201P	**Versión:** 02

Objetivo.

Determinar los criterios y las actividades necesarias para atender las vulnerabilidades sobre los equipos conectados a la red de datos de la EAAB-ESP, con el fin de mantener un nivel adecuado de aseguramiento de la plataforma tecnológica de la Empresa.

Alcance.

Inicia desde el descubrimiento de equipos conectados a la red de datos hasta la remediación de las vulnerabilidades detectadas en la plataforma tecnológica.

Términos y definiciones.

ADMINISTRADOR DE EQUIPO: Quién tiene los privilegios para cambiar la configuración de un equipo informático.

GESTOR DE SEGURIDAD INFORMATICA: Responsable de la operación y configuración de la seguridad de los equipos informáticos.

GRUPO DE CONTROL DE VULNERABILIDADES – GCV: Grupo que identifica y hace seguimiento a las vulnerabilidades y su remediación en la infraestructura informática.

INCIDENTE INFORMÁTICO: Evento que afecta la disponibilidad de los servicios informáticos

INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN
Cualquier evento adverso que afecte o haya afectado la seguridad de la información en cualquiera de sus atributos de Integridad, Confidencialidad y Disponibilidad.

OPERADOR SERVICIOS DE INFORMÁTICA: Grupo técnico de personas encargadas de atender la operación de los equipos informáticos en la EAAB-ESP.

RIESGO: Es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio (pérdida continuidad, imagen, incumplimiento, pérdida de ingresos, entre otros).

VULNERABILIDAD: Es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procesos de una entidad.

PROCEDIMIENTO		
Proceso - Subproceso: Gestión de TIC - Gestión de Seguridad de la Información	**Página 1 de 5**	
Procedimiento: Atención de vulnerabilidades informáticas **Sello de protección** (Clasificación por transparencia: **público**)	**Código:** MPFT0201P	**Versión:** 02

Normatividad.

- Resolución 740 de 2018 - Política General de Seguridad y Privacidad de la Información de la EAAB ESP
- Resolución 004 del 2017 de la Comisión Distrital de Sistemas (CDS) de Bogotá D.C.

Políticas Generales y de Operación

1. La totalidad de los elementos y equipos físicos o virtuales que conforman la plataforma informática y que tengan asignada una dirección IP que permita su comunicación sobre la red de datos de la EAAB-ESP, deben estar sujetos a una revisión periódica de vulnerabilidades.

2. Todo equipo que se conecte a la red de datos de la Empresa debe contar con la autorización del GCV, quien mantiene el registro de la totalidad de los equipos incluidos en el proceso de Gestión de Vulnerabilidades. Únicamente los equipos incluidos en este registro cuentan con autorización expresa (Número de autorización) de conexión a la red de datos, de acuerdo con lo contemplado en los procedimientos "MPFT0204P – Conexión de equipos a la red de datos". Las infracciones detectadas a esta política constituyen incidente de seguridad. Aplica la Excepción de número de autorización individual para los equipos ingresados masivamente al comienzo del contrato de Servicios Informáticos (periodo de transición).

3. La identificación, análisis y medición permanente de las vulnerabilidades de los equipos conectados a la red de datos de la EAAB-ESP la realiza el Grupo de Control de Vulnerabilidades -GCV- con las herramientas de detección de vulnerabilidades con que cuenta la EAAB-ESP, de la cual el GCV es responsable por su administración. Adicionalmente, el Operador de Servicios de Informática tiene la obligación de reportar otras vulnerabilidades complementarias que detecte, al GCV.

4. Es responsabilidad de los Administradores de los equipos ajustar la configuración para permitir el análisis automatizado de vulnerabilidades mediante herramientas.

5. Las vulnerabilidades que se descubran en equipo o componente de la infraestructura informática deberán ser remediados directamente por el Administrador del equipo respectivo. En caso de que haya impedimentos que no permitan su remediación el Administrador y el Operador de Servicios de Informática/Dirección Servicios de Informática deberá implementar medidas compensatorias para la disminución del riesgo asociado y demostradas con evidencia al GCV.

6. Los equipos de terceros conectados a la red de datos de la Empresa y los equipos conectados en redes de terceros que tengan comunicación directa con la red de datos de la EAAB-ESP deberán ser remediados por su Administrador técnico.

7. Si el equipo de un tercero no puede ser remediado por ausencia de su Administrador Técnico, entonces el equipo no podrá ser ingresado o mantenido dentro de la red de la EAAB-ESP y solo podrá obtener servicios informáticos de EAAB desde Internet.

8. Los equipos que se detecten conectados a la red de datos de la Empresa y que no se encuentren incluidos en el plan de escaneo periódico y no hayan sido autorizados a conectarse a la red deben ser reportados como incidentes de seguridad, para su bloqueo en la red de datos hasta tanto el GCV se autorice su conexión.

9. El GCV tiene como función priorizar las vulnerabilidades que deben ser atendidas en primer lugar y revisar el cumplimiento de las prioridades de acuerdo con el nivel de riesgo asociado.

10. En caso de presentarse un problema durante la ejecución del escaneo, el GCV junto con el administrador/responsable del equipo deben analizar los registros de la aplicación afectada y de la herramienta de escaneos de vulnerabilidades para determinar la causa del problema. El GCV junto con el administrador/ responsable del equipo deben dejar constancia vía correo al Líder de Seguridad Informática y al Gestor de Seguridad Informática sobre el problema presentado y la causa del mismo.

ACTIVIDADES	PUNTO DE CONTROL	RESPONSABLE (DEPENDENCIA Y CARGO)	DOCUMENTOS Y REGISTROS
1. IDENTIFICAR EQUIPOS			
1.1 Además de todos los equipos autorizados por GCV para conectarse a la red de datos de la Empresa se contemplan los equipos encontrados con las herramientas de descubrimiento para el análisis automatizado de vulnerabilidades.		Grupo de control de vulnerabilidades	Lista equipos aprobados MPFT0204P – Conexión de equipos a la red de datos
2. CONFIGURAR EQUIPO			
2.1. Aplica la configuración y suministra la cuenta de acceso necesaria para que el equipo pueda ser accedido y evaluado por la herramienta de escaneo de vulnerabilidades, de acuerdo con la agenda que se pacte entre las partes.		Administrador del equipo	Agenda de scan
2.2. Mantiene la configuración durante el tiempo que el equipo se encuentre conectado a la red de datos, para continuar realizando el análisis de manera efectiva y sin que cause problemas en la operación del equipo.			

3. REALIZAR ESCANEO PERIÓDICO			
3.1. Realiza escaneos periódicos de acuerdo a la agenda de escaneos acordada y divulgada para determinar el estado de aseguramiento de los equipos. Todas las actividades de escaneo, sin importar si están previamente programados, deben cumplir con el siguiente protocolo en coordinación del GCV y del Administrador/ responsable del equipo: • Antes de iniciar la actividad el GCV debe notificar al administrador/responsable del equipo central de plataforma, el inicio de la actividad. • El administrador/responsable del equipo tiene la potestad de solicitar la detención inmediata de la actividad por problemas que se presenten, o de solicitar cambiar la fecha de realización del escaneo con la correspondiente justificación. • El GCV no debe realizar escaneos que no estén previamente acordados y sin conocimiento del administrador/responsable del equipo. • Si se requiere realizar una actividad adicional se debe acordar previamente entre las dos partes. • El administrador/responsable del equipo central, debe garantizar su presencia para el acompañamiento de la actividad de escaneo.	Balance de equipos vigilados	Grupo de Control de Vulnerabilidades Administrador del equipo	Agenda de scan
4. PRESENTAR PLANES DE REMEDIACIÓN			
4.1. Presenta los planes de remediación de vulnerabilidades a las que solicite atención el GCV, de acuerdo con las prioridades y resultados obtenidos de los escaneos periódicos. Estos planes están orientados a indicar las vulnerabilidades que se van a remediar para mantener y mejorar el nivel de aseguramiento de la plataforma informática y deben ser presentados por los administradores/responsables de lo equipos para su ejecución.		Administrador del equipo	Plan de remediación

Los planes de remediación para los elementos conectados a la red de datos la EAAB-ESP se deben presentar con una frecuencia mensual al GSV.			
5. REMEDIAR VULNERABILIDADES			
5.1. Ejecuta los planes de remediación para corregir las vulnerabilidades de mayor riesgo detectadas y comunicadas por el GCV. El umbral para el nivel de cumplimiento de los planes de remediación no es inferior a la tasa de crecimiento de vulnerabilidades. El umbral debe ser atendido por cada uno de los Operadores de Servicios de Informática. Nota: La remediación de equipos de terceros, es responsabilidad del tercero. Para la remediación de las vulnerabilidades detectadas y reportadas se cuenta con la asesoría del Grupo de Control de Vulnerabilidades.		Administrador del equipo	Plan de remediación
6. PRESENTAR INDICADORES			
6.1. Calcula y presenta periódicamente los indicadores de vigilancia, vulnerabilidades, remediación de vulnerabilidades y de cumplimiento de los planes de remediación sobre la totalidad de los equipos incluidos en el proceso de gestión de vulnerabilidades.		Grupo de Control de Vulnerabilidades	