BOGOTÁ D.C.

MICHAEL BRAYAN PINILLA COY <mbpinillac@ipes.gov.co>

Solicitud de información sobre soportes de actividades de TI

2 mensajes

Hans Lwver Carlosama Alferez <hlcarlosamaa@ipes.gov.co> 17 de marzo de 2026 a las 10:16
Para: MICHAEL BRAYAN PINILLA COY <mbpinillac@ipes.gov.co>

Buenos días, Ing. Michael:

Agradezco su colaboración con la siguiente información relacionada con las actividades que se detallan a continuación.

Para cada una de ellas, por favor indicar si se cuenta con el respectivo soporte (documento, matriz, informe, reporte, propuesta, herramienta, inventario, base de datos, certificado, política, entre otros), y relacionarlo claramente.

En caso de que no se disponga de soporte para alguna actividad, agradecería informar si se tiene contemplado desarrollar durante el presente año, así como el responsable o área encargada.

Actividades:

- Identificar riesgos o vulnerabilidades de seguridad en los activos de TI.
- Implementar controles de seguridad tecnológica.
- Realizar seguimiento al cumplimiento de políticas de seguridad.
- Realizar inventario de software instalado.
- Verificar el licenciamiento y legalidad del software.
- Implementar controles frente al uso indebido de software.
- Revisar o analizar las políticas de operación tecnológica vigentes.
- Proponer actualizaciones o nuevas políticas tecnológicas.
- Socializar o implementar las políticas tecnológicas actualizadas.

Quedo atento a su amable respuesta.

Cordialmente,

--

ALCALDÍA MAYOR DE BOGOTÁ D.C. | BOGOTÁ

Hans Lwver Carlosama Alferez
Profesional Especializado
Subdirección de Diseño y Análisis Estratégico
Instituto para la Economía Social - IPES
Tel: (57) 2976030 Ext 204

MICHAEL BRAYAN PINILLA COY <mbpinillac@ipes.gov.co> 17 de marzo de 2026 a las 16:47
Para: Hans Lwver Carlosama Alferez <hlcarlosamaa@ipes.gov.co>
Cc: Adriana Villamizar Navarro <avillamizarn@ipes.gov.co>

Buen día ingeniero,

Espero que se encuentre muy bien.

En atención a su solicitud, presento a continuación el detalle de los soportes y cronogramas de las actividades relacionadas con la gestión de seguridad digital y operación tecnológica conforme al plan de tratamiento de riesgo y plan de seguridad y privacidad de la información 2026:

- **Identificar riesgos o vulnerabilidades de seguridad en los activos de TI:** La identificación técnica, correspondiente a la actividad de Gestión de Vulnerabilidades (ejecución de escaneos Nessus/OpenVAS y documentación de hallazgos), está programada para ejecutarse entre el **01/03/2026** y el **15/12/2026**. Por otro lado, la actividad de Valoración de Riesgos, enfocada en identificar, analizar y evaluar los riesgos inherentes y residuales de seguridad digital en los procesos, se llevará a cabo desde el **01/03/2026** hasta el **28/09/2026**.

- **Implementar controles de seguridad tecnológica:** La selección de los controles apropiados (basados en el Anexo A de la norma ISO 27001 de 2022) para mitigar o aceptar los riesgos se formaliza en la Definición del Plan de Tratamiento (PTR). Esta actividad de implementación y aprobación de controles se ejecutará entre el **18/04/2026** y el **30/08/2026**.

- **Realizar seguimiento al cumplimiento de políticas de seguridad:** El seguimiento estructurado se realizará en diferentes frentes y cronogramas. La recolección de datos y la Medición de Indicadores de eficacia operará desde el **31/03/2026** hasta el **01/12/2026**. El Seguimiento a Comités para verificar evidencias de cumplimiento se realizará entre el **13/06/2026** y el **18/12/2026**. Finalmente, la validación estricta de las políticas se dará mediante la Revisión Independiente (Auditoría), programada del **10/11/2026** al **30/11/2026**.

- **Realizar inventario de software instalado:** Esta acción corresponde explícitamente a la actividad de Actualización de Inventarios. Las mesas de trabajo con los líderes de procesos para actualizar los inventarios de información, software y hardware están proyectadas para iniciar el **16/03/2026** y finalizar el **29/09/2026**.

- **Verificar el licenciamiento y legalidad del software:** Esta verificación es inherente al levantamiento y control de los activos de la entidad. Por consiguiente, se acoge a los tiempos definidos para la Actualización de Inventarios de software y hardware, cuya ejecución abarca desde el **16/03/2026** hasta el **29/09/2026**.

- **Implementar controles frente al uso indebido de software:** Al igual que las demás medidas tecnológicas de restricción y protección, la implementación de controles para evitar instalaciones no autorizadas hace parte de la gestión de riesgos residuales de la entidad. Estas acciones deben quedar definidas y aprobadas en el Plan de Tratamiento (PTR) entre el **18/04/2026** y el **30/08/2026**.

- **Revisar o analizar las políticas de operación tecnológica vigentes:** El análisis y revisión metodológica inicial para integrar los lineamientos de Seguridad Digital en la política vigente, bajo la actividad de Actualización Metodológica, se realizará entre el **01/03/2026** y el **22/03/2026**. Posteriormente, la revisión para el cumplimiento del normograma institucional iniciará en **mayo**.

- **Proponer actualizaciones o nuevas políticas tecnológicas:** La estructuración oficial de las nuevas directrices se consolida en la actividad de Revisión Documental (enfocada en actualizar políticas, manuales y procedimientos del SGSI). Esta labor tiene un margen de ejecución que va desde el **01/05/2026** hasta el **17/10/2026**.

- **Socializar o implementar las políticas tecnológicas actualizadas:** La comunicación a los funcionarios se enmarca en el Plan de Cambio, Cultura y Apropiación. La ejecución de campañas, pruebas y capacitaciones generales se extenderá de forma transversal desde el **01/02/2026** hasta el **29/12/2026**. Asimismo, la actividad específica de Capacitación y Sensibilización en Riesgos para los líderes se dictará entre el **22/02/2026** y el **22/11/2026**.

Quedo atento a cualquier inquietud adicional.

Cordialmente,

Michael Brayan Pinilla Coy

[El texto citado está oculto]