



<b>GESTIÓN APOYO ADMINISTRATIVO – TECNOLOGIA DE LA INFORMACIÓN</b>	Código: TI-SS-PD-015
	Versión: 0
<b>PROCEDIMIENTO DE PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS</b>	Vigencia: 15/07/2019
	Página 1 de 3

**1. OBJETIVO**

Proteger la información y el centro de procesamiento de la Unidad Administrativa Especial Junta Central de Contadores contra software malicioso (virus, troyanos, fishing, gusanos, spayware, keyloggers, etc.).

**2. ALCANCE**

Inicia con dar cumplimiento a los lineamientos establecidos y finaliza con la verificación del cumplimiento al Manual de lineamientos de PSI en los relacionados con la protección de códigos maliciosos.

**3. DEFINICIONES**

Remitirse al anexo Glosario de términos Tecnología de la Información UAE-JCC TI-SS-GL-001.

**4. MARCO LEGAL**

(Ver Normograma)

**5. DESARROLLO**

Actividad	Descripción de la Actividad	Responsable	Punto de Control	Registro
1 ✓ Cumplir con los lineamientos	(P) Alinear los requerimientos del manual de lineamientos con el catálogo de servicios tecnológicos para adquirir o renovar las herramientas de seguridad con el fin de proteger a la Entidad del software malicioso.	Líder de Tecnología de la Información – Grupo de apoyo administrativo		Catálogo de servicios tecnológicos
2 Instalar y/o mantener actualizadas las herramientas	(H) Se instala y/o se mantiene actualizado las herramientas de seguridad como antivirus, antispam, antispyware y firewall para proteger contra software malicioso la entidad.	Apoyos de Tecnología de la Información – Grupo de apoyo administrativo		Consola de Symantc endpoint manager. Watchguard system manager y/o Watchguard UI (Firewall)
3 Controlar uso de medios	(H) Controlar que en la Entidad únicamente se utilicen medios de almacenamiento físico o en la nube de carácter institucional	Líder Seguridad y Privacidad de la Información – Grupo de		Storage Drive google



<b>GESTIÓN APOYO ADMINISTRATIVO – TECNOLOGIA DE LA INFORMACIÓN</b>	Código: TI-SS-PD-015
	Versión: 0
<b>PROCEDIMIENTO DE PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS</b>	Vigencia: 15/07/2019
	Página 2 de 3

		como el storage y el drive de google.	apoyo administrativo		
4	Controlar instalación de los navegadores	(H) Controlar que en la instalación de los navegadores se permita el procesamiento de código Java Script, aplicaciones Flash para el chat de CCSNet y Java applets para SIIF Nación	Apoyos de Tecnología de la Información – Grupo de apoyo administrativo		
5	Verificar cumplimiento del manual de lineamientos de SPI	(V)(A) Verificar que se esté cumpliendo el manual de lineamientos de SPI en lo relacionado a la protección contra códigos maliciosos	Líder Seguridad y Privacidad de la Información – Grupo de apoyo administrativo	△	

**6. FORMATOS:**

N/A

**7. DOCUMENTOS ASOCIADOS:**

- 7.1 Política de Seguridad y Privacidad de la información.
- 7.2 Manual de Lineamientos de SPI PL-SP-MO-001
- 7.3 Catálogo de servicios tecnológicos TI-SS-CA-002

**8. CONTROL DE DOCUMENTOS**

FECHA	VERSIÓN N°	NOVEDADES Y/O CAMBIOS
24/08/2018	0	Teniendo en cuenta que la Entidad se encuentra en un proceso de fortalecimiento institucional en funciones relacionadas con tecnologías de la información y las comunicaciones, cumplimiento disposiciones normativas, modificación el mapa de procesos de la Entidad, en el sentido de incluir como proceso estratégico a Tecnologías de la Información, según Resolución 000-0236 del 29 abril de 2019.

	ELABORÓ	REVISÓ	APROBÓ
<b>NOMBRE</b>	Yaneth Rangels	Eric J. Flores A.	José O. Ramirez
<b>CONTRATISTA Y/O CARGO</b>	LIDER TECNOLOGIA DE LA INFORMACIÓN – GRUPO APOYO ADMINISTRATIVO	LIDER DEL SIG - ASESOR CÓDIGO 1020 GRADO 06	DIRECTOR GENERAL CÓDIGO 0015 GRADO 16
<b>FIRMA</b>			

¡Antes de imprimir este documento, piense en el Medio Ambiente!



<b>GESTIÓN APOYO ADMINISTRATIVO – TECNOLOGIA DE LA INFORMACIÓN</b> <b>PROCEDIMIENTO DE PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS</b>	Código: TI-SS-PD-015
	Versión: 0
	Vigencia: 15/07/2019
	Página 3 de 3

**FLUJOGRAMA:**



