AvePoint

HOJA DE REFERENCIA

Gestión de la seguridad de los datos (DSPM) y NIST CSF 2.0

Guía rápida para el sector público

Con NIST CSF 2.0 y DSPM, las agencias del sector público pueden desarrollar una estrategia de defensa proactiva y preparada para el futuro que proteja lo que más importa: la confianza del público, la continuidad operativa y el éxito de la misión.

Elementos fundamentales del NIST CSF 2.0

El Marco de Ciberseguridad (CSF) del NIST proporciona una guía flexible y orientada a los resultados. La versión 2.0 introduce actualizaciones clave adaptadas al sector público:

Pilar	Novedades	Impacto
Gobernanza	Responsabilidad a nivel empresarial del riesgo cibernético	Integra la seguridad en la estrategia empresarial
Confianza cero	Modelo «Nunca confíes, verifica siempre»	Control de acceso más estricto y segmentación
Riesgo de la cadena de suministro	Responsabilidad de terceros	Limita las vulnerabilidades heredadas
Seguridad en la nube y la inteligencia artificial	Énfasis en la orientación hacia el futuro	Está en línea con los objetivos de transformación digital

Hoja de ruta para la implementación del DSPM

01. Evaluar la posición actual y las vulnerabilidades

02. Definir objetivos en línea con los objetivos empresariales y normativos

03. Desarrollar una estrategia para las políticas, la tecnología y la mitigación de riesgos

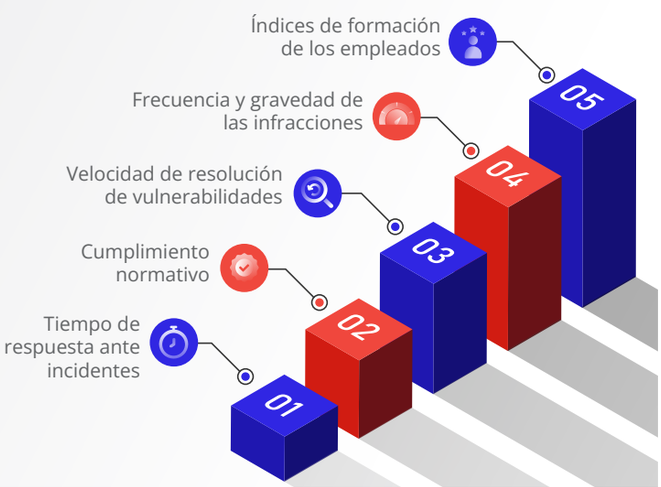
04. Implementar herramientas unificadas y automatizar siempre que sea posible

05. Formar al personal sobre los riesgos reales y los hábitos seguros

06. Supervisar y adaptarse continuamente a las amenazas en tiempo real

07. Revisar y mejorar mediante auditorías e indicadores clave de rendimiento (KPI).

Supervise el éxito con estos KPI



La seguridad cibernética es una maratón, no un sprint. AvePoint ayuda a las agencias gubernamentales a mantenerse al día.

AvePoint facilita a las organizaciones del sector público la alineación con NIST CSF 2.0 y la adopción de un enfoque proactivo de la seguridad informática.

Con AvePoint, las agencias pueden:

- **Identificar y clasificar** los datos confidenciales para garantizar una protección adecuada.
- **Aplicar el modelo de confianza cero** con controles de acceso automatizados y políticas basadas en el riesgo.
- **Detectar y responder** a las amenazas con una supervisión continua y una corrección automatizada.
- **Garantizar el cumplimiento** de las normativas en constante evolución.

Para obtener más información sobre las soluciones de AvePoint para el sector público, visite nuestro sitio web en **AvePoint.com**.

Reserve una demostración