

## RSA SECURID ACCESS



Sistema con **múltiples opciones de autenticación** para fortalecer el acceso seguro a la red corporativa. RSA SecurID Access puede ser implementado como un servicio on-premise o en la nube, y protege las aplicaciones y recursos empresariales tradicionales con una amplia gama de métodos de autenticación y políticas de acceso dinámicas y basadas en el riesgo.

Esta solución aumenta el nivel de seguridad en la validación de los usuarios con múltiples factores de autenticación, y además de usuario y password, incorpora otros mecanismos de reconocimiento (pin vía token, SMS o una validación adicional desde otros dispositivos por medio de la huella o el reconocimiento facial).

## CARACTERÍSTICAS



### Gestión de credenciales centralizada y personalizada.

Desde cualquier dispositivo, dentro y fuera de la red corporativa.



### Autenticación multifactor.

Reduce el empleo de contraseñas incluyendo múltiples factores móviles (notificación automática, contraseña de un solo uso, SMS y datos biométricos), así como tokens tradicionales y físicos para un acceso seguro.



### Control de acceso.

Aplicable en más de 500 aplicaciones locales y basadas en la nube con interoperabilidad certificada lista para usar.



### Conectividad centralizada basada en estándares.

Acceso seguro basado en políticas e inicio de sesión único, proxy inverso o bóveda de contraseñas. Permite agregar una autenticación sólida a sus aplicaciones personalizadas y de terceros utilizando una API de autenticación.



### Identidad segura.

Garantiza la identidad de los usuarios examinando una variedad de factores contextuales y correlacionarlos. Luego toma una decisión dinámica, en tiempo real, ya sea para permitir un acceso seguro o para requerir una autenticación adicional. Utiliza análisis de comportamiento de aprendizaje automático e inteligencia de amenazas para dibujar una imagen completa del usuario y una visión de 360° del riesgo asociado con su acceso.