UNMSM
Fundación
SAN MARCOS
Por el desarrollo de la Ciencia y la Cultura

DIPLOMADO DE ESPECIALIZACIÓN

GESTIÓN DE LA CIBERSEGURIDAD Y PRIVACIDAD

Digital Identity Guidelines

JULIO – OCTUBRE 2026

CENCAEP
CAPACITA

RESUMEN EJECUTIVO

Guía de Identidad Digital NIST SP 800-63-4

Nota de traducción: *Esta es una traducción/síntesis para fines académicos. La edición en inglés es la edición auténtica.*

PARTE I.

Introducción

La transformación digital ha cambiado profundamente la forma en que personas, empresas y gobiernos interactúan mediante plataformas digitales. En la actualidad, la mayoría de los servicios financieros, educativos, sanitarios, comerciales y gubernamentales requieren que los usuarios demuestren su identidad antes de acceder a información o realizar transacciones. En este contexto, la identidad digital se ha convertido en uno de los pilares fundamentales de la ciberseguridad moderna.

Sin embargo, el incremento de los servicios digitales también ha provocado un aumento significativo de amenazas como el robo de identidad, el fraude electrónico, las campañas de phishing, el uso indebido de credenciales, la suplantación de identidad y los ataques automatizados contra sistemas de autenticación. Estas amenazas afectan tanto a organizaciones públicas como privadas y representan uno de los principales desafíos para la protección de la información.

Con el propósito de establecer un marco técnico común para afrontar estos riesgos, el **National Institute of Standards and Technology (NIST)** publicó la versión **SP 800-63-4 Digital Identity Guidelines**, la cual constituye una evolución respecto de la versión anterior (SP 800-63-3). Esta nueva edición incorpora un enfoque centrado en la gestión del riesgo, la protección de la privacidad, la experiencia del usuario y la adopción de tecnologías emergentes, como las credenciales verificables, las billeteras digitales (digital wallets) y mecanismos de autenticación resistentes al phishing.

A diferencia de versiones anteriores, el documento no se limita a definir controles técnicos, sino que propone una metodología integral para diseñar sistemas de identidad digital seguros, interoperables y adaptables a distintos contextos organizacionales.

Objetivos del documento NIST SP 800-63-4

El objetivo principal del estándar es proporcionar lineamientos técnicos para que las organizaciones implementen sistemas de identidad digital que garanticen niveles adecuados de confianza durante todo el ciclo de vida de una identidad electrónica.

Las directrices abarcan tres procesos fundamentales:

- Verificación de identidad (Identity Proofing).
- Autenticación de usuarios.
- Federación de identidad entre organizaciones.

Asimismo, el documento establece requisitos relacionados con:

- Gestión de credenciales.
- Registro de usuarios.
- Administración de autenticadores.
- Protocolos de autenticación.
- Gestión de riesgos.
- Protección de datos personales.
- Privacidad.
- Interoperabilidad entre plataformas.

Estos lineamientos son aplicables principalmente a organismos gubernamentales de los Estados Unidos; sin embargo, también constituyen una referencia internacional ampliamente utilizada por empresas privadas, entidades financieras, proveedores de servicios digitales y organismos reguladores.

La identidad digital como elemento estratégico de la ciberseguridad

Uno de los aportes más relevantes del NIST SP 800-63-4 consiste en redefinir el concepto de identidad digital desde una perspectiva basada en el riesgo.

El documento señala que una identidad digital no necesariamente representa la identidad legal de una persona. En determinados servicios puede bastar con una identidad seudónima o anónima, siempre que el nivel de confianza requerido por el servicio así lo permita. En otros escenarios, especialmente aquellos relacionados con operaciones financieras, servicios públicos o acceso a información sensible, será indispensable verificar rigurosamente la identidad real del usuario.

Este enfoque rompe con el paradigma tradicional según el cual todas las aplicaciones requieren el mismo nivel de identificación.

En cambio, el NIST propone responder primero preguntas como:

- ¿Qué impacto tendría una suplantación de identidad?
- ¿Qué información se encuentra protegida?

- ¿Cuál es el riesgo para la organización?
- ¿Cuál es el riesgo para el ciudadano?
- ¿Cuál sería el impacto sobre la privacidad?

Las respuestas permiten seleccionar los mecanismos de autenticación y los niveles de aseguramiento apropiados para cada servicio.

Principales innovaciones de la versión SP 800-63-4

La edición publicada en julio de 2025 incorpora cambios importantes frente a la versión SP 800-63-3. Entre los más destacados se encuentran:

A. Gestión del riesgo basada en resultados

La nueva guía abandona un enfoque centrado exclusivamente en el cumplimiento normativo y propone una metodología orientada a resultados. Esto implica que las organizaciones deben analizar sus amenazas específicas, identificar los riesgos asociados y seleccionar controles proporcionales a dichos riesgos, en lugar de aplicar un conjunto uniforme de requisitos.

B. Protección frente al fraude digital

El estándar incorpora nuevas medidas para reducir el fraude relacionado con la identidad, incluyendo mecanismos para prevenir ataques automatizados durante el proceso de registro, autenticadores resistentes al phishing y mejores prácticas para combatir el robo de credenciales.

C. Integración de nuevas tecnologías

La guía contempla tecnologías emergentes como:

- Licencias de conducir digitales.
- Credenciales verificables.
- Billeteras digitales controladas por el usuario.
- Arquitecturas modernas de identidad federada.

Estas tecnologías buscan ofrecer una mayor seguridad y facilitar la interoperabilidad entre diferentes organizaciones y plataformas.

D. Privacidad desde el diseño

La privacidad deja de ser un aspecto complementario para convertirse en un requisito transversal. Las organizaciones deben minimizar la recopilación de datos personales, proteger la información durante todo su ciclo de vida y comunicar de manera transparente el tratamiento de los datos.

PARTE 2

Modelo de Identidad Digital del NIST SP 800-63-4

1. El Modelo de Identidad Digital

Uno de los principales aportes del **NIST SP 800-63-4** consiste en definir un modelo de identidad digital flexible que pueda adaptarse a diferentes organizaciones, tecnologías y arquitecturas de autenticación. En lugar de imponer una única forma de implementar la identidad digital, el estándar describe un conjunto de funciones y responsabilidades que pueden ser desempeñadas por una o varias entidades, dependiendo de la infraestructura tecnológica de cada organización.

Este enfoque permite que tanto una institución pública como una entidad financiera o una empresa privada implementen soluciones de identidad digital ajustadas a sus necesidades operativas y a su nivel de riesgo.

El modelo parte de un principio fundamental: **la identidad digital no es un dato aislado, sino un proceso continuo que abarca el registro del usuario, la verificación de su identidad, la autenticación durante el acceso y la administración permanente de sus credenciales**.

Por ello, el NIST divide el ciclo de vida de la identidad digital en tres grandes procesos:

- Prueba de identidad y registro (Identity Proofing and Enrollment).
- Autenticación y administración de autenticadores.
- Federación de identidad e intercambio de atributos.

Estos procesos conforman el núcleo del modelo de identidad digital y constituyen la base sobre la cual se diseñan los sistemas modernos de autenticación segura.

1.1 Roles dentro del Modelo de Identidad Digital

Uno de los aspectos más importantes del estándar es la definición clara de los actores que participan en el proceso de identidad digital. Cada uno cumple funciones específicas y contribuye al establecimiento de la confianza entre el usuario y el servicio digital.

El Sujeto (Subject)

El término **Subject** hace referencia a la persona natural cuya identidad será gestionada dentro del sistema. Dependiendo de la etapa del proceso, el sujeto puede asumir tres roles diferentes:

Applicant

Es la persona que solicita incorporarse al sistema de identidad digital.

Durante esta etapa todavía no existe confianza sobre su identidad.

El solicitante deberá presentar documentos, evidencias y atributos personales que permitan verificar quién es realmente.

Ejemplos:

- Un ciudadano que solicita crear una cuenta en un portal gubernamental.
- Un cliente que abre una cuenta bancaria digital.
- Un estudiante que solicita acceso a una universidad virtual.

Subscriber

Una vez que la organización verifica satisfactoriamente la identidad del solicitante, éste se convierte en **Subscriber**.

En esta fase ya existe una cuenta oficial dentro del sistema y se asocian uno o varios autenticadores.

El Subscriber será responsable de proteger sus credenciales y cumplir las políticas establecidas por la organización.

Claimant

Cada vez que el usuario intenta ingresar al sistema deja de actuar como Subscriber y pasa temporalmente a ser **Claimant**.

En ese momento debe demostrar que realmente posee los autenticadores registrados.

Por ejemplo:

- Introducir una contraseña.
- Utilizar una llave criptográfica.

- Aprobar una autenticación biométrica combinada con otro factor.

Una vez validada su identidad vuelve a actuar como Subscriber durante la sesión autenticada.

1.2 El Credential Service Provider (CSP)

El **Credential Service Provider (CSP)** constituye uno de los componentes más importantes del modelo de identidad digital.

Su responsabilidad consiste en administrar el ciclo de vida completo de las credenciales digitales.

Entre sus principales funciones destacan:

- verificar la identidad del solicitante;
- registrar nuevos usuarios;
- crear cuentas de suscriptores;
- asociar autenticadores a cada usuario;
- mantener actualizada la información del suscriptor;
- administrar el estado de las credenciales;
- gestionar la recuperación de cuentas.

En términos prácticos, el CSP representa la autoridad que certifica que una determinada identidad digital pertenece realmente a una persona específica.

Sin un CSP confiable, todo el sistema de autenticación pierde credibilidad.

1.3 El Verifier

El **Verifier** tiene la función de comprobar que quien intenta autenticarse realmente posee el autenticador registrado.

Para ello utiliza protocolos criptográficos capaces de validar la autenticidad del autenticador presentado.

Es importante comprender que el Verifier **no determina quién es la persona**.

Su función consiste únicamente en comprobar que el usuario controla el autenticador asociado previamente durante el proceso de registro.

Este mecanismo reduce considerablemente las posibilidades de suplantación de identidad.

1.4 El Relying Party (RP)

El **Relying Party (RP)** corresponde al sistema o aplicación que ofrece el servicio digital.

Ejemplos:

- un portal tributario;
- una plataforma bancaria;
- un sistema de historia clínica electrónica;
- un campus virtual.

El RP no realiza directamente la verificación de identidad.

En cambio, **confía en las afirmaciones (assertions)** emitidas por el Verifier o por el proveedor de identidad.

Cuando recibe una autenticación satisfactoria, concede acceso al recurso solicitado.

Esta separación de responsabilidades permite construir arquitecturas mucho más seguras y escalables.

1.5 El Identity Provider (IdP)

Cuando la organización utiliza un modelo federado aparece una nueva entidad denominada **Identity Provider (IdP)**.

El IdP administra las credenciales principales del usuario y genera afirmaciones digitales (Assertions) que otras organizaciones pueden aceptar.

Gracias al IdP un usuario puede autenticarse una sola vez y acceder posteriormente a múltiples servicios sin volver a introducir sus credenciales.

Este mecanismo constituye la base del conocido **Single Sign-On (SSO)**.

Además de mejorar la experiencia del usuario, reduce la proliferación de contraseñas y facilita la administración centralizada de identidades.

2. Proceso de Prueba de Identidad (Identity Proofing)

La prueba de identidad constituye el primer paso para establecer confianza entre una persona y un sistema digital.

Durante esta fase el CSP solicita información que permita verificar que el solicitante realmente es quien afirma ser.

Dependiendo del nivel de aseguramiento requerido, la organización podrá exigir:

- Documento nacional de identidad.
- Pasaporte.
- Licencia de conducir.
- Datos biométricos.
- Evidencia documental.
- Verificación presencial o remota.

Posteriormente el CSP ejecuta tres actividades fundamentales:

Resolución de identidad: determina si la persona es única dentro del sistema.

Validación: comprueba la autenticidad de los documentos presentados.

Verificación: confirma que los atributos pertenecen efectivamente al solicitante.

Solo cuando estas tres etapas finalizan exitosamente el usuario puede ser registrado como Subscriber.

2.1 Registro (Enrollment)

Después de completar la prueba de identidad comienza el proceso denominado **Enrollment**.

Durante esta etapa el CSP crea oficialmente la cuenta del usuario.

Asimismo:

- asigna un identificador único;
- registra atributos personales;
- vincula autenticadores;

- almacena la información necesaria para futuras autenticaciones.

Desde este momento la identidad digital queda oficialmente establecida dentro del sistema.

El estándar destaca que el suscriptor tiene la responsabilidad de proteger sus autenticadores frente a pérdida, robo o uso indebido y de cumplir las políticas definidas por el CSP para conservar la validez de su cuenta.

PARTE 3

Autenticación Digital y Niveles de Aseguramiento según el NIST SP 800-63-4

1. La autenticación digital

Una vez que la identidad del usuario ha sido verificada y registrada, el siguiente desafío consiste en garantizar que cada intento de acceso sea realizado por el titular legítimo de la identidad digital. Para ello, el NIST SP 800-63-4 define la **autenticación** como el proceso mediante el cual un usuario demuestra el control de uno o más autenticadores previamente registrados durante el proceso de inscripción.

Es importante diferenciar dos conceptos que con frecuencia se confunden:

- **Verificación de identidad (Identity Proofing):** confirma quién es la persona antes de crear su identidad digital.
- **Autenticación (Authentication):** confirma que quien intenta acceder es el titular de la identidad previamente registrada.

Esta diferencia es esencial, ya que un usuario puede haber demostrado correctamente su identidad durante el registro, pero posteriormente perder el control de sus credenciales o ser víctima de un ataque de suplantación. Por ello, la autenticación debe realizarse cada vez que se solicita acceso a un sistema o recurso protegido.

El estándar enfatiza que la autenticación no debe considerarse un evento aislado, sino un proceso continuo que puede requerir nuevas verificaciones durante la sesión cuando cambian las condiciones de riesgo, como el uso de un nuevo dispositivo, una ubicación geográfica inusual o un comportamiento anómalo del usuario.

1.1 Factores de autenticación

El NIST clasifica los autenticadores en función de la evidencia utilizada para demostrar la identidad del usuario. Tradicionalmente, estos factores se agrupan en tres categorías:

a) Algo que el usuario conoce

Corresponde a información que únicamente debería conocer el usuario legítimo. Algunos ejemplos son:

- Contraseñas.
- Números de identificación personal (PIN).
- Frases secretas.

Aunque continúan siendo ampliamente utilizadas, las contraseñas presentan limitaciones importantes. Los usuarios suelen reutilizarlas en múltiples servicios, elegir combinaciones fáciles de adivinar o almacenarlas de forma insegura, lo que incrementa el riesgo de ataques de fuerza bruta, diccionario o reutilización de credenciales.

b) Algo que el usuario posee

Este factor se basa en la posesión de un dispositivo físico previamente registrado. Entre los ejemplos más comunes se encuentran:

- Llaves criptográficas de hardware (FIDO2).
- Tokens OTP.
- Tarjetas inteligentes.
- Aplicaciones autenticadoras instaladas en dispositivos móviles.

La ventaja de este enfoque es que un atacante no puede autenticarse únicamente conociendo la contraseña; también necesita acceder físicamente al dispositivo registrado.

c) Algo que el usuario es

Este factor utiliza características biométricas propias del individuo, tales como:

- Huella dactilar.
- Reconocimiento facial.
- Iris.
- Reconocimiento de voz.

El NIST aclara que la biometría no debe emplearse como único mecanismo de autenticación en niveles elevados de seguridad, sino como complemento de otro factor, ya que las características biométricas no pueden modificarse si resultan comprometidas.

1.2 Autenticación Multifactor (MFA)

Uno de los pilares de la versión SP 800-63-4 es la recomendación de utilizar **Autenticación Multifactor (Multi-Factor Authentication, MFA)** para reducir significativamente el riesgo de acceso no autorizado.

La MFA combina dos o más factores de autenticación pertenecientes a categorías diferentes. Por ejemplo:

- Contraseña + aplicación autenticadora.
- Contraseña + llave FIDO2.
- PIN + tarjeta inteligente.
- Llave criptográfica + verificación biométrica.

Este enfoque incrementa considerablemente la seguridad, ya que un atacante necesitaría comprometer simultáneamente varios mecanismos independientes para obtener acceso.

El estándar resalta que la autenticación multifactor representa actualmente una de las medidas más eficaces para mitigar ataques de robo de credenciales y suplantación de identidad.

1.3 Autenticadores resistentes al phishing

Uno de los cambios más relevantes introducidos por la versión SP 800-63-4 es la incorporación de mecanismos específicamente diseñados para resistir ataques de phishing.

Durante años, el phishing ha sido uno de los métodos más utilizados por los ciberdelincuentes para obtener credenciales mediante sitios web falsificados o correos electrónicos fraudulentos.

El NIST recomienda priorizar autenticadores capaces de verificar el dominio legítimo del servicio antes de completar el proceso de autenticación. Entre ellos destacan:

- Llaves de seguridad compatibles con FIDO2/WebAuthn.
- Passkeys basadas en criptografía de clave pública.
- Autenticadores criptográficos vinculados al dispositivo.

Estos mecanismos utilizan criptografía asimétrica, evitando la transmisión de secretos reutilizables y reduciendo drásticamente la efectividad de los ataques de phishing.

2. Niveles de aseguramiento (Assurance Levels)

Una de las contribuciones más importantes del NIST consiste en establecer diferentes niveles de confianza para los sistemas de identidad digital. En lugar de exigir los mismos controles para todos los servicios, el estándar propone adaptar las medidas de seguridad al riesgo asociado con cada aplicación.

Para ello define tres dimensiones independientes:

- **Identity Assurance Level (IAL):** nivel de confianza en la identidad del usuario.
- **Authentication Assurance Level (AAL):** nivel de confianza durante la autenticación.
- **Federation Assurance Level (FAL):** nivel de confianza cuando la identidad es compartida entre organizaciones.

Esta separación permite diseñar soluciones más flexibles y eficientes.

2.1 Identity Assurance Level (IAL)

El IAL mide el grado de confianza alcanzado durante el proceso de verificación de identidad.

A mayor nivel de aseguramiento, mayores serán los controles aplicados para confirmar la identidad del solicitante.

IAL1

No requiere verificar formalmente la identidad de la persona. Es adecuado para servicios de bajo riesgo, donde basta con crear una cuenta utilizando información básica.

Ejemplos:

- Foros públicos.
- Boletines informativos.
- Portales con contenido abierto.

IAL2

Exige verificar la identidad utilizando evidencias confiables y procedimientos definidos por la organización. Es el nivel recomendado para la mayoría de los servicios gubernamentales, financieros y corporativos.

IAL3

Representa el máximo nivel de aseguramiento. Requiere procedimientos reforzados de verificación, evidencias de alta confianza y controles adicionales para minimizar el riesgo de fraude de identidad. Se reserva para servicios críticos o de alto impacto.

2.2 Authentication Assurance Level (AAL)

El AAL evalúa la fortaleza del proceso de autenticación.

AAL1

Permite mecanismos sencillos de autenticación y está orientado a sistemas con bajo riesgo.

AAL2

Requiere autenticación multifactor o mecanismos equivalentes que proporcionen una mayor resistencia frente al compromiso de credenciales.

AAL3

Exige autenticadores con protección criptográfica reforzada y resistencia frente a ataques avanzados, incluyendo el phishing. Está destinado a infraestructuras críticas, sistemas gubernamentales sensibles y entornos donde el impacto de una intrusión sería muy elevado.

2.3 Federation Assurance Level (FAL)

El FAL determina el grado de confianza cuando una organización acepta afirmaciones de identidad emitidas por otra entidad, como ocurre en arquitecturas de federación o Single Sign-On.

A mayor nivel de FAL, mayores serán las garantías sobre la integridad, confidencialidad y autenticidad de las afirmaciones intercambiadas entre el proveedor de identidad y la organización que presta el servicio.

Este modelo facilita la interoperabilidad entre instituciones sin sacrificar la seguridad ni la protección de la identidad del usuario.

PARTE 4

Federación de Identidad, Credenciales Verificables, Gestión del Riesgo, Privacidad y Recomendaciones

1. Federación de Identidad (Federated Identity)

Uno de los avances más importantes del NIST SP 800-63-4 es el fortalecimiento del modelo de **federación de identidad**, el cual permite que múltiples organizaciones compartan información de autenticación de manera segura y controlada. En este modelo, una organización confía en la verificación realizada por otra entidad, evitando que el usuario deba registrarse y autenticarse de forma independiente en cada sistema.

La federación de identidad mejora la experiencia del usuario, reduce la duplicación de credenciales y facilita la interoperabilidad entre plataformas gubernamentales, financieras, educativas y corporativas.

En este esquema intervienen principalmente dos actores:

- **Identity Provider (IdP):** administra la identidad del usuario y emite afirmaciones (assertions) sobre ella.
- **Relying Party (RP):** recibe dichas afirmaciones y decide si concede o no acceso al servicio solicitado.

Este modelo constituye la base tecnológica de soluciones ampliamente utilizadas, como el **Single Sign-On (SSO)**, que permite al usuario autenticarse una sola vez para acceder posteriormente a múltiples aplicaciones.

1.1 Beneficios de la Federación de Identidad

La implementación de un sistema de identidad federada ofrece numerosas ventajas para organizaciones y usuarios:

- Reducción del número de contraseñas que debe administrar el usuario.
- Disminución del riesgo asociado a la reutilización de credenciales.
- Administración centralizada de identidades.

- Mayor facilidad para revocar accesos cuando un usuario deja de pertenecer a la organización.
- Integración entre instituciones que prestan servicios digitales.

No obstante, el estándar advierte que la federación también introduce nuevos riesgos. Si el proveedor de identidad es comprometido, el atacante podría acceder a múltiples servicios. Por ello, el IdP debe implementar controles de seguridad robustos, autenticación multifactor y mecanismos criptográficos adecuados.

2. Credenciales Verificables y Billeteras Digitales

La versión SP 800-63-4 incorpora tecnologías emergentes que están transformando la gestión de la identidad digital.

Entre ellas destacan las **Credenciales Verificables (Verifiable Credentials)** y las **Billeteras Digitales (Digital Wallets)**, diseñadas para otorgar al usuario un mayor control sobre sus atributos personales.

Una credencial verificable es una representación digital de un atributo o documento emitido por una entidad confiable y protegida mediante mecanismos criptográficos. Puede acreditar, por ejemplo:

- Identidad personal.
- Edad.
- Título profesional.
- Licencia de conducir.
- Certificados académicos.
- Permisos laborales.

Las billeteras digitales permiten almacenar estas credenciales en dispositivos controlados por el usuario, facilitando su presentación únicamente cuando sea necesario.

Este modelo reduce la exposición innecesaria de datos personales y fortalece la privacidad.

3. Gestión del Riesgo en la Identidad Digital

Uno de los cambios conceptuales más importantes introducidos por el NIST SP 800-63-4 consiste en adoptar un enfoque de **gestión del riesgo basada en resultados**, en lugar de un enfoque centrado únicamente en el cumplimiento normativo.

Antes de implementar un sistema de identidad digital, la organización debe analizar aspectos como:

- El impacto de una posible suplantación de identidad.
- El valor de la información protegida.
- Las amenazas existentes.
- La probabilidad de fraude.
- Los riesgos para los usuarios.
- Los riesgos para la organización.

A partir de este análisis se seleccionan los niveles de aseguramiento (IAL, AAL y FAL) y los controles de seguridad más apropiados.

Este enfoque evita aplicar medidas excesivas en servicios de bajo riesgo y, al mismo tiempo, garantiza controles reforzados cuando las consecuencias de un incidente son significativas.

4. Protección de la Privacidad

La privacidad constituye uno de los principios transversales del NIST SP 800-63-4. El estándar establece que las organizaciones deben diseñar sus sistemas de identidad respetando el principio de **privacidad desde el diseño (Privacy by Design)**.

Entre las principales recomendaciones se encuentran:

- Recopilar únicamente los datos estrictamente necesarios.
- Limitar el acceso a la información personal.
- Proteger los datos durante todo su ciclo de vida.
- Informar de manera transparente cómo serán utilizados los datos.
- Establecer mecanismos para que el usuario pueda ejercer control sobre su información.

La confianza del usuario depende no solo de la seguridad técnica del sistema, sino también de la percepción de que su información personal será tratada de manera ética y responsable.

5. Experiencia del Usuario y Accesibilidad

El documento reconoce que un sistema excesivamente complejo puede generar errores, aumentar los costos operativos y provocar que los usuarios adopten prácticas inseguras.

Por ello, el diseño de los sistemas de identidad debe equilibrar tres elementos fundamentales:

- Seguridad.
- Facilidad de uso.
- Accesibilidad.

El NIST recomienda implementar interfaces intuitivas, mecanismos de recuperación de cuentas seguros y procesos de autenticación que no generen una carga innecesaria para el usuario. Esto contribuye a una mayor adopción de las medidas de seguridad y reduce la probabilidad de comportamientos inseguros, como la reutilización de contraseñas o el almacenamiento de credenciales en lugares no protegidos.

6. Implicaciones para América Latina

Aunque el NIST SP 800-63-4 fue desarrollado para las agencias federales de los Estados Unidos, sus principios pueden aplicarse eficazmente en organizaciones públicas y privadas de América Latina.

Su adopción puede fortalecer iniciativas como:

- Plataformas de gobierno digital.
- Banca electrónica.
- Comercio electrónico.
- Servicios de salud digital.
- Educación virtual.

- Sistemas nacionales de identidad electrónica.

Países que impulsan procesos de transformación digital pueden utilizar estas directrices como referencia para diseñar marcos de identidad interoperables, seguros y alineados con estándares internacionales.

Conclusiones

El **NIST SP 800-63-4 Digital Identity Guidelines** representa una evolución significativa en la gestión de la identidad digital. Su principal aporte consiste en abandonar un enfoque centrado exclusivamente en el cumplimiento de requisitos técnicos y adoptar una estrategia basada en la gestión del riesgo, la privacidad y la experiencia del usuario.

Entre los aspectos más relevantes destacan:

- La separación entre verificación de identidad, autenticación y federación.
- La utilización de niveles de aseguramiento (IAL, AAL y FAL) adaptados al riesgo.
- La promoción de autenticadores resistentes al phishing.
- La incorporación de credenciales verificables y billeteras digitales.
- La integración de principios de privacidad desde el diseño.
- La interoperabilidad entre organizaciones mediante modelos de federación de identidad.

Estas directrices constituyen una referencia internacional para el desarrollo de ecosistemas digitales confiables y resilientes frente a las amenazas actuales.