

Seguridad de la información

ADR - UTN - FRBA -2020

¿Por qué es importante la ciberseguridad?

Los Ciberataques son considerados uno de los principales riesgos dentro del mundo de los negocios Digitales. Las nuevas tecnologías tienen como propósito otorgar diversos beneficios sin embargo, **estas ventajas también pueden convertirse en amenazas**

- **Inteligencia Artificial (AI):** Manipulación tendenciosa a través de fake news y deepfakes*
- **Tecnología móvil de quinta generación (5G):** Deberán modernizarse la Infraestructura tecnológica, para poder combatir el déficit significativo de cobertura, seguridad y confiabilidad.

Más información relacionada:

<https://www.welivesecurity.com/la-es/2019/11/15/deepfakes-estamos-preparados-impacto/> (*deepfake)

<https://www.osi.es/es/actualidad/blog/2020/07/31/tecnologia-5g-y-riesgos-de-ciberseguridad>

¿Por qué es importante la ciberseguridad? Continuación

- ▶ **Computación Cuántica:** La computación cuántica podría reducir drásticamente el tiempo necesario para resolver los problemas matemáticos en los que actualmente se apoyan las técnicas de cifrado. Esto es importante teniendo en cuenta que la capacidad de procesamiento podría volver imprácticos los algoritmos criptográficos de la actualidad.
- ▶ **Computación en la nube:** Este nuevo concepto tiene la capacidad de potenciar y expandir la tecnología implementada en cada negocio, fomentando así que las empresas vuelquen en ella cada vez más información personal, lo que crea potenciales riesgos a la privacidad y la seguridad de los datos.

Más información relacionada:

<https://www.welivesecurity.com/wp-content/uploads/2019/12/Tendencias-Ciberseguridad-2020-ES.pdf>

La información en la organización

“La información es un activo que, como otros, resulta esencial para el negocio de la organización y consecuentemente debe protegerse adecuadamente.”

“La información es poder”

¿Qué es la seguridad de la información?

La seguridad de la información hace referencia a todas aquellas **medidas preventivas, reactivas** de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la **confidencialidad, la disponibilidad y la integridad** de la misma.

Principios básicos de la seguridad de la información



Sistema de Gestión de Seguridad de la Información (SGSI)

La gestión de la Seguridad de la Información busca establecer y mantener **programas, controles y políticas** que tengan como finalidad conservar la confidencialidad, integridad y disponibilidad de la información.

Es un proceso continuo.

El sistema Gestión de Seguridad de la Información

Debe comprender los siguientes elementos:



¿Qué es la seguridad de la información?

- ▶ **Evento de seguridad de la información:** ocurrencia identificada en un sistema, servicio o estado de una red que indica una posible violación de la política de seguridad o falla en los controles, o una situación previamente desconocida que podría ser relevante para la seguridad.
- ▶ **Incidente de seguridad de la información:** evento individual o serie de eventos de seguridad de la información inesperados o no deseados que tiene una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Plan de respuesta a incidentes

Fases

- ▶ Acción inmediata para **detener o minimizar** el incidente
- ▶ **Investigación** del incidente
- ▶ **Restauración** de los recursos afectados
- ▶ **Reporte** del incidente a los canales apropiados

Plan de respuesta a incidentes

Componentes

- ▶ Equipo de expertos
- ▶ Una estrategia legal revisada y aprobada
- ▶ Soporte financiero de la organización
- ▶ Soporte ejecutivo de la gerencia superior de la compañía o áreas afectadas
- ▶ Recursos físicos

Principales ataques a las organizaciones

- ▶ Ataques de phishing
- ▶ Criptojacking
- ▶ Malware
- ▶ Ciberextorsiones
- ▶ Explotación de vulnerabilidades

Más información relacionada:

<https://www.welivesecurity.com/la-es/2018/12/14/cibercrim-en-ataques-comunes/>

Seguridad lógica

- ▶ Restringir el acceso a los programas y archivos
- ▶ Asegurar que los usuarios puedan trabajar sin supervisión minuciosa sin afectar ningún dato, programa ni archivo que no deban.
- ▶ Asegurar que se están utilizando los datos, archivos y programas correctos en cada situación.
- ▶ Que la información transmitida sea recibida sólo por el destinatario deseado.
- ▶ Que la información recibida sea la misma que ha sido enviada
- ▶ Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos

Seguridad lógica

Servicios de Seguridad

No repudio

- ▶ No repudio de origen: Prueba que el mensaje fue enviado por la parte específica
- ▶ No repudio de destino: Prueba que el mensaje fue recibido por la parte específica

Seguridad lógica

Tipos de usuario

- ▶ Propietario
- ▶ Administrador
- ▶ Usuario principal o referente (Key User)
- ▶ Usuario de explotación
- ▶ Usuario de auditoria

Seguridad Física

- ▶ Administración de respaldos de información (Backups)
- ▶ Disponibilidad
- ▶ Gestión de centros de cómputos principales y secundarios

Seguridad de datos

Acciones y Herramientas.

- ▶ Análisis de vulnerabilidades en códigos fuentes y aplicaciones
- ▶ Adecuado uso de ambientes de desarrollo, testing, preproducción y producción
- ▶ Test (unit test, code review, integración, regresión, etc.)
- ▶ Control y auditoría de acceso
- ▶ Restricción de la visibilidad de datos

ISO/IEC 27000

- ▶ Marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización
- ▶ ISO/IEC 27001: Norma principal de la serie, contiene los requisitos del sistema de gestión de seguridad de la información y es la norma que se certifica por auditores externos.
- ▶ ISO/IEC 27002: Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable.

ISO/IEC 27000

Algunos Puntos de la Norma

- ▶ Anexo A 9.1 Requisitos de la empresa para el control de acceso (p.e Sistema de gestión de contraseñas, Uso de programas de utilidad privilegiada, Control de acceso al código fuente del programa, Revisión de los derechos de acceso del usuario)
- ▶ Anexo A 10.1 Controles criptográficos
- ▶ Anexo A 11.1 Áreas seguras (controles de acceso físico)
- ▶ Anexo A 12.1 (Procedimientos y responsabilidades operativas, Protección contra malware, Respaldo, Registros y monitoreo, Control del software en producción, Gestión de vulnerabilidades técnicas

COBIT 5

Figura 4—Principios de COBIT 5

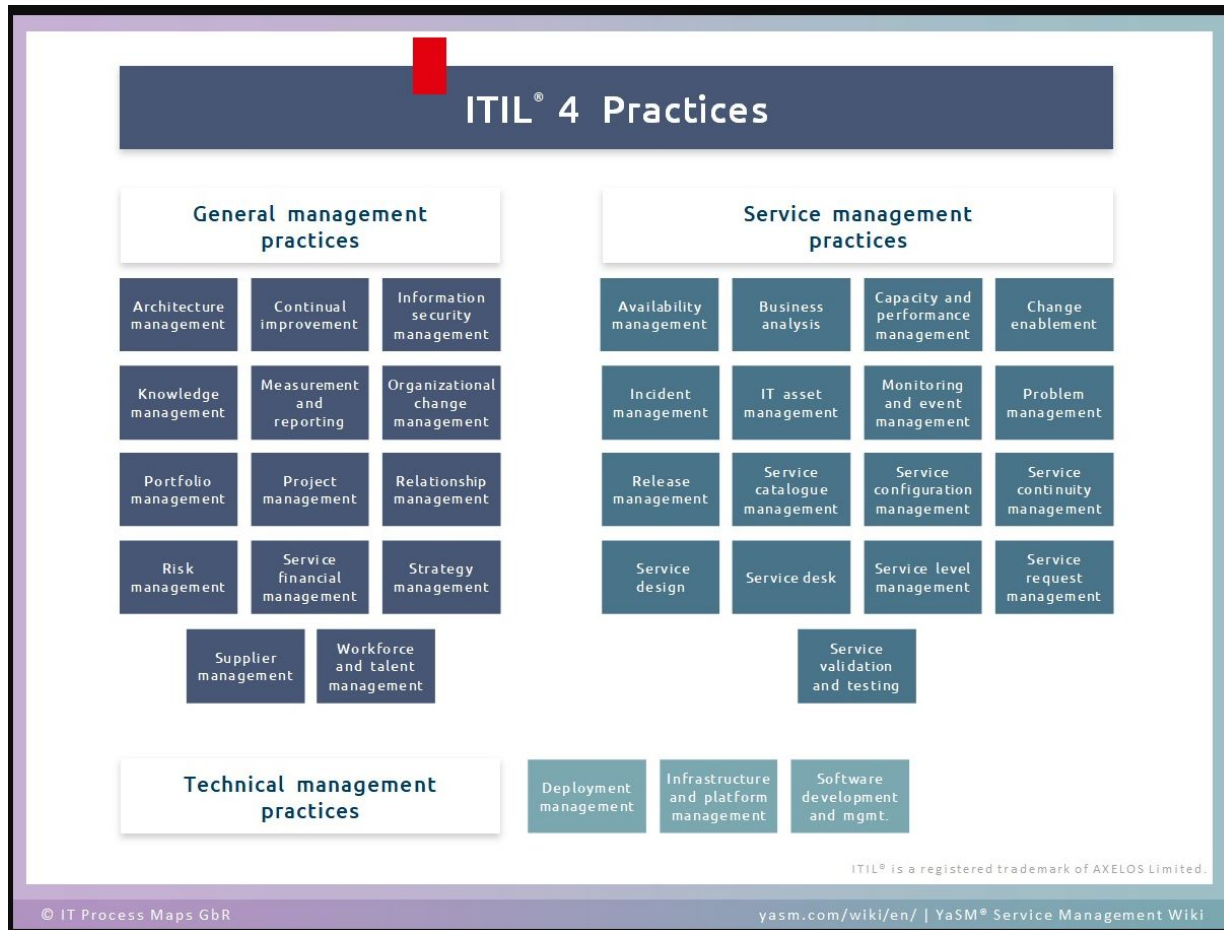


COBIT 5

COBIT 5 for Information Security

- ▶ Complemento de procesos Cobit 5 (Gestión de la seguridad, Gestión de la continuidad y Gestión de Servicios de seguridad)
- ▶ Seguridad como disciplina transversal con un enfoque holístico.
- ▶ Alinear la seguridad de la información con los objetivos de la organización.
- ▶ Mapeo de procesos con cláusulas y controles de otros estándares como ISO 27001 o NIST (National Institute of Standards and Technology)

ITIL - V4



Referencia:

<https://www.hiberus.com/crecemos-contigo/novedades-til-v4/>

Information Security Management (ITIL 4)



Autenticación

No Repudio

Procesos para respaldar la gestión de la seguridad de la información:

- ▶ Gestión de incidentes
- ▶ Gestión de riesgos
- ▶ Revisión y auditoría
- ▶ Gestión de identidad y acceso
- ▶ Gestión de eventos
- ▶ Pruebas de penetración, escaneo de vulnerabilidades, etc.
- ▶ Procedimientos para administrar cambios relacionados con la seguridad de la información

Referencia:

<https://wiki.process-symphony.com.au/framework/lifecycle/process/information-security-management-itol-4/>

PCI (Payment Card Industry Data Security Standard)

La adopción de pagos sin contactos o "tap and go" se ha incrementado a nivel mundial. Esta nueva modalidad en las compras busca opciones accesibles, flexibles y seguras para la aceptación de pagos sin contactos.

Para ello se ha desarrollado y establecido una norma, que permite focalizar ciertos estándares que garantizan la seguridad de la información de la transacción.

La norma: Pagos sin contactos en dispositivos comerciales estándar (Contactless Payments on COTS, CPoC™) de PCI para soluciones que aceptan pagos sin contactos en dispositivos móviles de comerciantes que utilizan NFC

Referencia: <https://www.pcisecuritystandards.org/>

PCI

PCI Contactless Payments on COTS (CPoC™)



*Note this is a conceptual, high-level depiction of CPoC.



Referencia:

https://www.pcisecuritystandards.org/about_us/press_releases/pr_12042019

PCI - Estructura del Estándar para CPoC

CPoC™								
#	Requerimientos de Seguridad y de Prueba		#	Requerimientos de Seguridad y de Prueba		#	Requerimientos de Seguridad y de Prueba	
1.1	Requisitos Básicos	Protección de servicios sensibles	2.1	Pagos contactless en la aplicación COTS	Protección contra manipulaciones e ingeniería inversa	3.1	Sistemas de back-end: monitoreo / certificación	Línea de base del sistema COTS
1.2		Números aleatorios	2.2		Criptografía protegida por software	3.2		Mecanismo de certificación
1.3		Criptografía aceptable	2.3		Procesamiento en línea	3.3		Tipo 1: certificación de la plataforma COTS
1.4		Gestión de claves	2.4		Autenticidad de la aplicación	3.4		Tipo 2: certificación de la aplicación CPoC
1.5		Canales seguros	2.5		Aplicación segura	3.5		Identificación y validación de componentes
1.6		Datos correlacionables	2.6		Aprovisionamiento seguro	3.6		Seguridad del entorno de supervisión y certificación
1.7		Gestión operativa	2.7		Registros de auditoría	4.1	Sistemas de back-end: procesamiento	Seguridad del entorno de procesamiento de datos de la cuenta
1.8		Prácticas de desarrollo de software seguro	2.8		Lectura contactless de los datos de la cuenta	5.1	Kernel contactless	Funcionalidad del kernel contactless
1.9		Desarrollo, mantenimiento y difusión del Manual del Usuario de la solución	2.9		Cifrado de datos de cuenta	5.2		Requisito de seguridad del kernel contactless

PCI - Estructura del Estándar para CPoC

Lectura complementaria de Interés:

1. https://www.pcisecuritystandards.org/document_library
2. <https://blog.pcisecuritystandards.org/just-published-pci-contactless-payments-on-cots>
3. <https://blog.pcisecuritystandards.org/coming-soon-new-contactless-standard>
4. <https://blog.pcisecuritystandards.org/pqi-on-mobile-payment-acceptance-spot-and-contactless-updates>

Firma Digital - Ley 25506

► Firma digital vs firma electrónica

- ARTICULO 2° – Firma Digital. Se entiende por firma digital al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control...
- ARTICULO 5° – Firma electrónica. Se entiende por firma electrónica al conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerada firma digital. En caso de ser desconocida la firma electrónica corresponde a quien la invoca acreditar su validez.

Identidad y autenticación

Todo acceso a cualquier Aplicación o interfaz debe estar restringido a personas autenticadas y autorizadas.

Una autenticación débil puede permitir el acceso no autorizado a sus sistemas, lo que puede resultar perjudicial para la organización y la información que resguarda.

Es importante que la autenticación se realice a través de canales seguros.

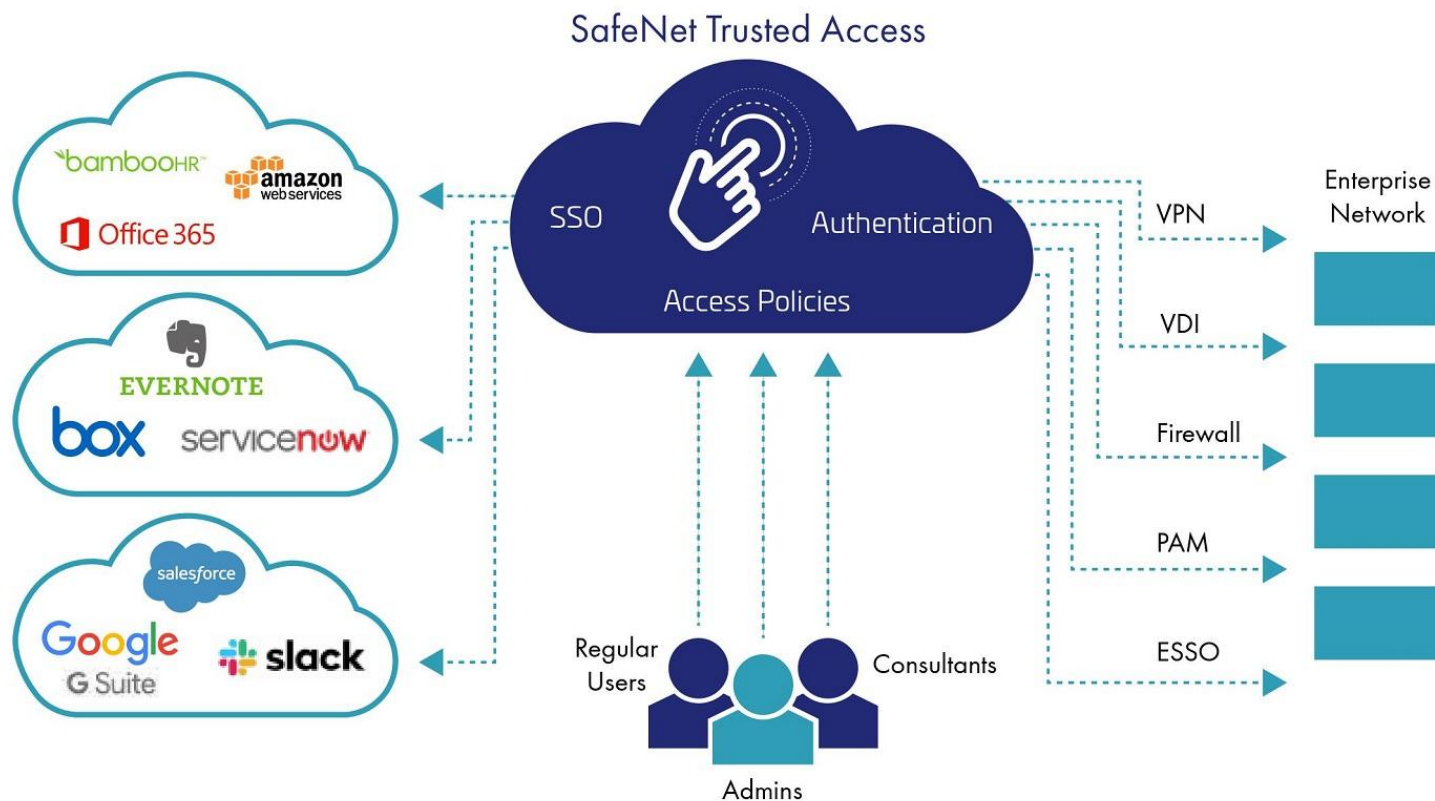
Aspectos Clave -Identidad y autenticación:

Debe tener confianza en que los controles de identidad y autenticación garantizan que los usuarios están autorizados a acceder a interfaces específicas.

Servicios de autenticación

Authentication as a Service (AaaS)

La autenticación como servicio (AaaS) permite a las organizaciones aplicar fácilmente la autenticación multifactor para proteger el acceso a cualquier aplicación, desde cualquier dispositivo y en cualquier lugar.



Servicios de autenticación

Authentication as a Service (AaaS)

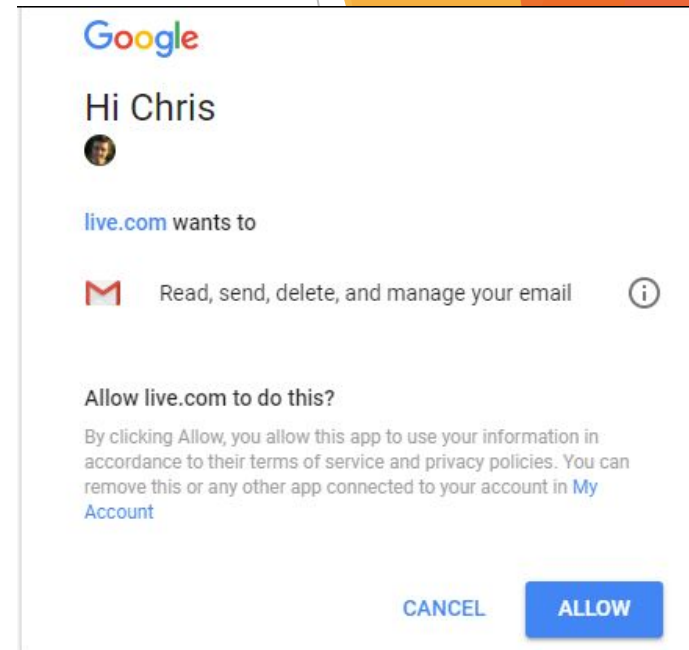
Referencias:

1. <https://cpl.thalesgroup.com/access-management/authentication-as-a-service>
2. <https://auth0.com/>

OAuth 2.0 (RFC 6749)

Autorización

- ▶ Es un protocolo abierto que permite flujos de autorización para todo tipo de aplicaciones (web, mobile, desktop, api)
- ▶ Permite el acceso limitado a recursos propios por parte de aplicaciones de terceros.
- ▶ Delega la autenticación de usuario al servicio que gestiona las cuentas
- ▶ Se utiliza por ej. para dar acceso a aplicaciones de terceros a datos de cuentas de cuentas de Twitter, Facebook, Google o Microsoft



OAUTH 2.0 (RFC 6749)

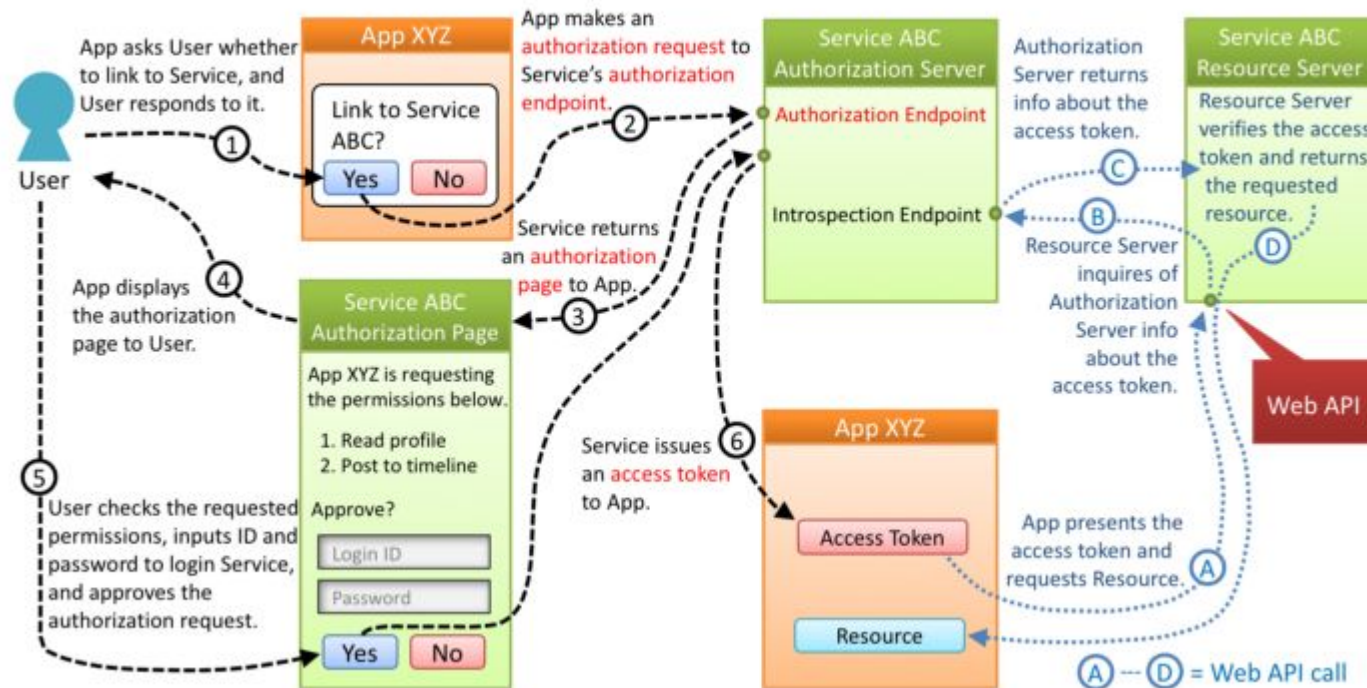
Referencias:

1. <https://oauth.net/2/>
2. <https://www.oauth.com/>
3. <https://aaronparecki.com/oauth-2-simplified/>
4. <https://medium.com/@programmercito/oauth2-para-humanos-ffd00b40ec73>

OAUTH 2.0 (RFC 6749)

Autorización

Implicit Flow (RFC 6749, 4.2)



© 2017 Authlete, Inc. <https://www.authlete.com/>

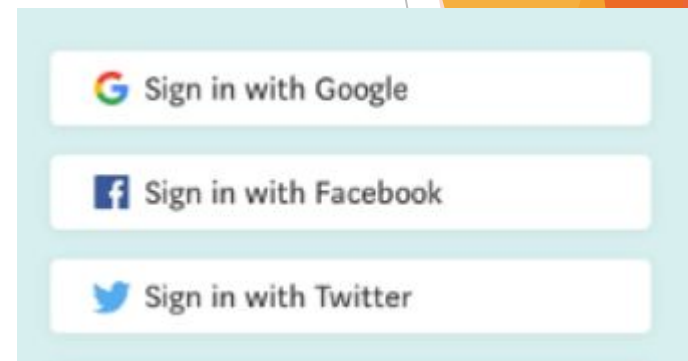
Referencia:

<https://medium.com/@darutk/diagrams-and-movies-of-all-the-oauth-2-0-flows-194f3c3ade85>

OIDC - OpenID Connect

Autenticación

- ▶ OpenID Connect es una capa de identidad simple que opera sobre el protocolo OAuth 2.0
- ▶ Provee un protocolo estándar para verificar la identidad de un usuario final
- ▶ El usuario es autenticado en un gestor de identidades que conoce, sin necesidad de nuevos procedimientos de registro o intercambio de contraseñas.
- ▶ Minimiza el riesgo para el usuario de mantener registrada su identidad en n lugares con n claves.

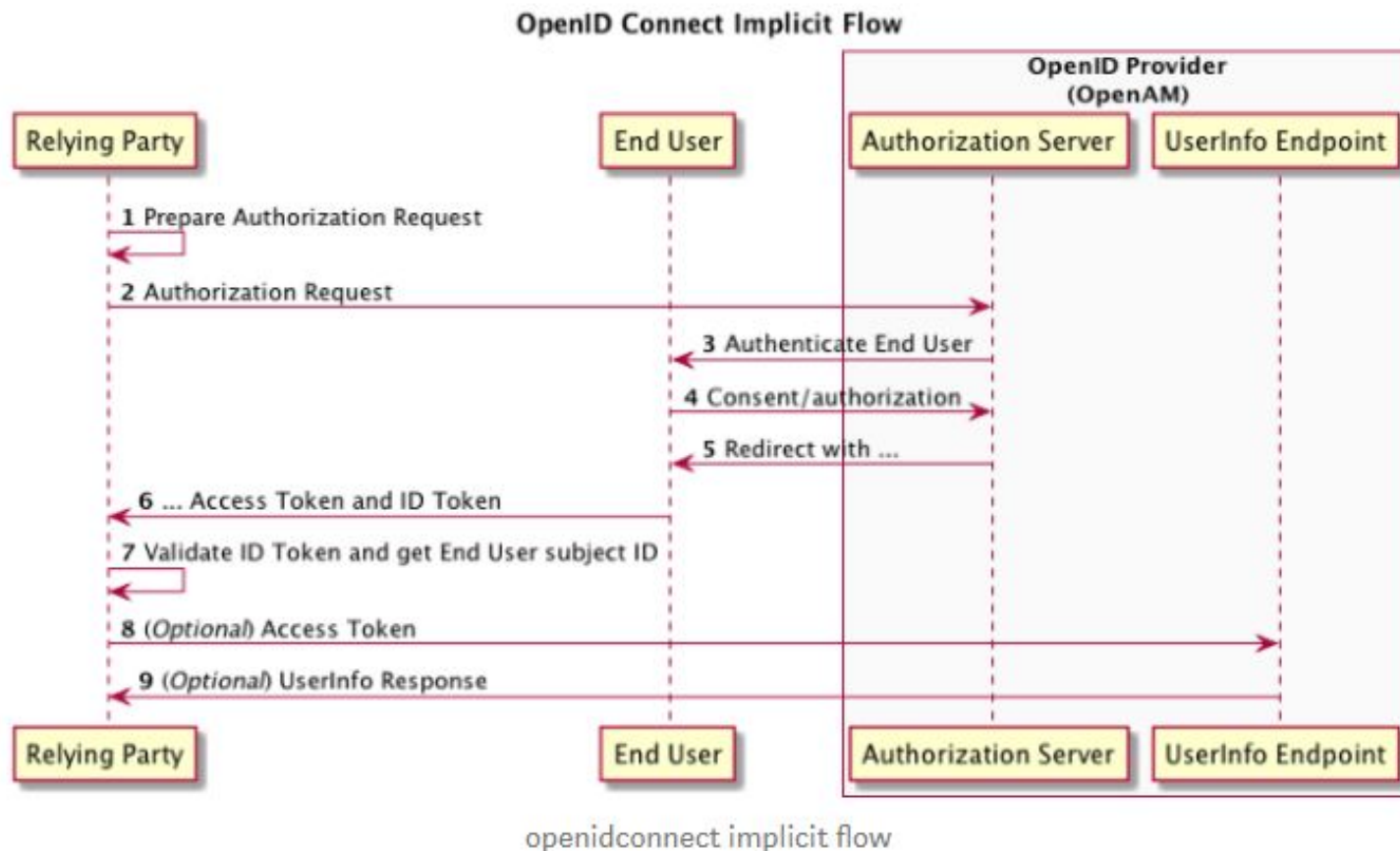


Referencia:

<https://openid.net/connect/>

<http://www.arquitectoit.com/api-management/breve-introduccion-open-id-connect/>

OIDC - OpenID Connect Autenticación



Referencia:

<https://medium.com/@nilasini/real-world-example-to-understand-oidc-implicit-flow-ecdf1b1d0156>

GRACIAS

The background features a series of overlapping, semi-transparent triangles in shades of orange and yellow, creating a dynamic, geometric pattern. Thin, light gray lines intersect across the composition, adding to the abstract design. The overall aesthetic is modern and minimalist.