**UNIVERSIDAD NACIONAL AUTÓNOMA DE HONDURAS (UNAH).**

**FACULTAD DE INGENIERÍA.**

**DEPARTAMENTO DE INGENIERÍA EN SISTEMAS**

**Asignatura:**

Industria del software (IS-902)

**Sección:**

1600

**Catedrática:**

Ing. Rafael Diaz del Valle.

**Investigación:**

Autentificación en Línea.

**Grupo # 3.**

**Integrantes.**

|  |  |
| --- | --- |
| Nombre | Número de Cuenta. |
| Adán Young | **20141001860** |
| Luis Irías | **20151002776** |
| Maverick Martínez | **20141001825** |

Ciudad Universitaria, Tegucigalpa MDC, Francisco Morazán 8 de septiembre del 2019.

Tabla de contenido

[Introducción. 3](#_Toc18760223)

[Objetivos. 4](#_Toc18760224)

[Objetivos Generales. 4](#_Toc18760225)

[Objetivos Específicos. 4](#_Toc18760226)

[Marco Teórico. 5](#_Toc18760227)

[Tipos de autenticación 6](#_Toc18760228)

[Autenticación física 6](#_Toc18760229)

[Autenticación lógica 6](#_Toc18760230)

[Autenticación en Línea. 7](#_Toc18760231)

[¿Cómo demostrar quiénes somos en el mundo online? 7](#_Toc18760232)

[Factor de conocimiento. 7](#_Toc18760233)

[Factor de posesión o propiedad. 8](#_Toc18760234)

[Factor de inherencia o existencia. 8](#_Toc18760235)

[¿Cuándo un factor no es suficiente? 9](#_Toc18760236)

[Los factores del futuro. 10](#_Toc18760237)

[¿Qué características debe tener un sistema de autenticación? 11](#_Toc18760238)

[Autenticación en Sistemas Empresariales. 11](#_Toc18760239)

[Política de seguridad. 12](#_Toc18760240)

[¿Autenticación o identificación? 13](#_Toc18760241)

[Siete elementos de autenticación. 13](#_Toc18760242)

[Conclusión. 17](#_Toc18760243)

[Bibliografías. 18](#_Toc18760244)

# Introducción.

La autenticación es un método muy importante de realizar para verificar si las personas son quienes dicen ser, el método principal de autenticación para los humanos es el rostro o características físicas específicas, para los sistemas informáticos y servicios en línea se suelen utilizar distintos métodos de autenticación que derivan de las características o conocimientos de los usuarios.

# Objetivos.

## Objetivos Generales.

* Describir los métodos de autenticación utilizados para validar usuarios.

## Objetivos Específicos.

* Conocer las generalidades de la autenticación.
* Describir los diferentes métodos de autenticación en línea.
* Brindar herramientas para la autenticación en línea.

# Marco Teórico.

La Autenticación es el proceso que debe seguir un usuario para tener acceso a los recursos de un sistema o de una red de computadores. Este proceso implica identificación (decirle al sistema quién es) y autenticación (demostrar que el usuario es quien dice ser).

La autenticación por sí sola no verifica derechos de acceso del usuario, estos se confirman en el proceso de autorización.

En general, la seguridad de las redes de datos requiere para conceder acceso a los servicios de la red, tres procesos:

* Autenticación,
* Autorización
* Registro.

Autenticación: proceso por el cual el usuario se identifica en forma inequívoca; es decir, sin duda o equivocación de que es quien dice

ser.

Autorización: el proceso por el cual la red de datos autoriza al usuario identificado a acceder a determinados recursos de la misma.

Registro: el proceso mediante el cual la red registra todos y cada uno de los accesos a los recursos que realiza el usuario, autorizado o no.

Estos tres procesos se conocen por las siglas en inglés como AAA, o Authentication, Authorization, y Accounting.

## **Tipos de autenticación**

Se puede efectuar autenticación usando uno o varios de los siguientes métodos:

* Autenticación por conocimientos: basada en información que sólo conoce el usuario.
* Autenticación por pertenencia: basada en algo que posee el usuario.
* Autenticación por características: basada en alguna característica física del usuario.

De lo anterior se deduce que la autenticación involucra aspectos físicos y lógicos relacionados con el acceso, la utilización y la modificación de los recursos de la red o sistema.

## **Autenticación física**

La autenticación física se basa en algún objeto físico que posee el usuario, o en alguna característica física del usuario; en tal caso utiliza algún tipo de mecanismo biométrico.

La información capturada en el proceso de autenticación, pasa al proceso de autorización realizado por personas, dispositivos electrónicos de seguridad o sistemas de seguridad informática.

## **Autenticación lógica**

La autenticación lógica puede utilizarse para identificar personas o sistemas y se basa en información que sólo conoce el usuario. La autenticación y autorización las realiza software especializado.

Si se combinan dos o más métodos de autenticación, esta se denomina autenticación múltiple (multi-factor authentication) y es una autenticación más segura. Por ejemplo, autenticación doble si el usuario debe presentar dos tipos de identificación, una física (una tarjeta) y la otra algo que el usuario ha memorizado como una clave de seguridad o un número de identificación personal. Este es el caso de una tarjeta bancaria que se utiliza con un cajero automático. Más aún, algunos sistemas utilizan autenticación triple (con tres factores): un objeto físico, una contraseña y algún dato biométrico como la huella digital.

# Autenticación en Línea.

En el mundo offline, el proceso de autenticación es simple y universal. La mayoría de los países cuentan con procedimientos bien documentados mediante los cuales se puede obtener un pasaporte que demuestre una identidad en cualquier lugar donde se encuentre. En el mundo de las computadoras, no existe un documento único que sirva para probar una identidad donde sea que nos encontremos. Como resultado, la mayoría de los sitios web y servicios utilizan distintas técnicas de autenticación.

Si uno no sabe quién es realmente un usuario, no puede saber a qué recursos o servicios debe tener derecho de acceso, ni tampoco es posible identificar las acciones que realizaron.

## **¿Cómo demostrar quiénes somos en el mundo online?**

Cuando tenemos que demostrar que somos quienes aseguramos ser, debemos buscar algo único e inalterable acerca nuestro. Para ello, podemos recurrir a algunas estrategias:

* Factor de conocimiento: lo que se sabe.
* Factor de posesión o propiedad: lo que tienes.
* Factor de inherencia o existencia: lo que eres.

### **Factor de conocimiento.**

Involucrar un dato que (idealmente) solo conoces tú (la persona cuya identidad se está tratando de verificar) y la persona o proceso que está verificando tu identidad.

Hay ciertas cosas que se utilizan comúnmente como “factores de conocimiento”: las contraseñas, las claves de acceso, las frases de contraseña o el PIN (que es el acrónimo en inglés de Número de Identificación Personal). Muchas personas no se dan cuenta de que las “preguntas secretas” (que algunos sitios web te exigen que utilices además de tu contraseña) también son factores de conocimiento.

### **Factor de posesión o propiedad.**

Involucra un objeto entregado por la persona u organización que te está verificando, que puedes mostrar para verificar tu identidad.

La mayoría de nosotros tenemos al menos un “factor de propiedad” en la billetera, posiblemente varios. Si bien tu licencia de conducir o tu documento de identidad sin duda pertenecen a esta categoría, las tarjetas de pago también lo son, por lo que a veces está permitido utilizarlas como una forma muy básica de identificación.

Las tarjetas de crédito o débito que llevas en la billetera no son solo una señal de que el banco te considera capaz de pagar tus deudas; también indican que el banco ya ha verificado tu identidad.

Pero el documento personal y las tarjetas de pago no son los únicos ejemplos de “factores de propiedad”. Cualquier cosa que pueda vincularse a ti en forma exclusiva es útil; por ejemplo, una dirección de correo electrónico, un dispositivo móvil o un número telefónico.

Los sitios online también pueden generar códigos de claves temporales y enviártelos por mensajes SMS, llamadas de voz o correos electrónicos, para que luego los puedas usar como credenciales de inicio de sesión.

### **Factor de inherencia o existencia.**

Involucra las cosas que forman parte de lo que eres; por lo general son cosas que nunca cambiarán.

Este factor de autenticación que antes solo estaba disponible para los espías, hoy en día está presente en muchos smartphones o equipos portátiles. El escáner de huellas dactilares, que es el ejemplo más común, tiene el propósito de verificar el patrón único de las puntas de tus dedos. Algunos smartphones ahora vienen con un escáner de iris, que verifica las manchas y coloraciones exclusivas de tus ojos.

La Oficina de Aduanas y Protección Fronteriza de los Estados Unidos está probando escáneres de reconocimiento facial, como una manera de automatizar la verificación de la identificación mediante fotografías.

## **¿Cuándo un factor no es suficiente?**

El uso de más de un factor para autenticar a propietarios de cuentas es cada vez más popular.

A esta altura, la mayoría de nosotros conocemos a alguien cuya cuenta online fue comprometida. La autenticación que solo utiliza el nombre de usuario y la contraseña le genera tantos problemas de seguridad a tanta gente que los investigadores buscan constantemente nuevas formas de autenticar a sus usuarios en forma rápida y segura. El uso de más de un factor para autenticar a los propietarios de cuentas es una opción cada vez más popular.

El inicio de una sesión mediante el uso de dos factores de autenticación se denomina “autenticación en dos fases”, “autenticación de dos factores”, “verificación en dos pasos”; o, para abreviar, 2FA. Si un proceso de inicio de sesión tiene habilitada la 2FA, incluso si los usuarios dan a conocer sus credenciales (ya sea accidental o intencionalmente), sus cuentas aún seguirán protegidas si el atacante no tiene también acceso al segundo factor.

### **Los factores del futuro.**

Otro método para mejorar la seguridad de la autenticación es encontrar nuevos factores, hay un par que ya se están utilizando sin que la gente lo sepa:

* Factor de ubicación: dónde estás
* Factor de comportamiento: lo que haces

Pueden parecer un poco extraños, porque la gente viaja y su comportamiento va cambiando con el tiempo. Seguramente te preguntarás cómo pueden ser únicos si los datos cambian. Pero al parecer pueden ser muy útiles, en especial cuando se usan en conjunto con otros factores.

El “factor de ubicación” se basa en que es posible esperar que una persona esté en cierto lugar en determinado momento (es decir, en casa o en el trabajo) o que use ciertas máquinas específicas. Obviamente, no siempre será el caso; entonces, por sí misma, esta información solo tiene utilidad marginal. Pero si te encuentras en un lugar conocido o estás usando una dirección IP o MAC conocida, puede utilizarse como tu segundo factor de autenticación, además del nombre de usuario y la contraseña. De lo contrario, si no estás en ese lugar conocido o en ese equipo conocido, se te pedirá que utilices un factor diferente de autenticación, como un código de clave temporal.

Por otra parte, el “factor de comportamiento” se basa en que los comportamientos pueden ser tan únicos como las huellas dactilares; por ejemplo, nuestros hábitos de navegación, nuestras voces, nuestros movimientos del mouse o en la pantalla táctil, o nuestra letra cuando escribimos a mano. Algunos smartphones ya están utilizando este factor. Si configuras una clave de acceso numérica o gestual, no solo registran el código en sí, sino también la forma en que lo escribes o deslizas el dedo para ingresarlo.

## **¿Qué características debe tener un sistema de autenticación?**

1. Para que un determinado sistema de autenticación se pueda implementar fácilmente debe cumplir con los siguientes requisitos:
2. Fiabilidad: la probabilidad de error debe ser mínima.
3. Viabilidad: debe ser económicamente asequible para la empresa que lo quiera implementar. Si cuesta más que los datos que se quieren proteger, estaremos seleccionado el sistema de autenticación equivocado.
4. Seguridad: debe ser resistente a posibles ciberataques.
5. Usabilidad: debe de ser fácil de usar para el cliente o usuario que se debe autenticar.

# Autenticación en Sistemas Empresariales.

La autentificación es la primera etapa del proceso de conexión de un usuario

Toda organización que se basa en un sistema de información tiene que garantizar el proceso de conexión a los sistemas y aplicaciones.

La creación de una fuente única y fiable de las identidades, asociada a la gestión de los derechos son los dos pilares de una buena infraestructura de gestión de las identidades y accesos. El proceso de conexión de un usuario puede entonces efectuarse. Se articula en general alrededor de 4 etapas;

**Proceso inicial: común a todas las conexiones**

1. Abertura de una sesión sobre del puesto de trabajo y autenticación del usuario

2. Se comprueba los derechos del usuario y lo conecta a sus recursos

**Proceso de conexión a una aplicación**

1. Ejecución por el usuario de una aplicación y autenticación sobre esta aplicación.

2. La aplicación comprueba los derechos del usuario y lo conecta a sus

transacciones y datos.

La autenticación del usuario es uno de los puntos clave de este proceso. Es ella que debe permitir del Sistema de Información asegurarse de la identidad del usuario y asociarle sus derechos.

Existen numerosos métodos de autenticación. Cada una de estos métodos posee sus características propias.

## **Política de seguridad.**

Toda organización tiene, o debería tener, una política de seguridad relativa a la protección de los puestos de trabajo, de las aplicaciones, de los datos o también de los sistemas del SI. Esta política de seguridad puede definir niveles mínimos de autenticación en función de la criticidad del recurso utilizado. Por ejemplo, es posible imaginar, como en muy buena película de espionaje, que se coloca un puesto de trabajo crítico en una sala protegida por un acceso controlado por

un código confidencial, por la introducción de una tarjeta inteligente y por una definición biométrica del ojo derecho. La protección es entonces a su máximo, ya que para registrar es necesario proporcionar un elemento que se sabe (el código), que se posee (la tarjeta) y que es (el ojo).

Este mecanismo permite efectivamente proteger un puesto de trabajo, pero es costoso desde un punto de vista de la aplicación (requiere una sala por PC, así como los lectores adecuados) y de la explotación (¿qué pasa si un usuario olvida su código, pierde su tarjeta y se devuelve tuerto del ojo derecho?).

### **¿Autenticación o identificación?**

Existe una diferencia muy simple entre identificación y autenticación: el comprobante.

Una identificación se basa en una simple declaración como la recepción o la lectura

de un código de identificación (identificador, n° serie, código barra,). Este código de

identificación no se supone secreto. Es un dato público.

La autenticación se basa en un elemento de prueba como un secreto compartido o un

secreto asimétrico. La autenticación permite asegurarse con un nivel de confianza

razonable de la identidad del usuario.

# Siete elementos de autenticación.

Para autentificarse, un usuario proporciona en general al menos 2 elementos:

* Su identificador que permite su definición.
* Uno o más elementos que permiten garantizar la propia autenticación.

Encontramos así estos elementos bajo distintas formas. Ahí tienes el más

ampliamente utilizados:

|  |  |
| --- | --- |
| Tipo. | Descripción. |
| El identificador y la contraseña | El identificador y la contraseña son el par de autenticación más  conocido. Simple, robusto, incluso rústico, su más grande defecto es que el nivel de seguridad depende directamente de la complejidad  de la contraseña. Contraseñas simples son escasas, y contraseñas demasiado complejas conducen a los usuarios a aplicar estrategias no siempre correctas para gestionarlas: Post-it® lista en un archivo Excel o en el SmartPhone,… |
| El identificador y la contraseña OTP (One-Time Password). | El OTP permite asegurar el uso de la contraseña en la red. En efecto, con un sistema OTP el usuario posee un calculador especializado que le proporciona bajo petición una contraseña. Esta contraseña es válida solo durante una duración limitada, y para una única utilización. Esta solución se aplica en general para el proceso de  autenticación inicial para los accesos externos mediante  IP/VPN |
| Los certificados PKI sobre tarjeta inteligente o token USB | Los certificados X.509 aplican una tecnología avanzada de codificación que permite calcular o firmar mensajes sin tener que compartir de secreto. El identificador es un certificado público que es firmado y en consecuencia garantizado por una autoridad de certificación reconocida. El usuario debe proporcionar un secreto para poder utilizar los distintos elementos criptográficos: “el código PIN de su tarjeta o su tecla USB”. Esta solución se aplica en general para el proceso de autenticación inicial o para las conexiones a las aplicaciones Red o de servicio de mensajería. |
| Tecla “Confidencial Defensa” | Se trata de una declinación particular del ejemplo anterior. Es en general una llave multifunciones: almacenamiento de certificado X.509, almacenamiento de datos, recurso criptográfico etc… |
| El identificador y la contraseña sobre una tarjeta inteligente | El almacenamiento del identificador y la contraseña sobre una tarjeta inteligente permite suplementar la protección del proceso de autenticación. La contraseña puede así ser muy compleja y cambiada regularmente de manera automática y aleatoria. Sin la tarjeta, y sin su código PIN, no se puede acceder a la contraseña. Esta solución se aplica generalmente para el proceso de autenticación inicial |
| Biométrica | La autenticación por biométrica se basa en la verificación de un elemento del cuerpo del usuario (generalmente la huella dactilar). Puede basarse en un distribuidor central, en el puesto de trabajo o en una tarjeta inteligente para almacenar los datos biométricos del usuario. Esta solución se aplica en general para el proceso de autenticación inicial y/o para proteger el acceso a aplicaciones muy sensibles. |
| La definición sin contacto | El RFID es una tecnología que hoy se despliega en los proyectos de Identificación/Autenticación. Un chip RFID es insertada en una tarjeta y lleva un número de identificación. Este número se asocia a continuación a un usuario en un sistema informático. A la base es una tecnología de Identificación que puede, acoplado a una contraseña proporcionada por el usuario, por ejemplo, utilizarse en procedimientos de autenticación. Existe 2 declinaciones de esta tecnología: El RFID pasivo o HID, que supone que la tarjeta no posee alimentación propia. La tarjeta es abastecida en la lectura por un campo electromagnético generado por el lector. Este sistema se utiliza comúnmente para el control de acceso físico por tarjeta o el pago al restaurante de empresa. La detecta una tarjeta HID a algún centímetro. El RFID activo se basa en los protocolos de comunicación RFID pero asocia a la carta una alimentación propia. |

# Conclusión.

La autenticación es un elemento muy importante para proteger información sensible que no debe estar al alcance de terceros, es un factor que no se puede dejar por fuera al momento de utilizar cualquier producto o servicio informático,

Un factor de autenticación es una categoría de credencial utilizada para la verificación de identidad. Las tres categorías más comunes se describen como algo que conoces (el factor de conocimiento), algo que tienes (el factor de posesión) y algo que eres (el factor de inherencia).

# Bibliografías.

* <http://www.oas.org/en/citel/infocitel/2006/junio/seguridad_e.asp>
* <https://www.welivesecurity.com/la-es/2016/05/04/autenticacion-como-probar-que-eres-tu/>
* <https://blog.signaturit.com/es/como-verificar-la-identidad-digital-de-tus-clientes>
* <https://www.evidian.com/pdf/wp-strongauth-es.pdf>