SESIÓN 04

CONTROL DE ACCESOS Y PERFILES

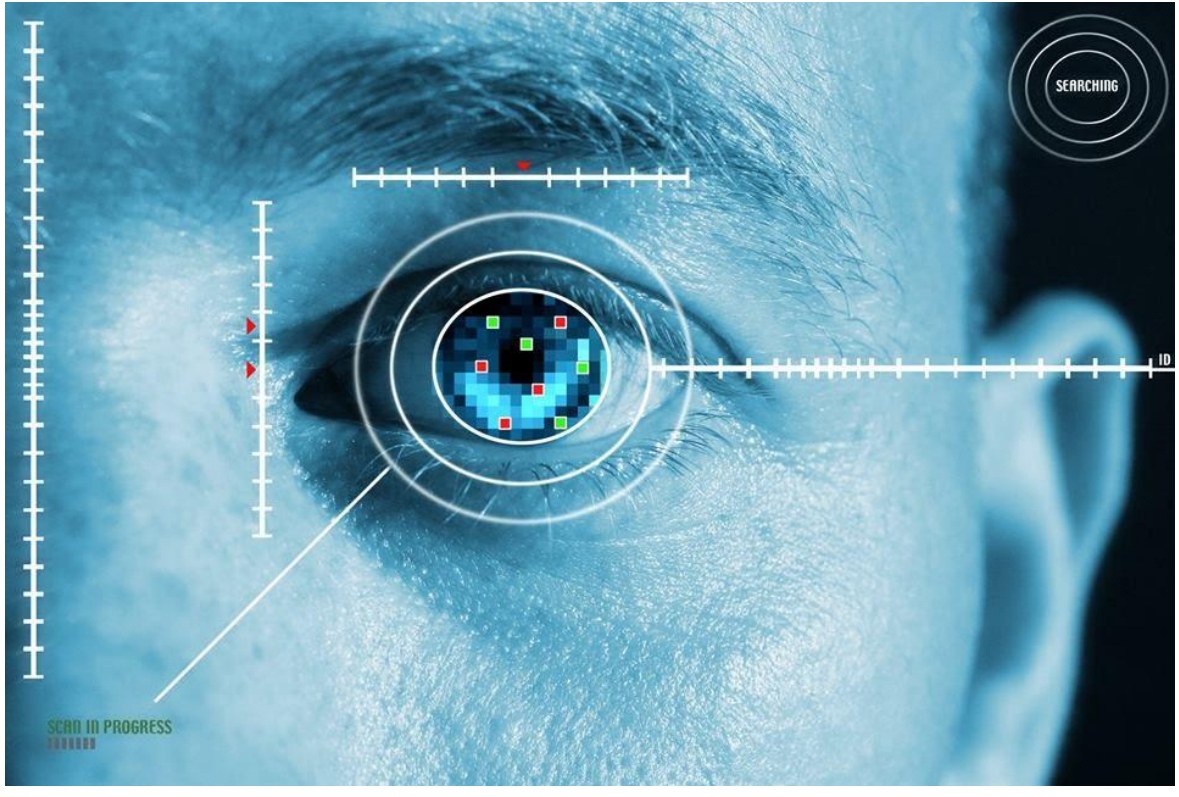
- Control de Accesos y Perfiles

Implementa los procesos de control de accesos y perfiles

Acceso a redes y los servicios de red

Gestión de Contraseñas

Autenticación secreta

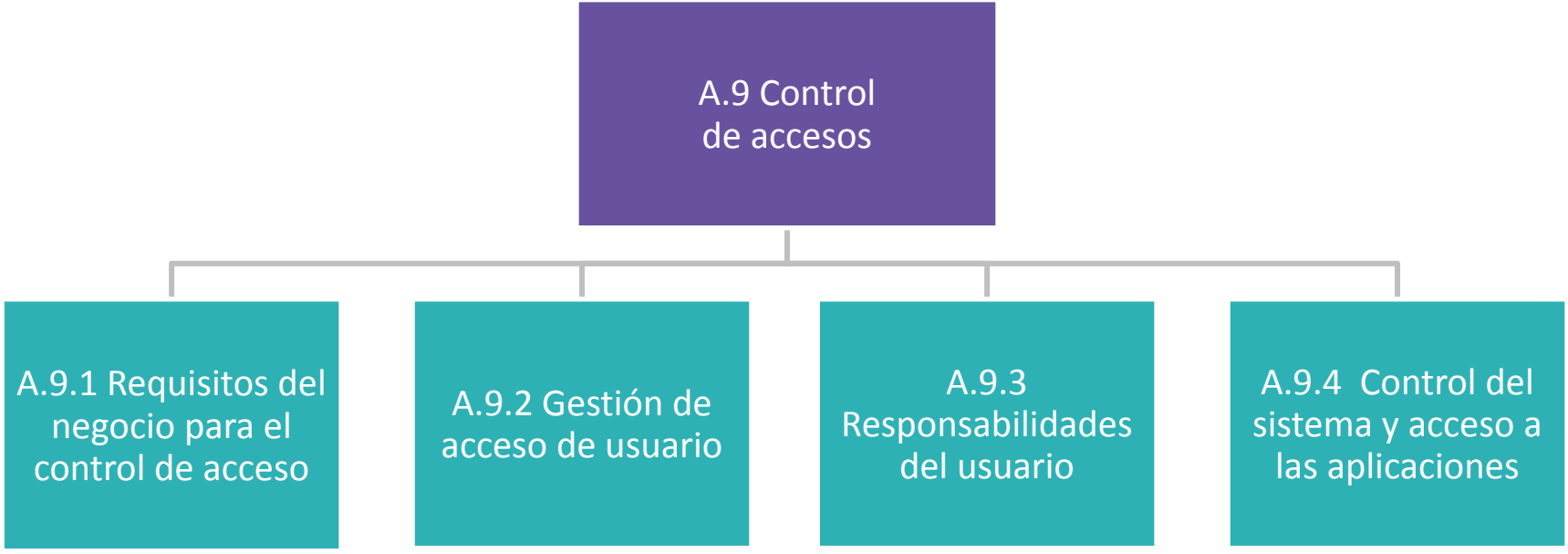


/ CONTROL DE ACCESOS Y PERFILES

AGENDA

- Objetivo
- Requisitos del negocio
- Acceso de usuario
- Responsabilidades del usuario
- Control del sistema y acceso a aplicaciones

CONTROL DE ACCESOS



A.9.1 Requisitos del negocio para el control de acceso
Objetivo: Para limitar el acceso a la información y las instalaciones de procesamiento de la información.

A.9.1.1 Política de control de acceso.
A.9.1.2 El acceso a las redes y los servicios de red.

A.9.1.1 Política de control de acceso

Se debe establecer, documentar y revisar una política de control de acceso basada en los requisitos de negocio y de seguridad de la información.

A.9.1.2 El acceso a las redes y los servicios de red

Se debe proporcionar a los usuarios únicamente el acceso a la red y a los servicios de la red para los que hayan sido específicamente autorizados.

A.9.2 Gestión de acceso de usuario

Objetivo: Asegurar el acceso de un usuario y prevenir el acceso no autorizado a los sistemas y servicios.

A.9.2.1 Registro y des-registro de usuario.
A.9.2.2 Provisión de acceso de usuario.
A.9.2.3 Gestión de derechos de acceso privilegiado.
A.9.2.4 Gestión de información secreta de autenticación de los usuarios.
A.9.2.5 Revisión de los derechos de acceso de usuario.
A.9.2.6 Eliminación o ajuste de los derechos de acceso.

A.9.2.1 Registro y des-registro de usuario

Deberá ser implementado un proceso formal de registro y des-registro de usuario para habilitar la asignación de derechos de acceso.

A.9.2.2 Provisión de acceso de usuario

Deberá ser implementado un proceso formal de provisión de acceso de usuario para asignar o revocar derechos de acceso para todos los tipos de usuario en todos los sistemas y servicios.

A.9.2.3 Gestión de derechos de acceso privilegiado

La asignación y el uso de accesos de privilegio deberán estar restringidos y controlados.

A.9.2.4 Gestión de información secreta de autenticación de los usuarios

La asignación de información de autenticación secreta debe ser controlada a través de un proceso de gestión formal.

A.9.2.5 Revisión de los derechos de acceso de usuario

Los propietarios de activos deberán revisar los derechos de acceso de usuarios a intervalos regulares.

A.9.2.6 Eliminación o ajuste de los derechos de acceso

Los derechos de acceso a la información y a los recursos de tratamiento de la información de todos los empleados y terceros deben ser retirados a la finalización del empleo, del contrato o del acuerdo, o bien deben ser adaptados a los cambios producidos.

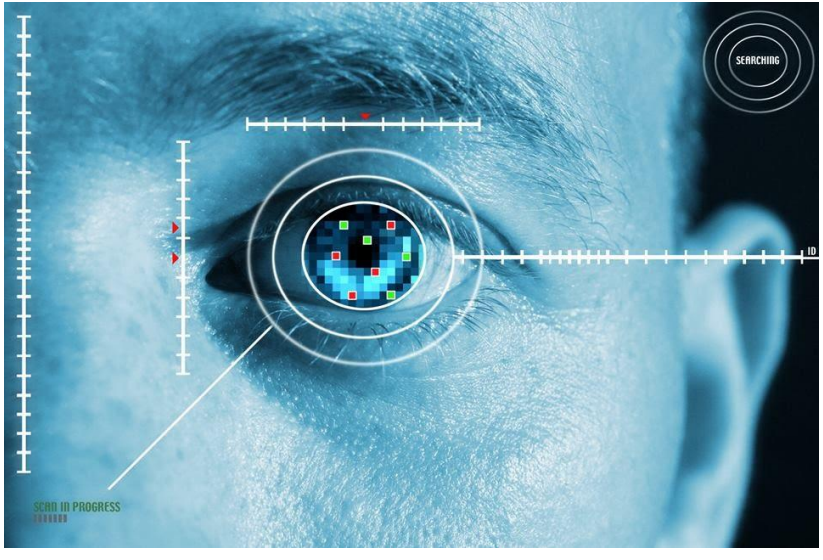
A.9.3 Responsabilidades de usuario

Objetivo: Hacer que los usuario sean responsables de salvaguardar su información de autenticación.

A.9.3.1 Uso de información de autenticación secreta.

A.9.3.1 Uso de información de autenticación secreta

Los usuarios deberán seguir las prácticas de la organización en el uso de información de autenticación secreta.



A.9.4 Control de sistema y acceso a las aplicaciones
Objetivo: Prevenir el acceso no autorizado a os sistemas y aplicaciones.

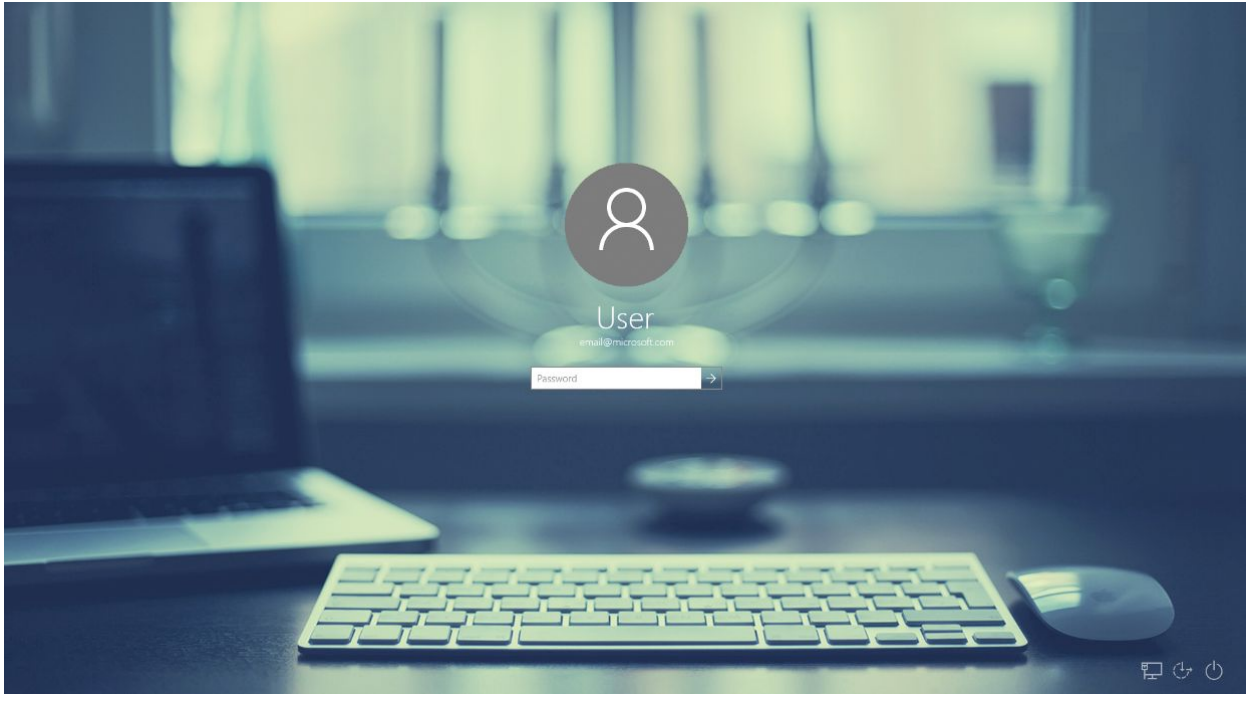
A.9.4.1 Restricción del acceso a la información.
A.9.4.2 Procedimientos seguros de inicio de sesión.
A.9.4.3 Sistema de gestión de contraseñas.
A.9.4.4 Uso de programas utilitarios privilegiados.
A.9.4.5 Control de acceso al código fuente de los programas.

A.9.4.1 Restricción del acceso a la información

Se debe restringir el acceso a la información y a las aplicaciones de acuerdo con la política de control de acceso.

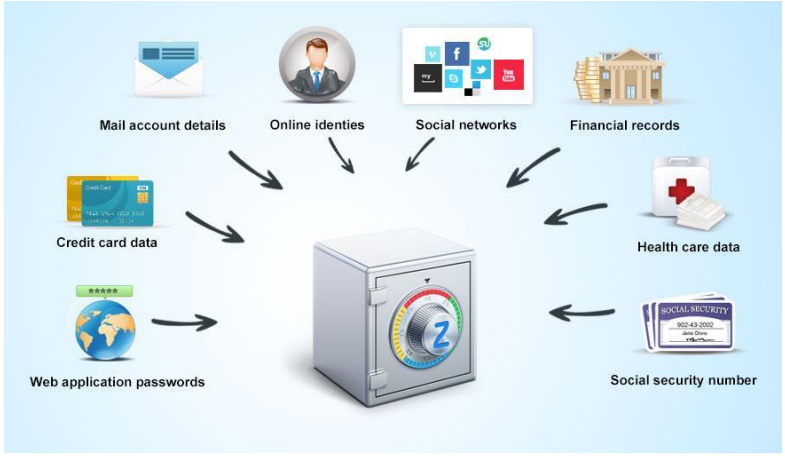
A.9.4.2 Procedimientos seguros de inicio de sesión

Cuando sea necesario por la política de control de acceso, el acceso a los sistemas y las aplicaciones deberá ser controlado por un procedimiento de registro seguro.



A.9.4.3 Sistema de gestión de contraseñas

Los sistemas de gestión de contraseñas deben ser interactivos y establecer contraseñas seguras y robustas.

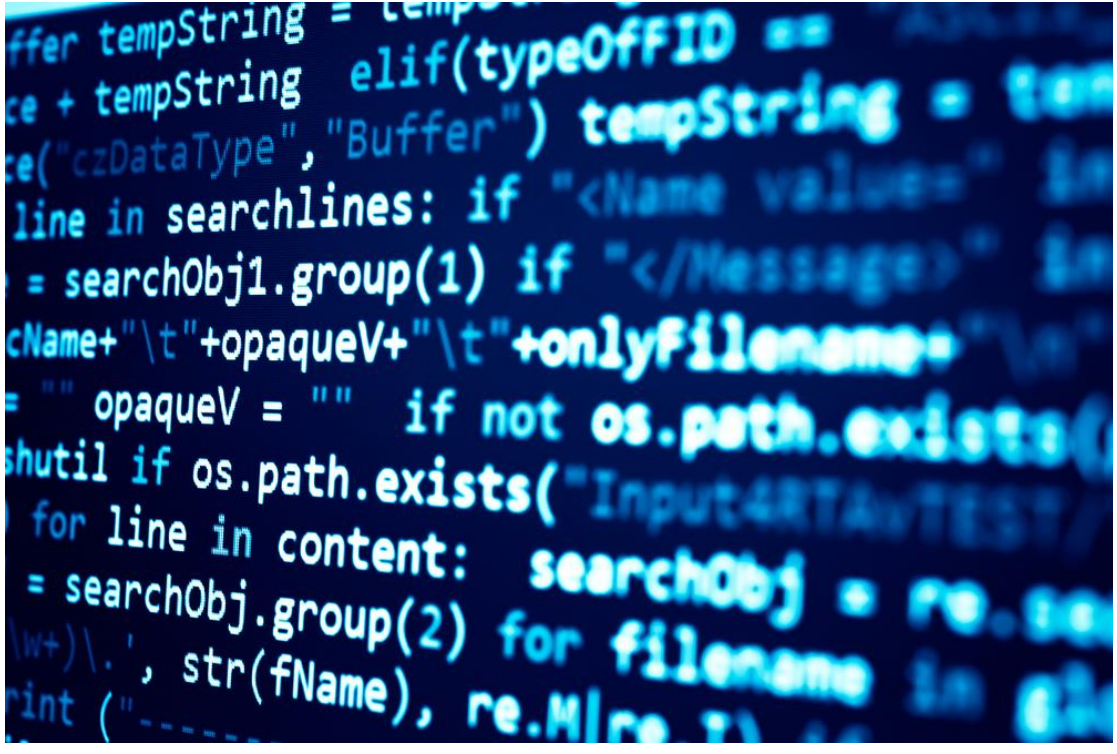


A.9.4.4 Uso de programas utilitarios privilegiados

Se debe restringir y controlar rigurosamente el uso de programas y utilidades que puedan ser capaces de invalidar los controles del sistema y de la aplicación.

A.9.4.5 Control de acceso al código fuente de los programas

Se debe restringir el acceso al código fuente de los programas .



TAREA GRUPAL

Objetivo

- Identificar el mecanismo de autenticación más adecuado para los diferentes escenarios que se plantean.

TAREA GRUPAL

En grupos de 5 participantes trabajar lo siguiente:

- En base a la tabla adjunta identificar y sustentar que técnica de autenticación utilizaría.

TÉCNICA	VENTAJAS	DESVENTAJAS
Reconocimiento de cara	Fácil, rápido y barato	La iluminación puede alterar la autenticación
Lectura de huella digital	Barato y muy seguro	Posibilidad de burla por medio de réplicas, cortes o lastimaduras pueden alterar la autenticación
Lectura de iris/retina	Muy seguro	Intrusivo (molesto para el usuario)
Lectura de la palma de la mano	Poca necesidad de memoria de almacenamiento de los patrones	Lento y no muy seguro
Reconocimiento de la firma	Barato	Puede ser alterado por el estado emocional de la persona
Reconocimiento de la voz	Barato, útil para accesos remotos	Lento, puede ser alterado por el estado emocional de la persona, fácilmente reproducible

TAREA GRUPAL

En grupos de 5 participantes trabajar lo siguiente:

- En un banco.
- En un colegio.
- Entidad de Gobierno.
- Compañía de Seguros

TAREA GRUPAL

Instrucciones para la entrega de la tarea.

- La tarea deberá ser realizada y expuesta en clase, por todos los miembros del grupo.

/ RESUMEN

Controles de Acceso y Perfiles.

Revisión de derechos.