**PROYECTO**

1. El Inicio, esta vista debe ser **intuitiva, amigable, sorprendente**, debe permitir validar un usuario, y una contraseña, con restricciones de mayúsculas y minúsculas, **parámetros de seguridad, para login,** debe permitir recuperar contraseña: permitiendo enviar a un teléfono celular una contraseña temporal o a un correo electrónico previamente almacenado.

* **Intuitivo:** Poder comprender las cosas al instante. El Usuario debe presentir lo que va a pasar con sus emociones al entrar al sistema. Conocimiento inmediato, directo y autoevidente.
* **Amigable:** el Usuario debe tener unión y conformidad con el sistema.
* **Sorprendente:** Debe estar fuera de lo común, debe causar gran admiración.

[**https://www.bps.gub.uy/bps/file/13151/1/fsi---iaa.pdf**](https://www.bps.gub.uy/bps/file/13151/1/fsi---iaa.pdf)

**SEGURIDAD INFORMATICA, login.**

* Identificación.
* Autenticación.
* Autorización.

**Usuarios y autenticación**

Existen dos razones para autenticar a los usuarios de un sistema:

* La identidad de usuario es un parámetro para la decisión de control de acceso.
* La identidad del usuario es registrada cuando se hace el loggin de eventos relevantes para la seguridad en la auditoria.

No es necesario basar el control de acceso en identidad, pero si es importante para auditar.

Cuando un usuario se conecta a un sistema el mismo debe proveer:

* User name – este paso se llama identificación.
* Password – este paso se llama autentificación.

La autentificación es el proceso de verificar una pretendida identidad.

Para verificar identidades, se pueden utilizar algunas de las siguientes opciones:

* Algo que se sabe (Ej. Password).
* Algo que se tiene (Ej. Bagge, token, Smart card).
* Algo que se es (Ej. Huella digitales, ADN,iris).
* Donde se está (Ej. Usando una terminal particular).

El proceso de autenticación consiste en varios pasos: obtener la información, analizar los datos y determinar si la información de autenticación es correcta.

**Métodos para encriptar password.**