Contrasinais seguras en Webs Dinámicas

Este documento trata sobre a seguridade das contrasinais e os datos de usuario nas aplicacións do proxecto **Webs Dinámicas**.

Cando iniciamos sesión como un usuario rexistrado en calquera das tres aplicacións do proxecto Webs Dinámicas da web do noso centro, envíanse por internet o nome de usuario e a contrasinal introducidos para que sexan validados polo servidor. Ata o de agora, esta información enviábase sen cifrar, co conseguinte risco de que fose interceptada por outras persoas.

Para solucionar este problema vanse habilitar os sistemas necesarios, polo momento na **Páxina Web** e na **Aula Virtual**. Queda pendente a **Galería** de imaxes. No caso da páxina web enviaranse cifrados os datos de inicio de sesión, os datos de autorexistro de usuarios, os datos de alta de usuarios por parte dos administradores, e os datos da edición do perfil de usuario. No caso da aula virtual só se cifrarán o nome de usuario e a contrasinal no momento do inicio de sesión.

Estes sistemas serán habilitados de oficio polos administradores do proxecto na **AMTEGA**, **e non é necesaria ningunha actuación por parte dos centros.**

Si que se recomenda que se instale o **certificado da FNMT** nos ordenadores do centro seguindo as instruccións que se achegan na última parte deste documento.

Información para os administradores das Webs Dinámicas nos centros

Descrición da solución para Drupal (Versión 6)

No caso de Drupal, instalouse o módulo *securelogin*, que ademais foi adaptado as características do proxecto. Este módulo asegura o envío de información para catro funcións distintas de Drupal:

- O inicio de sesión, tanto desde o bloque "*Iniciar Sesión*" como desde a ruta *user/login.*
- A edición do perfil de usuario, incluíndo o cambio de contrasinal.
- O autorexistro de usuarios (ruta *user/register*).
- O rexistro de usuarios por parte do administrador (ruta *admin/user/user/create*)

O módulo *securelogin* será habilitado de oficio polos administradores do proxecto Webs Dinámicas na AMTEGA, e non deberá ser deshabilitado polos administradores nos centros educativos.

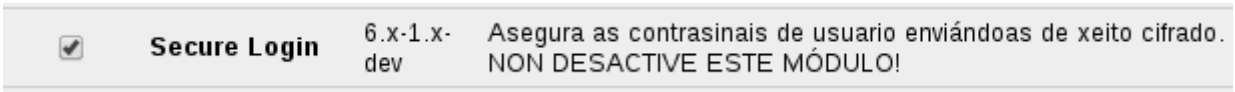

Fig. 1: O módulo *securelogin*

Se desactivamos este módulo recibiremos a seguinte mensaxe de advertencia:

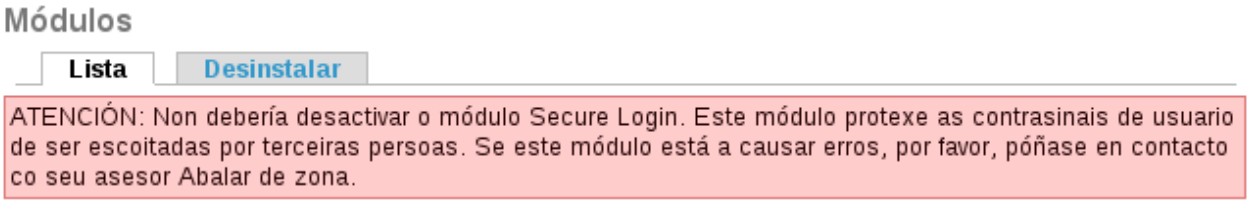

Fig. 2: Aviso pola desactivación do módulo *securelogin*

A configuración establecida por defecto para este módulo produce o seguinte comportamendo do mesmo:

- Os formularios nos que introduciremos os datos non se reciben de xeito seguro, só a información que se envía ao servidor cando enviamos o formulario vai cifrada. Así, cando estamos, por exemplo, no formulario de inicio de sesión, o protocolo que veremos na barra de dirección será o HTTP, non o HTTPS. Isto fai que o envío seguro da información sexa transparente para o usuario e que finalizado o envío, a conexión volte automaticamente ao protocolo non cifrado HTTP.
- Os envíos de información que se protexen son, como se dixo antes: o inicio de sesión, a edición do perfil de usuario, e os rexistros e autorexistros de usuarios.

Na páxina de configuración deste módulo hai un aviso de que só o *webmaster* pode modificar esta configuración. Os administradores de Drupal nos centros educativos atoparán deshabilitadas as opcións de configuración deste módulo, non podendo modificalas.

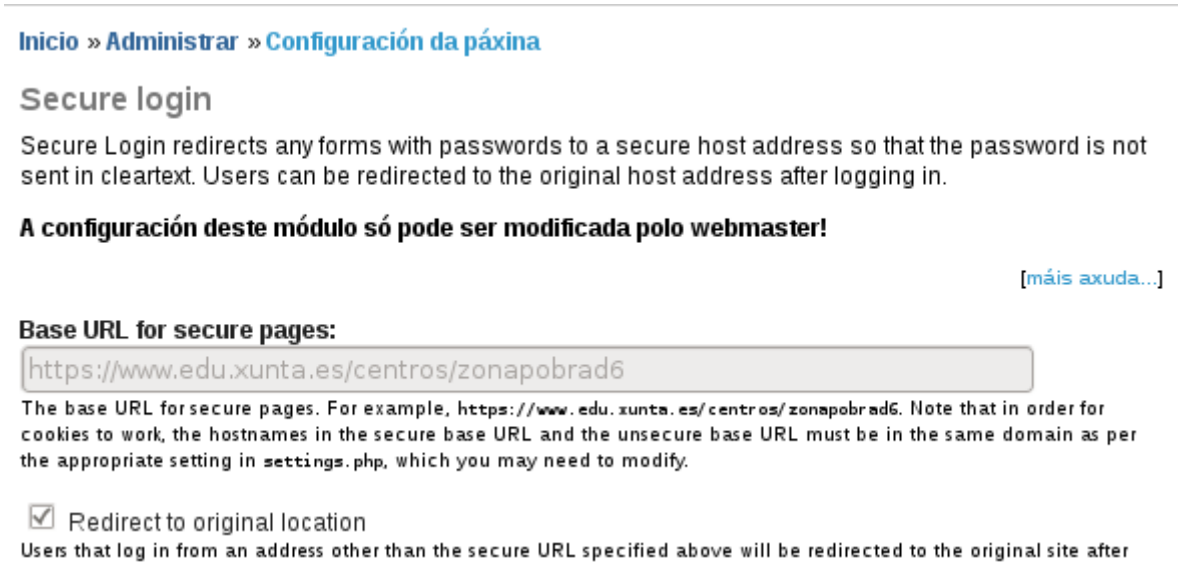

Fig. 3: Páxina de configuración deshabilitada

Descrición da solución para Moodle

No caso de Moodle, activarase a función propia deste software que fai o inicio de sesión seguro. Os administradores das aulas virtuais dos centros poden ver esta configuración en *Administración do sitio -> Seguranza -> Seguranza HTTP*, na opción "*Utilice HTTP para as conexións (loginhttps)*", que debe estar marcada. Esta opción será habilitada de oficio polos administradores do proxecto Webs Dinámicas na AMTEGA, e non deberá ser deshabilitada polos administradores nos centros educativos.

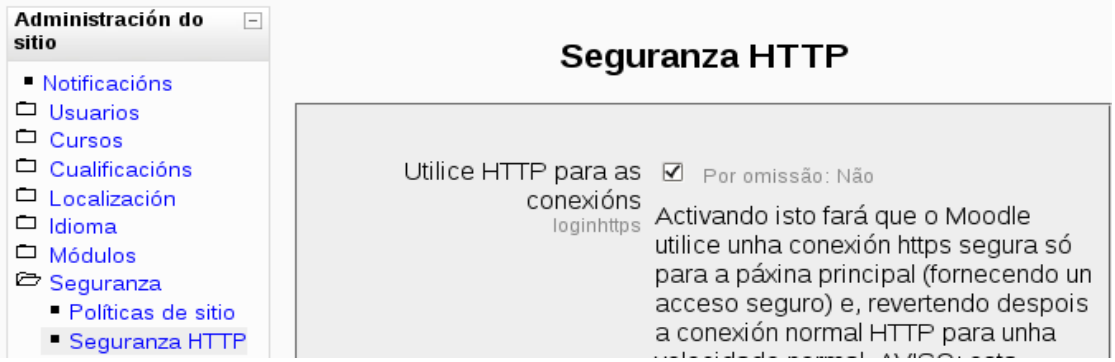

Fig. 4: Configuración do acceso seguro en Moodle

Con esta opción activa, cando abramos o formulario de inicio de sesión na aula virtual, a conexión cambiará ao protocolo HTTPS, tal como podemos ver na seguinte imaxe. Unha vez realizado o inicio de sesión, a conexión voltará ao protocolo HTTP.

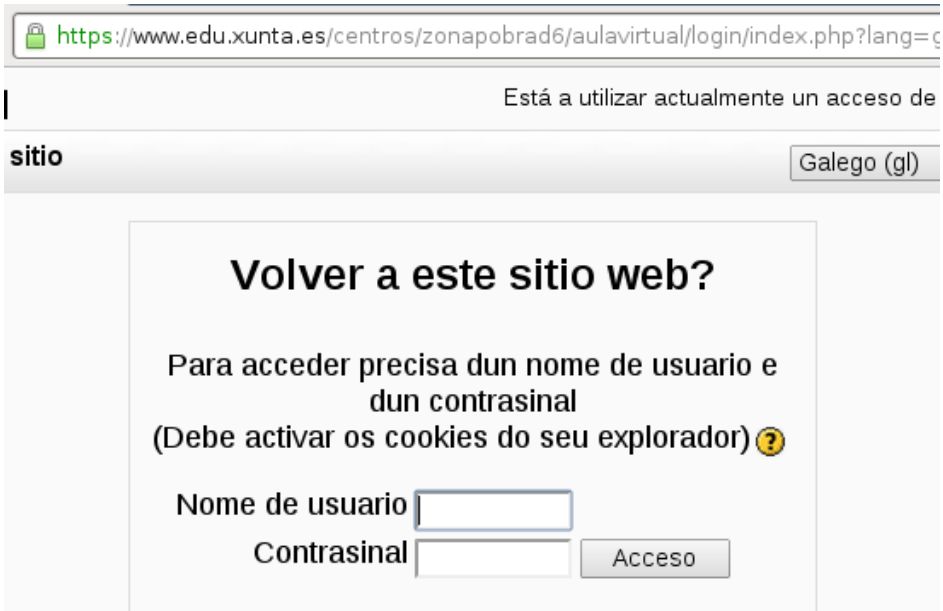

Fig. 5: Acceso por https á aula virtual

Información sobre os certificados

Para o envío seguro desta información, utilízase o protocolo HTTPS – Secure HTTP – sobre unha conexión cifrada SSL – Secure Socket Layer. Os servidores que admiten este tipo de conexións utilizan un certificado de chave pública, emitido por unha Entidade de Certificación, que contén chaves para cifrar e descifrar a información, e outros datos que serven para verificar a identidade do servidor.

Cando utilizamos una conexión deste tipo, o noso navegador de internet tenta comprobar que o servidor ao que imos enviar información é realmente o que nos queremos e non outro, impostor, que se meta no medio para quedarse coa nosa información. Para realizar esta comprobación o navegador pregunta á Entidade de Certificación que emiteu o certificado do servidor, pola autenticidade do mesmo, pero para poder facelo, o navegador precisa ter instalado un certificado desa Entidade Certificadora. No caso da Xunta de Galicia, o certificado foi emitido pola Fábrica Nacional de Moneda e Timbre, cuxo certificado non ven instalado por defecto nos navegadores.

Cando o navegador non ten instalado o certificado da Entidade Certificadora, daranos un aviso e preguntaranos se realmente estamos seguros de querer enviar a información. Isto pode pasarnos, por exemplo, entrando no correo corporativo, onde recibiriamos un aviso como estes:

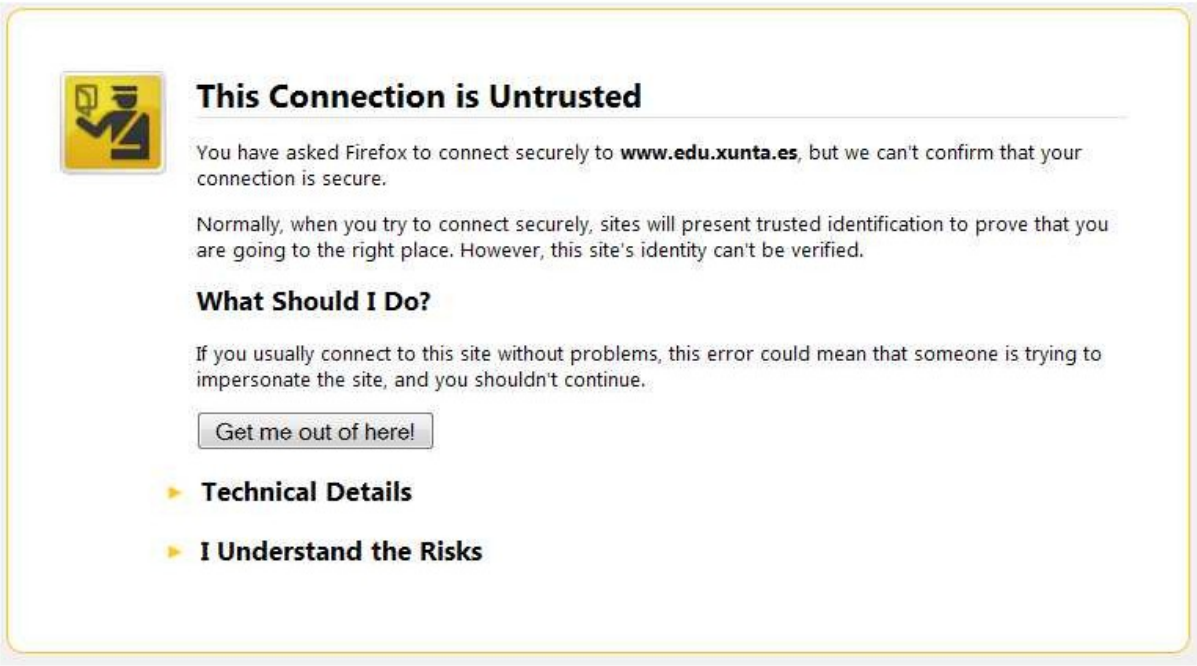

Fig. 6: Aviso de que non se pode comprobar a identidade do servidor (Firefox)

No caso do navegador Mozilla Firefox, nesta pantalla temos a posibilidade de engadir unha excepción para que o navegador se conecte a este servidor sen preguntarnos máis, pero isto non garante a seguridade, xa que non se comproba a identidade do servidor ao que nos estamos conectando. A información envíase cifrada pero non temos garantía de que o servidor que a recibe sexa o que nos esperamos.

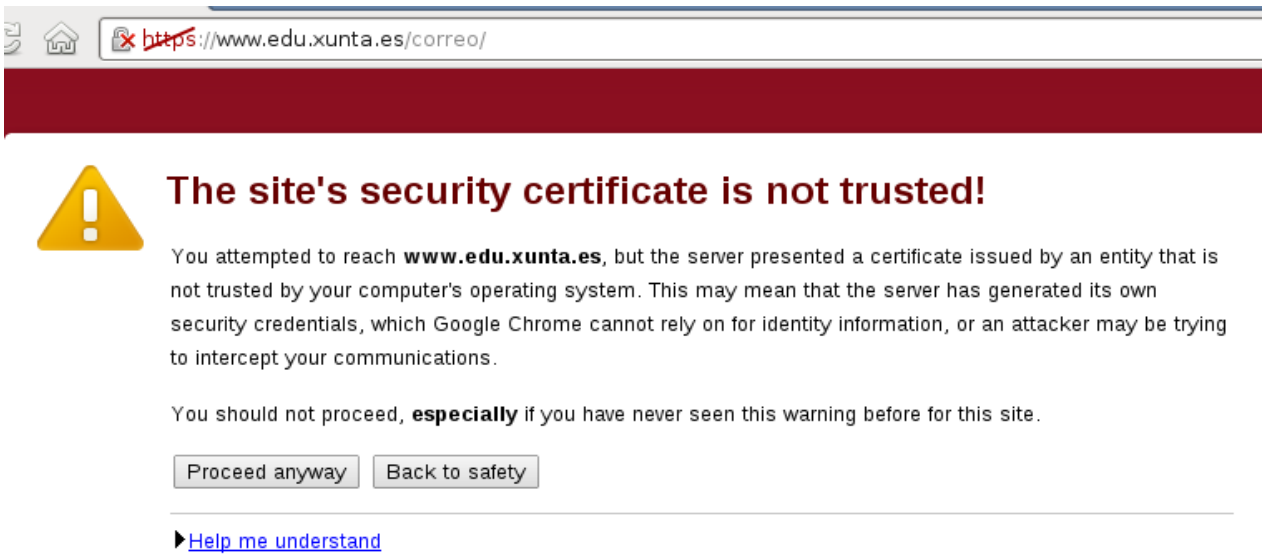

Fig. 7: Aviso de que non se pode comprobar a identidade do servidor (Chrome)

No caso do navegador Google Chrome, nesta pantalla temos a posibilidade de conectar de tódolos xeitos co servidor por esta vez, pero volverá a saír o mesmo aviso a próxima vez. Isto non garante a seguridade, xa que non se comproba a identidade do servidor ao que nos estamos conectando. Se establecemos a conexión nestas condicións, este navegador amosará na barra de dirección, o protocolo *https* tachado en vermello para recordarnos que a conexión non está garantida.
Para facer as cousas ben e garantir a seguridade debemos instalar nos nosos navegadores o

certificado da FNMT. Este certificado podémolo descargar nas seguintes direccións:

- Páxina de descarga (https://www.sede.fnmt.gob.es/descargas/certificados-raiz-de-la-fnmt)
- Descarga directa

Instalación do certificado da FNMT en distintos navegadores:

- MS Internet explorer (Versión 9 en Windows 7):
    1. Imos ao menú *Ferramentas*, *Opcións de Internet*. Imos á pestaña *Contido*, e pinchamos no botón *Certificados*
    2. Imos á pestaña E*ntidades de certificación raíz de confianza* e comprobamos se existe xa unha entrada para "FNMT Clase 2 CA". No caso de existir xa non facemos nada máis.
    3. Se non existe pinchamos no botón *Importar*, que abre o asistente de importación de certificados.
    4. Pinchamos en *Seguinte*.
    5. Pinchamos no botón *Examinar* e buscamos no ordenador o ficheiro F*NMTClase2CA.cer* que descargamos antes. Pinchamos en *Seguinte*.
    6. Marcamos a opción "*Selecionar automaticamente o almacen de certificados...*" Pinchamos en *Seguinte*.
    7. Pinchamos en *Finalizar*. Recibimos un aviso de que a importación se fixo con éxito.

- Google Chrome (en Windows):
    1. Imos á páxina de configuración do Google Chrome, ben polo botón de menú, ou ben escribindo a dirección *chrome://settings/*
    2. Ao final da páxina pinchamos no enlace *Mostrar opcións avanzadas...*
    3. Buscamos a sección *HTTPS/SSL* e pinchamos en *Administrar certificados*.
    4. Buscamos se xa existe unha entrada "FNMT Clase 2 CA", ou ben na pestaña *Entidades de certificación intermedias*, ou ben na pestaña *Entidades de certificación raiz de confianza*. No caso de existir xa non facemos nada máis.
    5. Se non existe pinchamos no botón *Importar* de calquera das dúas pestañas anteriores.
    6. Ábrese o asistente para importar certificados e seguimos os mesmos pasos descritos para o navegador MS Internet Explorer a partir do paso 4. Estes dous navegadores en Windows comparten a configuración de certificados.

- Mozilla Firefox (Versión 30.0 – Windows/Linux):
    1. Abrimos a ventana de *Opcións/Preferencias*, ben polo menú *Ferramentas/Editar*, ou polo botón de menú.
    2. Na ventana de opcións pichamos no icono de *Avanzadas*, á dereita de todo.
    3. Agora pinchamos na pestaña *Certificados*, á dereita de todo.
    4. Pinchamos no botón *Ver certificados*. Abre unha nova ventana.
    5. Imos á pestaña *Autoridades* e buscamos se existe unha entrada para *FNMT: FNMT Clase 2 CA – FNMT*. No caso de existir xa non facemos nada máis.
    6. Se non existe pinchamos no botón *Importar* e buscamos no ordenador o ficheiro *FNMTClase2CA.cer* que descargamos antes. Pinchamos en *Abrir*.
    7. Ábrese unha ventana con tres opcións que nos pregunta para que se debe usar este certificado, marcamos as tres opcións. *Aceptamos*.
    8. Aceptamos de novo. Xa está.

- Google Chrome (en Linux):
    1. Seguimos os pasos 1, 2 e 3 descritos para Chrome en Windows.
    2. Seguimos os pasos 5, 6 e 7 descritos para Mozilla Firefox.