EDUCACIÓN
SECRETARÍA DE EDUCACIÓN PÚBLICA

TECNM MÉXICO

SONORA
TIERRA DE OPORTUNIDADES

SECRETARÍA DE EDUCACIÓN Y CULTURA

ITESCA
Instituto Tecnológico Superior de Cajeme

ITESCA

INSTITUTO TECNOLÓGICO SUPERIOR DE CAJEME

DEPARTAMENTO DE SISTEMAS

ESTÁNDARES PARA EL DESARROLLO DE SOFTWARE INSTITUCIONAL

OCTUBRE 2024.

SONORA
TIERRA DE OPORTUNIDADES

GLOSARIO DE TÉRMINOS

1. **Ambiente de desarrollo:** el área de trabajo que proporciona condiciones suficientes al programador para realizar la generación y pruebas de código antes de pasar al ambiente de producción.
2. **Ambiente de producción:** el área de trabajo que proporciona las condiciones necesarias a los sistemas ya liberados para su operación y en donde se encuentran los datos e información de la solución.
3. **Coordinación de Desarrollo de Software:** el área involucrada de forma directa en el desarrollo de código fuente, módulos, funcionalidades y otros elementos de un sistema informático.
4. **Base de Datos:** el conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso.
5. **Código fuente:** el conjunto de líneas de texto escritas en algún lenguaje de programación que contiene las instrucciones dadas a la computadora para realizar la funcionalidad deseada de un programa.
6. **Entidad:** la representación de un objeto o concepto del mundo real que se describe en una base de datos.
7. **Entorno de desarrollo integrado:** la combinación de herramientas que automatizan o soportan al menos una gran parte de las fases del desarrollo de sistemas informáticos.
8. **Estándar:** el conjunto de especificaciones técnicas u otros criterios precisos para ser usados consistentemente como reglas, guías, o definiciones de características para asegurar la interoperabilidad o compatibilidad de los productos, procesos y servicios.
9. **Evaluación de riesgos:** la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operación del Instituto Tecnológico Superior de Cajeme.
10. **Fases de desarrollo:** a cada una de las etapas que componen el proceso de desarrollo de un sistema informático, definidas como: Análisis, Diseño, Desarrollo, Pruebas e implementación.
11. **Firma Electrónica:** es un conjunto de datos que se adjuntan a un mensaje electrónico, cuyo propósito es identificar al emisor del mensaje como autor legítimo de éste, tal y como si se tratara de una firma autógrafa.
12. **Mantenimiento del sistema:** la obtención de una nueva versión del sistema informático, necesaria para eliminar errores detectados o incorporar mejoras en el diseño o en la obtención de resultados.
13. **Manual:** al presente documento denominado Manual de Estándares para el Desarrollo de Sistemas Informáticos en el Instituto Tecnológico Superior de Cajeme.
14. **Plataforma de desarrollo:** el entorno de software común en el cual se desenvuelve la actividad de desarrollo de sistemas informáticos.
15. **Proyecto informático de desarrollo de sistemas:** el conjunto de acciones que implican la aplicación de recursos para la automatización de procesos, o parte de ellos, mediante la creación de un sistema informático o la modificación de uno existente.

GLOSARIO DE TÉRMINOS

16. **Responsable de desarrollo de sistemas de información:** el servidor público que representará, dirigirá y coordinará al área que desarrolla el proyecto informático durante todas sus fases.
17. **Sistema informático:** el conjunto de componentes físicos (hardware), lógicos (software) y humanos que se organizan para realizar una tarea o un proceso específico.
18. **Sistema de consulta:** el sistema que precisan la interacción con el usuario para petición de datos y elección de opciones, pero que no requieren adicionar, eliminar, modificar o alterar la información que se está consultando.
19. **Sistema transaccional:** el sistema diseñado para recolectar, almacenar, modificar y recuperar información que es generada por las transacciones. Una transacción un proceso que genera o modifica la información que se encuentran eventualmente almacenados en un sistema de información.

    19.1. **Software:** el conjunto general de programas que conforman el equipamiento lógico o soporte lógico de una computadora digital.
    19.2. **Vulnerabilidad:** cualquier debilidad que puede explotarse para causar pérdida o daño al sistema.
    19.3. **Web services:** tecnología que se utiliza para el intercambio de datos.

OBJETO

Establecer el marco tecnológico de referencia para el desarrollo y documentación de los sistemas informáticos que requiere el Instituto Tecnológico Superior de Cajeme, mediante la definición de los estándares técnicos aplicables.

ÁMBITO DE APLICACIÓN

Los estándares contenidos en el presente Manual son de observancia obligatoria para todo el personal que labora en el Instituto Tecnológico Superior de Cajeme o que es contratado con terceros para que realice actividades inherentes al diseño, desarrollo y documentación de sistemas informáticos.

DISPOSICIONES GENERALES

Proceso de solicitud para el desarrollo de sistemas informáticos

El personal y áreas de desarrollo de sistemas informáticos deben aplicar el procedimiento registrado en el sistema de gestión de calidad de ITESCA, PDA 08.08 DESARROLLO DE SOFTWARE Y PROVEEDOR DE DATOS INSTITUCIONALES.

PLATAFORMA DE DESARROLLO

La plataforma de desarrollo de los sistemas informáticos en el Instituto Tecnológico Superior de Cajeme, se define en la tabla siguiente:

TABLA 1: Plataforma de Desarrollo:

Tipo	Tipo de Desarrollo	Tecnología/Características
A. Sistema de Consulta B. Sistema Transaccional	I. Escritorio II. Web	· Lenguaje de programación · Entorno integrado de desarrollo (IDE) · Servidor de aplicaciones · Sistemas operativos · Interface de usuario · Herramientas para generar reportes · Servicios · Sistema manejador de base de datos · Seguridad

Lenguajes de programación

Los sistemas informáticos deben llevarse a cabo en estas opciones de lenguajes de programación:

TABLA 2: Lenguajes de programación:

Escritorio / Web
C# PHP JavaScript CSS VBSCRIPT Visual Basic

Entorno Integrado de Desarrollo (IDE)

Las herramientas IDE que se establecen para el desarrollo de aplicaciones (editor de código, compilador, depurador y constructor de interfaz gráfica), comprenden las siguientes opciones como recomendación:

TABLA 3: Entorno integrado de desarrollo (IDE)

Escritorio	Web
A. MS Visual Studio	I. DreamWeaver II. Visual Studio Code

Servidor de Aplicaciones

Para la implementación de las aplicaciones en ambientes de desarrollo, y producción se debe utilizar alguna de las siguientes opciones de preferencia:

TABLA 4: Servidor de aplicaciones

Servidor de Aplicaciones web
A. MS IIS

Sistemas Operativos

Para racionalizar la gestión de los recursos de hardware y proveer servicios para la ejecución de los sistemas informáticos, como opciones se incluyen:

TABLA 5: Sistemas operativos

Escritorio	Web
A. Windows	I. Windows Server

Interfaz de Usuario

La interfaz de usuario del sistema informático desarrollado debe cumplir con las disposiciones relativas a la imagen institucional. Los estándares para los elementos de imagen, audio y video para la presentación de información, como opciones se incluyen:

TABLA 6: Elementos de imagen, audio y video

Imagen	Audio y Video
GIF JPEG JPG PNG TIFF SVG	MPEG-1 Audio Layer III (MP3) MPEG-2 Audio Layer III (MP3) MPEG-4 Windows Media Video Real Media

Herramientas para generar reportes

Las herramientas de reporte serán aquellas que están incorporadas en los IDE a los que hace referencia este manual. Como opciones se incluyen:

TABLA 7: Reportadores

Re porteadores
A. Crystal Reports B. FPDF C. HTML to PDF

Sistemas en Red

Para los sistemas que basan su comunicación en TCP/IP, los protocolos que podrán utilizar para comunicarse serán *http, https, ssh* y/o *ftp.* Cuando se requiera utilizar un protocolo diferente, debe obtenerse antes el visto bueno del jefe de Departamento de Sistemas.

Sistemas manejadores de base de datos.

Los sistemas manejadores de bases de datos comprendidos en el estándar son las siguientes opciones como recomendación:

TABLA 8: Sistemas manejadores de base de datos

Escritorio / Web
A. MS SQL Server

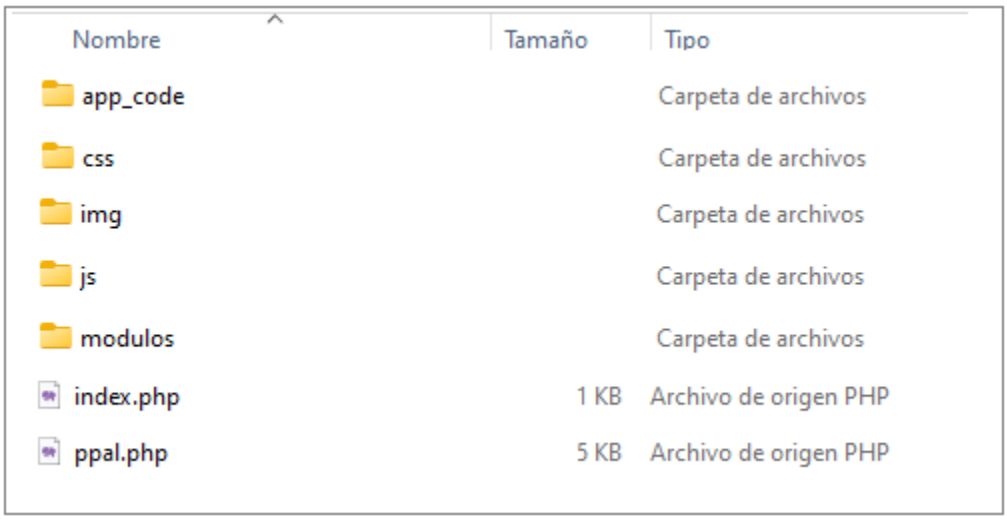
Plataforma tecnológica para la seguridad en el desarrollo de sistemas informáticos.

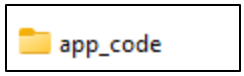
En la matriz siguiente se establece la plataforma tecnológica con las herramientas para una operación segura en los sistemas informáticos, como opciones se incluyen:

TABLA 9: Matriz de plataforma tecnológica para la seguridad en el desarrollo de sistemas informáticos

Aplicación	Escritorio	Web
a) Seguridad de la Información	I. Autenticación por BD.	i. Certificado digital SSL. ii. Autenticación por BD.
b) Conexiones Seguros	I. Secure Socket Host (SSH) II. VPN	i. Https ii. Uso de data Source / Pool de conexiones iii. Archivo de conexiones de cifrado. iv. Secure Socket Host(SSH) v. VPN
c) Respaldos	I. Es responsabilidad del área desarrolladora definir la periodicidad de sus respaldos de tal manera que no se afecten los proyectos en desarrollo	

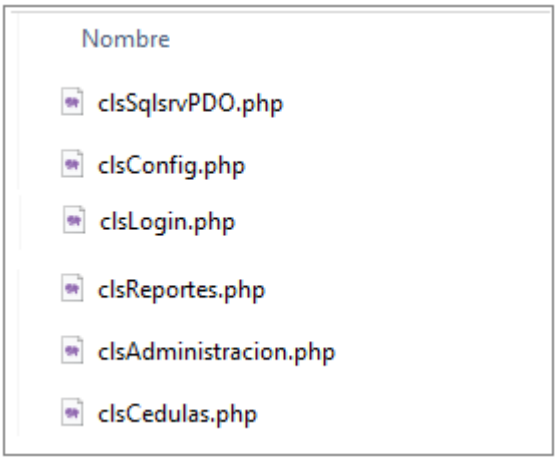
Estructura básica de un proyecto institucional de desarrollo de software.
Usando PHP Versión 7.0.33





Resguarda las clases por entidades, las clases contienen métodos que servirán para conectar a la base de datos y posteriormente extraer, ingresar, borrar o actualiza información.

Ejemplo:



Ejemplo:

clsUsuarios

```php
<?php
require_once("clsSqlsrvPDO.php");

class clsUsuarios {
    public $objSqlsrv;

   //Constructor
    public function __construct(){
      $this->objSqlsrv = new clsSqlsrv();
    }

    // Consulta de usuario por ID
    public function getDatosUsuario($user, $MQ=false){
        return $this->objSqlsrv->ejecutaSPSafe('dbDemo..sp_getUsuariobyID', array($user), $MQ); //se manda un array con parametros en el mismo orden que el SP los espera
    }

    // Listar usuarios de la base de datos
    public function getUsuarios($MQ=false){
        return $this->objSqlsrv->ejecutaSPSafe('dbDemo..sp_getUsuarios', array(), $MQ); //se manda un array vacio cuando no hay parametros
    }

    // guarda un usuario en la base de datos
    public function guardarUsuarios($sNombre, $sEmail, $sTelefono, $MQ=false){
        $this->objSqlsrv->ejecutaSPSafe('dbDemo..sp_RegistraUsuario', array($sNombre, $sEmail, $sTelefono), $MQ);
    }

    // eliminar un usuario en la base de datos
    public function eliminarUsuario($sID, $MQ=false){
        $this->objSqlsrv->ejecutaSPSafe('dbDemo..sp_EliminarUsuario', array($sID), $MQ);
    }

    // Actualizar un usuario en la base de datos
    public function actualizarUsuario($sID, $sNombre, $sEmail, $sTelefono, $MQ=false){
        $this->objSqlsrv->ejecutaSPSafe('dbDemo..sp_ActualizaUsuario', array($sID, $sNombre, $sEmail, $sTelefono), $MQ);
    }
}
```

clsSqlsrvPDO.php

se incluye en cada clase, y Sirve para conectar al motor de base de datos SQL SERVER y ejecutar consultas o Procedimientos almacenados.

La clase tiene un método para ejecutar un Store Procedure **ejecutaSPSafe** el cual recibe 3 parámetros,

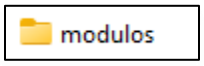
1. Nombre del **StoreProcedure**
2. Parámetros en un array, los parámetros deben ir en el mismo orden que el SP los espera.
3. Es una variable booleana para depurar, cuando es true, muestra la consulta que se está ejecutando.

clsConfig.php

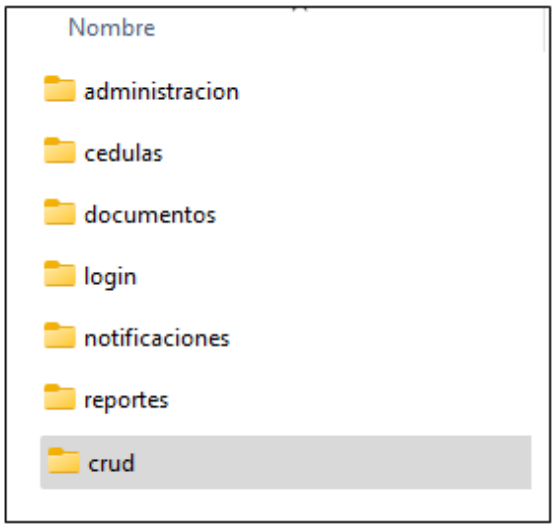
Sirve para establecer los datos necesarios para la cadena de conexión con el motor de base de datos.

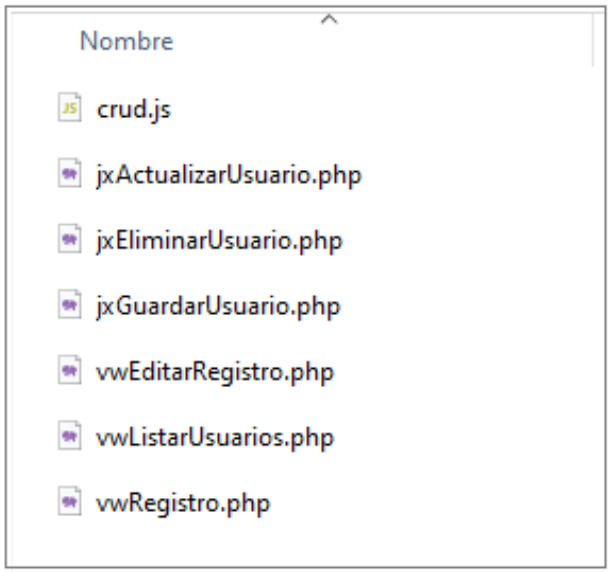
```php
<?PHP
class clsConfig {
        public $BD_HOST;
        public $BD_USER;
        public $BD_PWS;
        public $BD_DB;

       public function __construct() {
         $this->BD_HOST = "192.1.1.17";  // servidor
         $this->BD_USER = "sa";  // usuario de la base de datos
         $this->BD_PWS = "123456"; // password
         $this->BD_DB = "dbDemo"; // base de datos
         $this->DEPURAR = false; // depurar
       }
}
?>
```



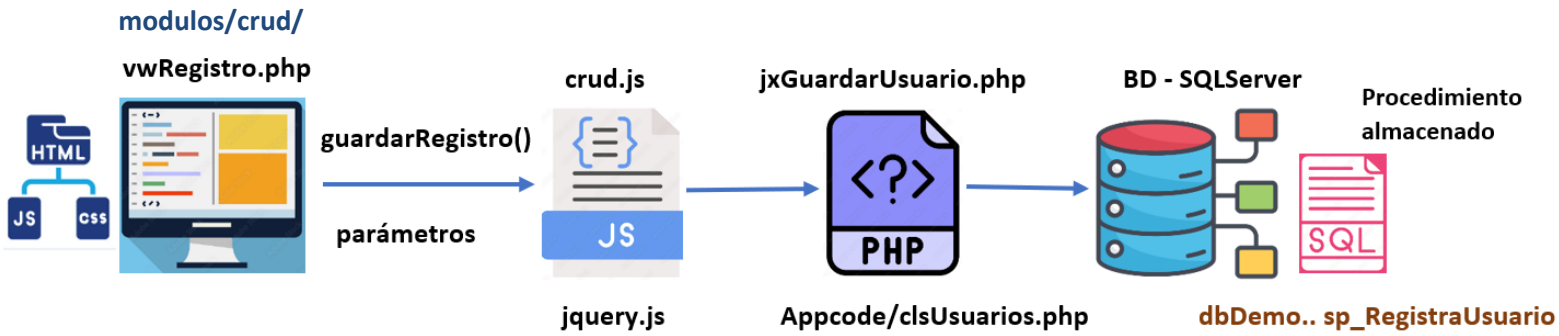
Contiene carpetas que se clasifica según las funciones o módulos del sistema, los cuales agrupan una o varias funcionalidades y pantallas. Para su creación se puede considerar las opciones disponibles en el menú principal del sistema.

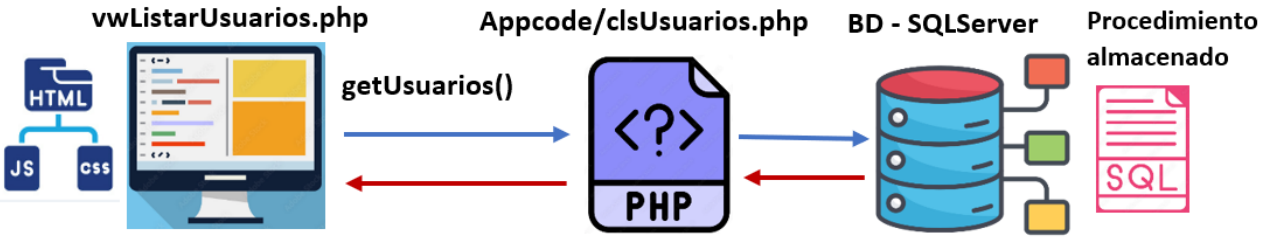


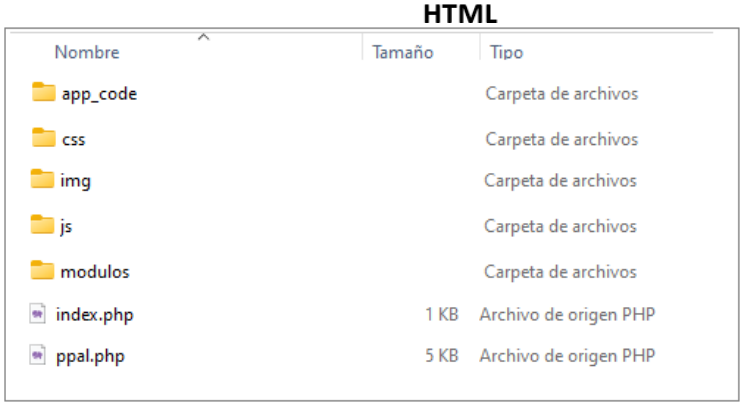


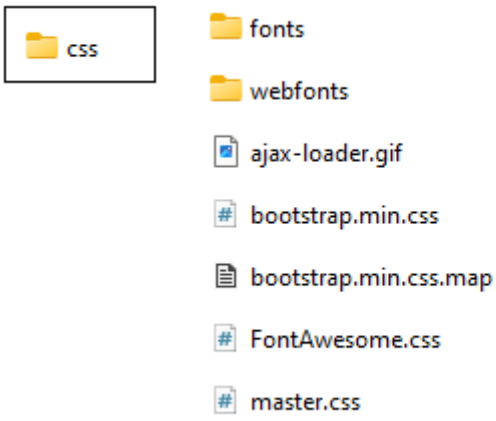
Dentro de cada carpeta vamos a encontrar archivos con prefijos específicos según la funcionalidad de cada archivo.

Para pantallas, vamos a especificar el nombre iniciando con la palabra **vw** (view).
Los **vw** están compuestas por HTML+CSS+JavaScript, realizan llamadas a PHP para recibir datos de la BD, via JavaScript Asíncrono.
Los archivos **jx** son archivos PHP que sirven de controlador, hacen uso de las clases para ejecutar una acción especifica en la base de datos, conectan los **vw** con la base de datos.



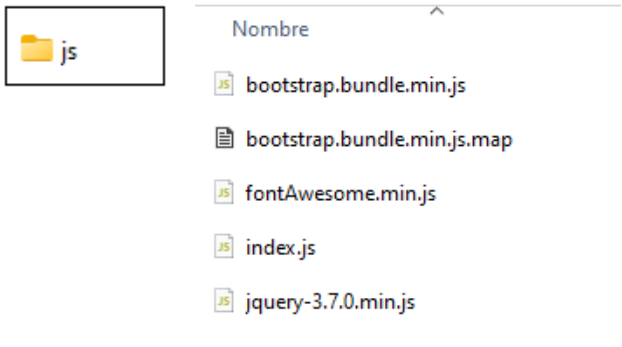






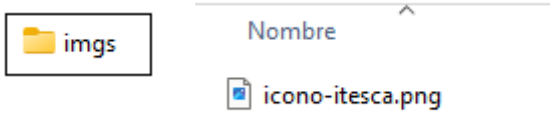
Repositorio de hojas de estilo del proyecto,

- Framework de CSS Bootstrap v5.3.x
- Fuente de iconos Font Awesome v6.x
- Fonts.
- Hojas de estilo propias. master.css



Repositorio de JavaScript

- Framework de CSS Bootstrap v5.3.x
- Fuente de iconos Font Awesome v6.x
- Jquery 3.7.x
- index.js JavaScript propio para
- uncionamiento general o de la raíz.



Recursos gráficos del proyecto

Archivos PNG o JPG

SEGURIDAD EN EL DESARROLLO DE SISTEMAS INFORMÁTICOS.

Ambientes de trabajo

El responsable del proyecto debe de considerar y gestionar ante el área que designe como responsable, dos ambientes de trabajo: ambiente de desarrollo, y ambiente de producción.

Manejo de usuarios

Como parte de la seguridad en el desarrollo de sistemas, se debe asignar a todas las cuentas de usuario del sistema solo los permisos autorizados sobre el sistema y la información que maneje.

Administración de sesiones

La función de cerrar sesión debe terminar completamente con la sesión o conexión asociada y liberar todos los recursos que se le hayan asignado.
Establecer el tiempo de vida de la sesión mínimo previendo que se puedan ejecutar los procesos sin interrupción, debiendo tomar en cuenta minimizar los riesgos en la seguridad.
Proteger la información sobre las sesiones del lado del servidor implementando los controles de acceso apropiados, con independencia de aquellas medidas establecidas del lado del cliente.

Control de acceso

Las aplicaciones desarrolladas en el Instituto Tecnológico Superior de Cajeme deben utilizar un mecanismo de control de acceso que garantice la Seguridad Informática.
Se deberá proteger con algún carácter (por ejemplo, asterisco) la contraseña ingresada al presentar retroalimentación al usuario en pantalla.

Autenticación

Los mensajes de retroalimentación al usuario sobre fallos en la autenticación no deben indicar cuál parte específica de la autenticación fue incorrecta. Cuando se transmita información que deba mantenerse reservada o que pueda poner en riesgo la confidencialidad de datos, se deberán utilizar protocolos que no dejen expuesta la información que se transmite de una aplicación a otra.

a) Se deberá evitar el uso de llamadas a sistemas que dejan expuestos los parámetros que se envíen. En la comunicación entre sistemas, los parámetros deberán enviarse encriptados.
b) La función de cerrar sesión debe estar disponible en todas las páginas protegidas por autenticación.
c) El sistema deberá contener mecanismos para verificar que se cierren todas las sesiones al abandonar la aplicación, cuidando que ningún recurso utilizado por la sesión quede pendiente de ser liberado.
d)
e) En medida de lo posible se deben registrar en bitácora todas las acciones del usuario, para detectar posibles amenazas e infiltraciones al sistema. La bitácora deberá contener los datos que permitan identificar al menos, el equipo desde donde se hizo el acceso, la hora y la cuenta del usuario con que se realizó la acción.
f) En ningún momento se deberá dejar por escrito en el código fuente de la aplicación o en archivos temporales sin encriptación, indicios como cuentas de usuario o contraseñas que puedan permitir acceder de manera automática a información restringida.

Autenticación

Los mensajes de retroalimentación al usuario sobre fallos en la autenticación no deben indicar cuál parte específica de la autenticación fue incorrecta. Cuando se transmita información que deba mantenerse reservada o que pueda poner en riesgo la confidencialidad de datos, se deberán utilizar protocolos que no dejen expuesta la información que se transmite de una aplicación a otra.

g) Se deberá evitar el uso de llamadas a sistemas que dejan expuestos los parámetros que se envíen. En la comunicación entre sistemas, los parámetros deberán enviarse encriptados.
h) La función de cerrar sesión debe estar disponible en todas las páginas protegidas por autenticación.
i) El sistema deberá contener mecanismos para verificar que se cierren todas las sesiones al abandonar la aplicación, cuidando que ningún recurso utilizado por la sesión quede pendiente de ser liberado.
j) En medida de lo posible se deben registrar en bitácora todas las acciones del usuario, para detectar posibles amenazas e infiltraciones al sistema. La bitácora deberá contener los datos que permitan identificar al menos, el equipo desde donde se hizo el acceso, la hora y la cuenta del usuario con que se realizó la acción.
k) En ningún momento se deberá dejar por escrito en el código fuente de la aplicación o en archivos temporales sin encriptación, indicios como cuentas de usuario o contraseñas que puedan permitir acceder de manera automática a información restringida.

Seguridad de datos

a) Establecer perfiles y/o roles con los privilegios mínimos necesarios que restrinjan el acceso a las funcionalidades, datos, objetos y sistemas de información que requieran para realizar sus tareas.
b) Eliminar todos los archivos y memoria de trabajo temporales cuando no sean requeridos.
c) Eliminar las cuentas predefinidas y que no son necesarias para las reglas del negocio.
d) Utilizar controles criptográficos para el resguardo de datos, cuando así se determine de la evaluación de riesgos realizada por el responsable de la Información.

Manejo de archivos

a) Transferir al servidor únicamente los tipos de archivo requeridos por las reglas del negocio, verificando su estructura.
b) Asegurar que los archivos y recursos de la aplicación sean de sólo lectura.

Manejo de errores y/o excepciones

a) Utilizar manejadores de errores y/o excepciones que no muestren información de depuración de código (ejemplo: no enviar querys a consola) o de memoria.
b) Implementar mensajes de error genéricos que reemplacen los mensajes de error del sistema.

Configuración de los sistemas

a) Remover código o funcionalidad de testeo que ya no sea útil, previo a realizar la puesta en producción.
b) Remover información innecesaria en los cabezales de http de respuesta referidas al sistema operativo, versión del servidor web y frameworks de aplicación.
c) La publicación de aplicaciones y sus posibles actualizaciones en el ambiente de producción sólo debe realizarla el equipo de desarrolladores de la coordinación de desarrollo de software.
d) El desarrollador deberá coordinarse con el coordinador de desarrollo de software para la afinación de las aplicaciones previa y durante la operación del sistema.

Respaldos y restauraciones.

a) El respaldo de un proyecto de desarrollo de sistemas informáticos incluye:
   1.1 Código fuente en su última versión conforme a la versión publicada en ambiente de producción.
   1.2 Archivos de recursos, librerías, componentes y otros elementos utilizados por el sistema.
   1.3 Consideraciones y archivos que sean necesarios para la reconstrucción y restauración del sistema.
b) Los medios para el respaldo de lo definido en el inciso anterior deben ser externos al equipo de trabajo, como: Google Drive, discos duros externos propios del Instituto.
c) Los respaldos y los procedimientos de restauración deben probarse conforme a los tiempos y períodos que defina el responsable de la información, para verificar que sean funcionales y que los medios utilizados continúen vigentes.
d) Los medios de almacenamiento deben encontrarse adecuadamente identificados, a través de una etiqueta que maneje como mínimo la fecha de generación del respaldo, nombre de la aplicación, tipo de información y periodo que se está respaldando.
e) Los procesos de respaldo deben coordinarse con los administradores de los servidores (de aplicación o base de datos) para que se ejecuten de forma programada. Los respaldos generados deberán conservarse en al menos tres ciclos (diario, semanal, mensual, entre otros.), que defina el responsable de la información.
f) Al término del proyecto de desarrollo, se debe generar un respaldo final que deberá conservarse como respaldo histórico. En caso de actualización al sistema, se debe generar la nueva versión del respaldo final.
g) Los formatos de los respaldos de base de datos a utilizar son:
   SQL Server: .ABF, .BAK y .MDF

APROBACIÓN Y CREACIÓN DEL MANUAL ESTÁNDARES PARA EL DESARROLLO DE SOFTWARE INSTITUCIONAL

Creado por todo el personal del área de sistemas de software y aprobado por jefe Departamento de Tecnologías de la Información y comunicación.

Ing. Tadrio Eugenio Terán Serrano

Jefe Departamento de Tecnologías de la Información y comunicación. TIC

FECHA DE CREACIÓN: 30 de marzo de 2022

ULTIMA MODIFICACIÓN: 28 de octubre de 2024

VERSIÓN: 1.4