ESTADO DE SONORA

Gobierno del
Estado de Sonora

Secretaría **de la Contraloría General**

Subsecretaría de **Desarrollo Administrativo y Tecnológico**

ESTÁNDARES PARA EL DESARROLLO DE SISTEMAS INFORMÁTICOS EN EL GOBIERNO DEL ESTADO DE SONORA

JUNIO, 2017.

SONORA
UNIDOS LOGRAMOS MÁS

GLOSARIO

a) **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 preproducción;

b) **Ambiente de preproducción:** el área de trabajo que proporciona condiciones suficientes al programador para probar y ajustar la funcionalidad de los módulos antes de implementarlos en el ambiente de producción;

c) **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;

d) **Áreas desarrolladoras:** las áreas involucradas de forma directa en el desarrollo de código fuente, módulos, funcionalidades y otros elementos de un sistema informático;

e) **Base de Datos:** el conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso;

f) **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;

g) **DDS:** Dirección de Desarrollo de Software;

h) **Entidad:** la representación de un objeto o concepto del mundo real que se describe en una base de datos;

i) **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;

j) **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;

k) **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 Gobierno del Estado de Sonora;

l) **Fases de desarrollo:** a cada una de las etapas que componen el proceso de desarrollo de un sistema informático, definidas como: Iniciación, Elaboración,

Construcción y Transición;

m) **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;

n) **Identificador:** la descripción de un objeto mediante el uso de abreviaturas, separadas por un guión de piso si la descripción consta de más de dos palabras significativas, o bien, cuando el lenguaje lo reconozca, iniciando con mayúscula cada palabra significativa;

o) **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;

p) **Manual:** al presente documento denominado Manual de Estándares para el Desarrollo de Sistemas Informáticos en el Gobierno del Estado de Sonora;

q) **Metadatos:** los datos estructurados que describen las características de contenido, calidad, condición, acceso y distribución de la información estadística o geográfica;

r) **Modelo de datos:** conjunto de conceptos que nos permiten describir los datos, las relaciones que existen entre ellos, la semántica y las restricciones de consistencia;

s) **Plataforma de desarrollo:** el entorno de software común en el cual se desenvuelve la actividad de desarrollo de sistemas informáticos;

t) **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;

u) **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;

v) **SDAT:** Subsecretaría de Desarrollo Administrativo y Tecnológico;

w) **Sistema informático:** el conjunto de componentes físicos (hardware), lógicos (software) y humanos que se organizan para realizar una tarea o un proceso específico;

x) **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;

y) **Sistema por lotes:** el sistema diseñado para la ejecución de un programa sin el control o supervisión directa del usuario. Se utiliza en tareas repetitivas sobre

grandes volúmenes de información;

z) **Sistema transaccional:** el sistema diseñado para recolectar, almacenar, modificar y recuperar información que es generada por las transacciones. Una transacción es un proceso que genera o modifica la información que se encuentran eventualmente almacenados en un sistema de información;

aa) **Software:** el conjunto general de programas que conforman el equipamiento lógico o soporte lógico de una computadora digital;

bb) **Unidad Administrativa:** es perteneciente a una estructura básica de una dependencia, facultada para ejercer gasto con el fin de llevar a cabo actividades que conduzcan al cumplimiento de objetivos y metas establecidas en los programas de una dependencia o entidad del Gobierno Estatal;

cc) **Vulnerabilidad:** cualquier debilidad que puede explotarse para causar pérdida o daño al sistema.

dd) **Webservices:** tecnología que utiliza un conjunto de protocolos y estándares que sirven para intercambiar datos entre aplicaciones;

OBJETO

Establecer el marco tecnológico de referencia para el desarrollo y documentación de los sistemas informáticos que requiere el Gobierno del Estado de Sonora, 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 Gobierno del Estado de Sonora o que es contratado con terceros para que realice actividades inherentes al diseño, desarrollo y documentación de sistemas informáticos.

DISPOSICIONES GENERALES

a) El desarrollo de sistemas informáticos que lleven a cabo las Dependencias y/o Entidades del Gobierno del Estado de Sonora, deberá efectuarse con apego a las disposiciones que establecen en el Manual de Políticas y Estándares de Seguridad Informática, Políticas para la Emisión de Dictámenes Técnicos y Estándares para el Desarrollo de Sistemas Informáticos.

b) Los estándares definidos en este Manual comprende aquellos recursos de hardware y software que están alineados a la plataforma tecnológica de la Subsecretaría de Desarrollo Administrativo y Tecnológico. Cualquier otro recurso de desarrollo, diferente a los contenidos en este Manual y que se requiera implementar, deberá justificarse ante la SDAT; el soporte a los sistemas informáticos desarrollados con estándares diferentes deberán ajustarse a los niveles de servicio que la DDS ofrece;

c) El desarrollo de sistemas informáticos deberá realizarse bajo el esquema de tres ambientes de trabajo: ambiente de desarrollo, ambiente de pruebas y ambiente de producción.

   Las condiciones de operación de cada uno de los ambientes será determinado por la SDAT;

d) Todos los sistemas informáticos deberán contar con el modelo de base de datos y/o con las descripciones de las estructuras de datos utilizadas;

e) Todas las bases de datos relacionales deben pasar mínimo por la segunda forma normal el proceso de normalización;

f) Cualquier proyecto de desarrollo de un sistema informático deberá documentarse durante todas sus fases con base en los estándares, metodologías que se están utilizando, que para este efecto se establece lo siguiente:

Documentación para el desarrollo de sistemas informáticos

El personal y áreas de desarrollo de sistemas informáticos deben aplicar los siguientes estándares para la presentación de la documentación inherente al desarrollo de sistemas informáticos.

En caso de contar con una metodología tradicional de desarrollo deberá contar con la siguiente documentación:

- Guía de Levantamiento de Requerimientos.
- Plan de Trabajo.
- Lista de reuniones.
- Manual de Usuario.
- Manual Técnico.
- Lista de Capacitación.
- Acta de Entrega.

En caso de contar la metodología de desarrollo ágil SCRUM deberá contar con la siguiente documentación:

- Sprint de Planificación.
    - Planificación de Requerimientos.
    - Observaciones de Requerimientos.
    - Aceptación de Requerimientos.
- Historias de usuario de los Requerimientos.
- Lista de Capacitación.
- Acta de Entrega.

PLATAFORMA DE DESARROLLO

La plataforma de desarrollo de los sistemas informáticos en el Gobierno, se define en la tabla siguiente:

TABLA 1: Plataforma de Desarrollo:

Tipo	Tipo de Desarrollo	Tecnología/Características
A. Sistema de Consulta B. Sistema Transaccional C. Sistema por lotes	I. Escritorio II. Web III. Móvil	• 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 de preferencia en estas opciones de lenguajes de programación:

TABLA 2: Lenguajes de programación:

Escritorio/Móvil/Web
A. C# B. PHP C. Java D. JavaScript E. CSS F. Angular G. Objective-C, Swift H. Visual Basic I. Node JS J. Ruby K. Python

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/Móvil	Web
A. MS Visual Studio B. JDeveloper C. Eclipse D. Netbeans E. XCode F. Xamarin G. Android Studio H. App Code	I. MS Visual Studio II. Eclipse III. Netbeans IV. PHP Storm Sublime Text

Servidor de Aplicaciones

Para la implementación de las aplicaciones en ambientes de desarrollo, pruebas y producción se debe

utilizar alguna de las siguientes opciones de preferencia:

TABLA 4: Servidor de aplicaciones

Servidor de Aplicaciones
A. WebLogic B. MS IIS C. Apache/Tomcat D. Nginx E. Lite Speed

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	Móvil
A. Windows B. Linux C. Mac OS	I. Windows Server II. Linux RedHat, Ubuntu, Centos, Fedora, Debian, III. Unix Solaris	I. Windows II. Android III. iOS

Interfaz de Usuario

La interfaz de usuario del sistema informático desarrollado debe cumplir con las disposiciones relacionadas con la publicación de información del Gobierno del Estado en intranet, Internet y las 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 BNP	Quicktime MPEG-1 Audio Layer III (MP3) MPEG-2 Audio Layer III (MP3) MPEG-4 Windows Media Video Real Media Waw

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: Reporteadores

Reporteadores
A. Jasper Report B. IReports C. MS Reporting Services D. Dev Express Reports E. Crystal Reports F. FPDF G. Stimulsoft Reports H. Telerik Reporting I. HTML to PDF

Sistemas en Red

Para los sistemas que basen 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 área de la SDAT encargada de la Seguridad Informática.

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	Móvil
A. MS SQL Server B. Oracle C. MS Analysis Services D. SQLite E. PostgreSQL F. MySQL G. Microsoft Access	I. SQL Server II. SQLite

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	Móvil
a) Seguridad de la Información	I. Autenticación por BD. II. Autenticación de usuarios a través de un archivo cifrado. III. Cifrado de Datos (Hash, DES, 3DES, RSA, PGP, NIST, MD5, SHA1, SHA2).	i. Certificado digital SSL. ii. Certificado X.509. iii. Directorio Activo. iv. Autenticación por BD. v. Las llaves de acceso a servicios deberán estar cifradas. vi. Cifrado de datos (Hash, DES, 3DES, RSA, PGP, NIST, MD5, SHA1, SHA2)	a) Autenticación por BD. b) Autenticación de usuarios a través de un archivo cifrado. c) Cifrado de datos (Hash, DES, 3DES, RSA, PGP, NIST, MDS, SHA1, SHA2)
b) Conexiones Seguros	I. Secure Socket Host (SSH) II. FTPS III. VPN	i. FTPS, Https, RFC 2660 ii. Uso de data Source / Pool de conexiones iii. Archivo de conexiones de cifrado. iv. Secure Socket Host (SSH) v. VPN	a) Secure Socket Host (SSH)
c) Control de versiones	I. SVN Subversion Server II. Team Foundation Server III. GIT Versión Control System		
d) Respaldos	I. Es responsabilidad del área desarrolladora definir la periodicidad de sus respaldos de tal manera que no se afecten los proyectos en desarrollo		

Para implementar el uso de firma electrónica avanzada es necesario usar el Web Service llamado "FirmaCWS" para verificar y decodificar los pkcs #7, solicitar estampillas de tiempo y autenticar los certificados digitales expedidos por la Autoridad Certificadora del Gobierno del Estado de Sonora.

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, tres ambientes de trabajo: ambiente de desarrollo, ambiente de preproducción y ambiente de producción.

Manejo de perfiles

Como parte de la seguridad en el desarrollo de sistemas, se debe asignar a todas las cuentas de usuario del sistema un rol para delimitar los permisos asignados 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

Con excepción de aquellos sistemas de consulta que no requieren contraseña, las aplicaciones desarrolladas en el Gobierno del Estado deben utilizar el mecanismo de control de acceso que determine la SDAT de acuerdo con las disposiciones que establezca el Responsable de la Seguridad Informática de la SDAT.

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 dejen 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) Se deben registrar en bitácora todos los intentos de autenticación, incluyendo los fallidos, 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.
e) 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) No guardar los archivos transferidos en la misma ruta del sistema informático. Se debe utilizar un contenedor sin permisos de ejecución.
c) 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 queries a consola) o de memoria.
b) Implementar mensajes de error genéricos que remplacen los mensajes de error de 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 webmaster o el administrador del servidor de aplicaciones.
d) El desarrollador deberá coordinarse con el webmaster para la afinación de las aplicaciones previa y durante la operación del sistema.

Bitácoras

a) El desarrollador debe implementar un registro de las acciones que se realizan en su aplicación de aquellos eventos que son importantes como:
    a. Accesos al sistema en producción.
    b. Cambios en la información del sistema.
    c. Cambios de estado de los procesos.
b) Restringir el acceso a las bitácoras, sólo a personal autorizado.

Respaldos y restauraciones.

a) El respaldo de un proyecto de desarrollo de sistemas informáticos incluye:
    a. Código fuente en su última versión conforme a la versión publicada en ambiente de producción.
    b. Archivos de recursos, librerías, componentes y otros elementos utilizados por el sistema
    c. Descripción de la estructura de carpetas del proyecto.
    d. Descripciones de las estructuras de información que se utilizan.
    e. 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: comunidades de Sharepoint, servicios ftp, discos duros externos o sistemas SAN/NAS 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:
    a. Oracle: DMP y TXT
    b. SQL Server: .ABF, .BAK y .TXT
    c. PostgreSQL: .BACKUP, .SQL y .TXT
    d. Otros formatos: DBF, .PDB, .DAT, y copia directa o compactada en formato.