DigiPro, S.A. de C.V.

Hoja de revisión.

Este documento fue creado conforme a los requerimientos institucionales, revisado por el área de Control y Cumplimiento y aprobado por la Dirección de Tecnologías de Información.

Estamos de acuerdo con su contenido e implementación, en caso de haber cualquier modificación o adición a este documento, es responsabilidad del área emisora indicar la modificación o adición, previa aprobación de las áreas involucradas para evitar errores, incrementar el control interno y/o mejorar la productividad de los departamentos involucrados.

Control de Cambios		
Versión	**Cambios realizados**	**Fecha**
01	Actualización Nuevo Formato.	13/12/2024

Contenido

1 Política de Desarrollo Seguro.

Los sistemas de información construidos externa o internamente deben:

1. Validar la información suministrada por los usuarios antes de procesarla, teniendo en cuenta aspectos como: tipos de datos, rangos válidos, longitud, listas de caracteres aceptados, caracteres considerados peligrosos y caracteres de alteración de rutas, entre otros.
2. El sistema siempre debe contar con autenticación y autorización en cualquier sección para poder mostrar información.
3. En caso de tener información sensible cifrar dicha información.
4. Contar con opciones de desconexión o cierre de sesión de los aplicativos (logout) que permitan terminar completamente con la sesión o conexión asociada, las cuales deben encontrarse disponibles en todas las páginas protegidas por autenticación.
5. Proporcionar la mínima información de la sesión establecida, almacenada en cookies y complementos, entre otros.
6. La no divulgación de la información sensible en respuestas de error, incluyendo detalles del sistema, identificadores de sesión o información de las cuentas de usuarios; así mismo, se deben implementar mensajes de error genéricos.
7. Retirar todas las funcionalidades y archivos que no sean necesarios para los aplicativos, previo a la puesta en producción.
8. Prevenir la revelación de la estructura de directorios de los sistemas de información construidos.
9. Evitar incluir las cadenas de conexión a las bases de datos en el código de los aplicativos. Dichas cadenas de conexión deben estar en archivos de configuración independientes, los cuales se recomienda estén cifrados.
10. Certificar el cierre de la conexión a las bases de datos desde los aplicativos tan pronto como estas no sean requeridas.
11. Proteger el código fuente de los aplicativos construidos, de tal forma de que no pueda ser leído, descargado ni modificado por los usuarios o personas no autorizadas.
12. Asegurar que no se permita que los aplicativos desarrollados ejecuten comandos directamente en el sistema operativo.

2 Principios de Ingeniería para la Seguridad de la Información.

1. Implementar medidas de seguridad al sistema en desarrollo, para satisfacer los objetivos de seguridad de la organización.
2. Proteger la información que es utilizada por el sistema en desarrollo, mientras está siendo procesada, en tránsito y en almacenamiento.
3. Usar únicamente los lenguajes y versiones autorizados. Visual Studio pro 2022 y .Net Framework 4.8(o las últimas versiones soportadas).
4. Realizar análisis de vulnerabilidades y/o pruebas de penetración que aseguren que el sistema es, y sigue siendo, resistente frente a las amenazas que se esperan.
5. Implementar tecnología, hardware, firmware y software de confianza.
6. Limitar el acceso a funcionalidades que permitan activar y desactivar funciones de seguridad del sistema o cambiar los privilegios de los usuarios o programas.
7. Identificar y prevenir errores comunes, evitar el uso de tecnologías o componentes vulnerables (Aprender del pasado).
8. Identificar requerimientos y en su caso implementar mecanismos que permitan la alta disponibilidad, replicación o sincronización de información.
9. Revisión de código manual de cada PR (Pull Request) en base a las directrices que proporciona OWASP (OWASP Code Review Checklist), en este se categoriza por el siguiente TOP 10.
10. OWASP proporciona pautas y herramientas para ayudar a los desarrolladores a escribir código seguro.

3 Políticas Técnicas para el Desarrollo de Sistemas o Aplicaciones.

1. Uso de Queries Parametrizados:
    a. Objeto modelo relacional.
    b. Patrón de diseño de Active Record.
    c. Stored Procedures.
    d. Mecanismos de escape como codificador de ESAPI:
        i. EncodeForLDAP ().
        ii. Encoder.EncodeforOS ().
2. Prohibir las consultas SQL dinámicas dentro de su organización.
3. Validación de rol para crear, leer, actualizar o eliminar datos.
4. Limitar el uso de número máximo de solicitudes por segundo / minuto / hora que el usuario puede realizar.
5. No almacenar datos HTML codificados en la base de datos.
6. Uso de Cifrado fuerte de comunicaciones con servidores de aplicaciones y cualquier otro servidor o usuarios administrativos.
7. No utilizar cifrado de base de datos RDBMS, a nivel de tabla o fila.
8. Seguir estrictamente los estándares de Codificación que se implementan en el desarrollo de sistemas y aplicaciones. ver documento: SGSI-A8-D6MN04 Manual Estándares de Codificación.
9. Prohibido el uso de librerías shareware, freeware, bibliotecas, componentes de terceros o frameworks sin previa autorización, estas deben ser autorizadas por el responsable del área antes de poder ser utilizadas, estas deben ser evaluadas de acuerdo con el documento **SGSI-A8-D6PR13 Procedimiento End of Life**.
10. El desarrollador debe seguir las directrices que proporciona OWASP (OWASP Secure Coding Practices-Quick Reference Guide) ya que proporciona una orientación y buenas prácticas para un mayor énfasis en las prácticas de código seguro.
11. Desarrollar con pautas de seguridad que proporciona OWASP Application Security Verification Standard (ASVS) nos proporciona una lista de requerimientos que debe cumplir el código para que sea seguro.
12. El desarrollador debe utilizar herramientas que proporciona OWASP para la revisión de código ".Net Code análisis" para el caso desarrollo en .Net, y usar "MobSF" en caso del desarrollo móvil.

4 Restricciones a los Cambios en los Paquetes de Software.

- Analizar los términos y condiciones de la licencia a fin de determinar si las modificaciones se encuentran autorizadas.
- Evitar los cambios en software empaquetado.
- Todo cambio a sistemas de información o software debe seguir lo establecido en el procedimiento de gestión de cambios.
- Implementar control de versiones de los cambios realizados a sistemas de información de acuerdo con el documento **SGSI-A8-D6PO13 Política para la generación de versiones.**
- Guardar el código o software original realizando cambios sobre una copia perfectamente identificada en el TFS o GIT, por si fuera necesario aplicarlo a nuevas versiones.

5 Protección de Aplicaciones de Servicios de Transacciones

- La capa de negocio de los servicios web del I&DPortal es la que gestiona las transacciones donde se iniciar una transacción desde el cliente y coordinar la transacción dentro de la operación del servicio.
- La comunicación se realiza el protocolo SOAP, REST, indicando en la cabecera del mensaje las credenciales de transport. Y en el cuerpo las imágenes cifradas.
- El transport administra él envió del paquete usando un canal seguro TLS1.2 o TLS 1.3 y calculando el ancho de banda parametrizado en el servicio web WCF Filetransfer (arquitectura Windows Communication Foundation)

6 Pruebas de Seguridad al Sistema.

- Ejecución de las pruebas automatizadas utilizando herramientas especializadas para la seguridad del sistema, detectando vulnerabilidades antes del deployment a producción
    - Control de acceso
    - Autorización
    - Logs
    - Cifrado
    - Gestión de Sesiones

Ver documento: **SGSI-A8-D6PR11 Procedimiento de análisis de vulnerabilidades.**

7 Seguridad en las Redes Públicas.

- Implementar medidas de seguridad como el cifrado en tablas y datos de cualquier información confidencial.
- Evitar la pérdida o duplicación de información de la transacción.
- Utilizar canales y protocolos de comunicación seguros que permitan asegurar la confidencialidad, integridad, durante el procesamiento envío y recepción de información dentro y fuera de la aplicación.

8 Cumplimiento.

- ISO / IEC 27001:2022 / A.8 Controles tecnológicos / A.8.26 Requisitos de seguridad de las aplicaciones
- ISO / IEC 27001:2022 / A.8 Controles tecnológicos / A.8.25 Ciclo de vida de desarrollo seguro
- ISO / IEC 27001:2022 / A.8 Controles tecnológicos / A.8.32 Gestión del cambio
- ISO / IEC 27001:2022 / A.8 Controles tecnológicos / A.8.27 Arquitectura segura del sistema y principios de ingeniería
- ISO / IEC 27001:2022 / A.8 Controles tecnológicos / A.8.31 Separación de los entornos de desarrollo, prueba y producción
- ISO / IEC 27001:2022 / A.8 Controles tecnológicos / A.8.30 Desarrollo subcontratado
- ISO / IEC 27001:2022 / A.8 Controles tecnológicos / A.8.29 Pruebas de seguridad en desarrollo y aceptación