PLT-02_ POLÍTICA DE DESARROLLO SEGURO

Política de Desarrollo Seguro

Ámbito de difusión:	Uso Público/ Todo el personal de la empresa
Responsable	COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

CONTROL DE VERSIONES					
Versión		**Autor**	**Resumen de modificaciones**	**Revisado**	**Aprobado**
Nº	**Fecha de Aprobación**				
1.0	05/06/2023	INGENIERÍA Y SOLUCIONES	Creación del documento	CISO	CE

Índice

1 Introducción

En el plan se describen las actividades y funciones que se deberán implantar durante el desarrollo del proyecto para que se ajuste al ciclo de vida de desarrollo del sistema seguro (SSDLC, por sus siglas en inglés). En este estándar del ciclo de vida de desarrollo del sistema seguro se establecen los requisitos de seguridad que deben tenerse en cuenta y aplicarse en cada SSDLC.

Los requisitos seguros (y sus casos de prueba asociados) se refieren a los siguientes aspectos del sistema:

- software;
- hardware;
- entornos y herramientas de desarrollo;
- información/Almacenamiento y manipulación de datos;
- acceso físico a la infraestructura.

Para trabajar de manera efectiva, los requisitos del sistema constituyen el elemento principal y se identifican y tratan como parte del SSDLC.

La seguridad de la información es el segundo pilar y se tiene en cuenta e integra en cada fase del SSDLC.

Este plan se aplica a Grupo Oesía, a sus filiales y a sus subcontratistas.

2 Objeto y ámbito de aplicación

Esta Política se aplica en todos los sistemas de información que dan soporte a los servicios internos corporativos del grupo Oesia, así como los servicios de infraestructura, comunicaciones y puestos de trabajo que los soportan, debiendo ser conocida y cumplida por todo el personal involucrado en la operación y mantenimiento de los mismos.

3 Normativa aplicable

Es aplicable toda la normativa establecida en el documento **ORG-01-02_Marco Normativo,** que se actualizara de forma periódica

4 Responsabilidades

Las responsabilidades del Sistema de Gestión de Seguridad de la Información se recogen en:

- **ORG-01-01_Política de Seguridad de la información del Grupo Oesía**

5 Definiciones

Consultar **MS-01 MANUAL DE TERMINOLOGÍA DEL SGSI**

6 Desarrollo

6.1 Consideraciones generales (Principios para un desarrollo seguro)

El criterio general adoptado por el Grupo Oesía para el desarrollo de proyectos afectados por restricciones de seguridad es incorporar los requisitos de seguridad (donde consideramos los requisitos para todas las dimensiones del proyecto: diseño, desarrollo, pruebas, construcción/fabricación, implementación, etc.) en el estándar regular del ciclo de vida de desarrollo de sistema (DDESIGN) de Oesía, que se convierte en un **ciclo de vida de desarrollo del sistema seguro (SSDLC, por sus siglas en inglés)**.

Este enfoque consiste en incorporar en cada fase de desarrollo del proyecto, ya sea un proyecto tradicional en cascada o un proyecto desarrollado con técnicas ágiles, los requisitos de seguridad, que se consideran, prueban y validan como cualquier otro requisito del proyecto, de manera que así se garantiza que la seguridad esté integrada en el desarrollo del proyecto desde el principio en cualquier extensión o dimensión del proyecto.

A lo largo de todo el plan se han tenido en cuenta las siguientes consideraciones:

6.1.1 Interés general: desarrollo seguro

Todos los participantes en el proyecto conocen y se comprometen con la normativa indicada en este plan de desarrollo seguro.

Todos los participantes en el proyecto reciben formación de forma periódica sobre los requisitos de seguridad para mantener sus conocimientos sobre seguridad actualizados.

Producir

6.1.2 un diseño limpio y sostenible

Con el fin de evitar la complejidad, se utilizarán siempre que sea posible diseños sencillos y sostenibles (*software* y *hardware*), mediante arquitecturas conocidas y buenas prácticas (principio: la complejidad es enemiga de la seguridad).

El código sigue la normativa de codificación del Grupo Oesía para así asegurar unas buenas prácticas de codificación, sostenibilidad y futuras ampliaciones. Estos mismos principios deben seguirlos todos los proveedores externos.

Tanto el hardware como el software deberán cumplir los requisitos de seguridad establecidos como base para todos los productos desarrollados por Grupo Oesía con requisitos de desarrollo seguros; véanse los Requisitos comunes para el desarrollo de software seguro, Requisitos comunes para el

desarrollo de hardware seguro y Requisitos comunes para la securización del sistema operativo (estos documentos son accesibles solo para quienes cuenten con el nivel de clasificación apropiado y una autorización específica otorgada por Grupo Oesía, debido a su contenido sensible: contenido de clasificación militar y contenido de derechos de propiedad intelectual)

6.1.3 Entornos de desarrollo seguro

Los entornos de desarrollo, así como las herramientas empleadas para el desarrollo, han sido homologados y revisados por el CISO de Grupo Oesía.
Si, por cualquier motivo, la seguridad se reduce temporalmente para simplificar un paso concreto en el desarrollo, se crea una nueva tarea marcada como "deuda de seguridad". Una vez finalizado el desarrollo en cuestión, se abordan, cierran y prueban las deudas de seguridad (los casos de prueba aseguran que no se permite ningún fallo)

6.1.4 Repositorio de código securizado

El repositorio de documentación y código fuente siempre está protegido por las credenciales de la empresa para cada empleado y queda registrado quién ha realizado cada cambio y cuándo. La política de credenciales de los empleados se establece en los documentos **ORG-01-01_Política de Seguridad de la Información y PRO-OP.EXP.2.1 Configuración y acceso a redes y sistemas**

6.1.5 Canalización segura de compilación e implementación

La integración continua se adopta en el Grupo Oesía como un procedimiento estándar general para el desarrollo y entrega de proyectos.
La herramienta de código abierto (Jenkins) se emplea para la integración continua de manera que se asegura la capacidad de inspeccionar el código de la herramienta.
Cada nueva versión entregada se prueba automáticamente, incluidos los casos de prueba con los que se controlan los requisitos de desarrollo seguro (véase el apartado 6.4.56.4.5 Proteger la canalización de compilación e implementación), de manera que se asegura siempre que cada versión cumple los requisitos de seguridad establecidos para el proyecto.

6.1.6 Pruebas de seguridad continuas

Las auditorías internas se realizan aleatoriamente (al menos una vez cada seis meses) y se examinan los siguientes aspectos de la seguridad del proyecto:

- acceso a las instalaciones;
- acceso a los entornos y a la infraestructura de desarrollo;

- almacenamiento de datos y accesibilidad;
- puntos débiles de las credenciales.

6.1.7 Informes continuos

El especialista en ciclo de vida de desarrollo seguro asignado al proyecto genera un informe de seguridad en vivo.
Los puntos débiles detectados se comunican y tratan junto con los planes de corrección o, al menos, de mitigación asociados a las brechas/riesgos que se hayan detectado durante los análisis y evaluaciones de seguridad.
Los resultados que se obtengan se incluirán en el informe de seguridad generado para el proyecto en cada fase de diseño que se realice durante el desarrollo del proyecto (ya sea un desarrollo tradicional en cascada o un desarrollo ágil) y se indicará, en su caso, el riesgo asumido. Para los riesgos asumidos, se realizará un análisis de cada riesgo y se indicará el nivel de ocurrencia (casi nunca, rara vez, a menudo, muy a menudo); para los riesgos correspondientes al nivel "a menudo" o superiores, se indicará un plan de mitigación mediante sistemas alternativos.
Los nuevos desarrolladores se forman para garantizar que tengan un conocimiento adecuado del producto a través de la documentación que se haya ido generando a lo largo de la vida del proyecto. El nivel de clasificación de la documentación a la que tienen acceso los nuevos desarrolladores se determina en función de la necesidad de saber en cada caso.

6.2 Definición de funciones

En el Grupo Oesía se tendrán en cuenta las funciones que se indican a continuación para el desarrollo de cualquier sistema. Según el alcance del sistema, no estarán involucradas todas las funciones:

Función	Descripción
Comité de seguridad de la información del Grupo Oesía	Se encarga de proporcionar formación de forma periódica sobre seguridad/protección a todos los miembros del personal, formación especializada en seguridad/protección al personal seleccionado, actualizar el manual de seguridad, supervisar el mantenimiento adecuado de todo el equipo de seguridad/protección e implantar todos los procedimientos de seguridad/protección que sean necesarios.
CISO	Se encarga de la seguridad general de los sistemas de información de una organización, incluido el desarrollo y la implantación de

	políticas y procedimientos de seguridad, de la comprensión de la actividad de la red y de la preparación frente a posibles amenazas, de la supervisión de la respuesta a incidencias y de la planificación de la recuperación ante desastres, de la coordinación de las actividades de respuesta y recuperación cuando se produce una violación de seguridad o de datos, informando al superior jerárquico designado (CIO).
Ingeniero jefe	Se encarga de definir procedimientos y herramientas corporativos para el desarrollo del producto/proyecto y es el referente tecnológico para los equipos de desarrollo del Grupo Oesía.
Especialista en ciclo de vida de desarrollo seguro	Responsable corporativo asignado al proyecto para la entrega total del proyecto al equipo de implementación o a los clientes y garantizar el cumplimiento de los requisitos de seguridad establecidos en el Grupo Oesía.
Gestor del proyecto	Se encarga de la asignación de las funciones descritas en el documento a personas físicas. Determina el equilibrio entre los requisitos de seguridad y los beneficios comerciales del proyecto (junto con el especialista en ciclo de vida de desarrollo seguro).
Ingeniero de proyecto DevSecOps	Se encarga de la definición, despliegue y operación del entorno DevOps de acuerdo a los requerimientos del proyecto, incluida la política de acceso y la securización del entorno.
Ingeniero de *hardware* seguro del proyecto	Se encarga de la aplicación y del cumplimiento de los requisitos de seguridad establecidos en el documento de Requisitos comunes para el desarrollo de hardware seguro aplicable al proyecto. Asimismo, es el encargado de mantener actualizado el documento Requisitos comunes para el desarrollo de hardware seguro.
Ingeniero de software seguro del proyecto	Se encarga de la aplicación y del cumplimiento de los requisitos de seguridad establecidos en los documentos Requisitos comunes para el desarrollo de software seguro y Requisitos comunes para la securización de los sistemas operativos aplicables al proyecto. Asimismo, es el encargado de mantener actualizados los documentos Requisitos comunes para el desarrollo de software seguro y Requisitos comunes para la securización de los sistemas operativos.

6.3 Gestión de la seguridad del proyecto

6.3.1 Funciones involucradas

- Comité de seguridad de la información del Grupo Oesía
- Especialista en ciclo de vida de desarrollo seguro
- Gestor del proyecto

6.3.2 Requisitos de seguridad del proyecto

El primer requisito que hay que cumplir cuando se inicia un nuevo proyecto es identificar y evaluar todas las vulnerabilidades del mismo. El gestor del proyecto y el especialista en ciclo de vida de desarrollo seguro son los encargados de crear una matriz de vulnerabilidades para el proyecto, así como de su priorización y asignación al personal correspondiente para su gestión.
A la hora de priorizar las vulnerabilidades detectadas, se tiene en cuenta el equilibrio entre riesgo y beneficio. En caso de desacuerdo entre el gestor del proyecto y el especialista en ciclo de vida de desarrollo seguro, el comité de seguridad de la información de Grupo Oesía tiene la última palabra.
Las vulnerabilidades identificadas sirven para determinar los requisitos de seguridad que se deben incluir en el proyecto. Estos requisitos se tratan a lo largo del proyecto como cualquier otro requisito del proyecto, incluidas sus pruebas y validación.

6.3.2.1 Enfoque de desarrollo en cascada frente a enfoque de desarrollo ágil

Independientemente del paradigma de desarrollo seleccionado, el Grupo Oesía establece siempre una fase SRR (en el caso de proyectos desarrollados que siguen el paradigma en cascada) o una iteración KOM (que siempre es la primera iteración obligatoria en los proyectos que siguen el paradigma ágil) durante la que se realiza la evaluación de vulnerabilidades del proyecto.
Una vez finalizado el modelo de amenazas, el especialista en ciclo de vida de desarrollo establece los requisitos para los diferentes subsistemas del proyecto.
Estos requisitos se acuerdan con el responsable de cada subsistema durante la revisión de requisitos del sistema (SRR, por sus siglas en inglés) interna o la iteración KOM mencionadas anteriormente.
En el caso de SRR (enfoque en cascada), se establecen nuevos requisitos durante la fase SRR. En el caso de la metodología ágil durante la iteración KOM obligatoria, los historiales de usuario y las tareas se elaborarán tanto como sea posible para que estén listos para ser asignados posteriormente o durante la asignación de tareas sprint.

6.3.3 Riesgos del proyecto debido a requisitos de seguridad

Una vez que se han establecido las vulnerabilidades del proyecto, el especialista en ciclo de vida de desarrollo seguro realiza un estudio de riesgos como parte de la identificación de riesgos del proyecto descrita en el documento "**RGS-OP.PL.1.2 Plan de Tratamiento de Riesgos".**

6.4 Desarrollo seguro para software

6.4.1 Funciones involucradas

- CiSO
- Especialista en ciclo de vida de desarrollo seguro
- Ingeniero de software seguro del proyecto
- Ingeniero de proyecto DevSecOps

6.4.2 Requisitos de código

Todos los proyectos parten por defecto de una base de datos común de desarrollo de código seguro, tal como se especifica en el documento Requisitos comunes para el desarrollo de software seguro, en el que los requisitos de seguridad se describen como una obligación que debe cumplir el código fuente. En cada proyecto, estos requisitos se ajustan en función de su alcance. Ej.: si un proyecto no está basado en la web, se eliminarán todos los requisitos de seguridad que afecten a los formularios web.

Cada requisito aplicable tiene casos de prueba asociados para controlar que el proyecto cumple correctamente el requisito.

Se aplican dos enfoques diferentes cuando se prueba la seguridad del código:

Análisis estático. Análisis del código para identificar problemas o configuraciones incorrectas (entradas no validadas, verificación de límites de memoria insuficientes, reglas de cortafuegos configuradas incorrectamente, etc.).

Análisis dinámico. Pruebas del código en ejecución (escaneo de puertos de escucha inesperados en los sistemas, parámetros de entrada "fuzzing" para ver si los datos anómalos desencadenan un evento no deseado, etc.).

Además de las pruebas automáticas, se pueden establecer pruebas de seguridad manuales si el responsable de seguridad lo considera necesario (si las pruebas manuales se pueden replicar mediante herramientas de automatización, se preferirá este último método); el experto en seguridad del proyecto determina la cobertura y el alcance de las pruebas manuales. Las pruebas manuales se incluyen como requisitos de seguridad que debe cumplir el proyecto.

En las fases de diseño de cada proyecto con requisitos de seguridad, siempre participa un experto interno en seguridad y los diseños del proyecto debe aprobarlos oficialmente el experto en seguridad antes de continuar con el desarrollo, tanto si se trata de un proyecto desarrollado con el modelo en cascada como si se ha seguido el modelo iterativo.

Los requisitos de seguridad se establecen al comienzo del proyecto y, si para el desarrollo del proyecto se ha elegido el modelo iterativo, los requisitos de seguridad se verifican en cada iteración del proyecto. Según la clasificación de los requisitos, se deberá establecer un acuerdo con el cliente para el empleo de datos reales durante las fases de prueba del sistema. Para cada proyecto se deberá establecer en el documento de descripción del entorno la política acordada para el proyecto.

Cada implementación, como parte de la política de integración continua del Grupo Oesía, se somete a casos de prueba de seguridad aplicables a la iteración en curso, lo que garantiza la seguridad de cada implementación. Si la iteración muestra algún problema de seguridad (detectado durante el procedimiento de prueba de seguridad como parte del proceso de integración continua). Según la gravedad de la violación (que analiza el experto en seguridad del proyecto), se puede llegar a detener la implantación y a no implantar una nueva versión hasta que se resuelva el problema de seguridad.

6.4.3 Calidad y sencillez del código

Al comienzo del proyecto, se identifican y establecen los KPI de calidad del software para su verificación en cada iteración; de manera que así se asegura la calidad del código.

Cada diseño de arquitectura de software se documenta mediante diagramas UML simples antes de escribir el código. Cada bloque de código habrá delineado sus responsabilidades. Se garantizará la trazabilidad del diseño hasta el código al menos a nivel de función.

Por diseño, las credenciales secretas, como las contraseñas y las claves privadas, se aislarán lógicamente de la base del código principal, para evitar así que se registren en repositorios de códigos públicos. No se permiten credenciales de codificación fija en el código fuente.

Los principios SOLID (por sus siglas en inglés) son obligatorios durante las fases de diseño (si resultan aplicables):

- **S** - Single Responsibility (Responsabilidad única) Una clase por comportamiento
- **O** - Open-Closed (Abierto-cerrado) Las clases estarán abiertas para ampliación, pero cerradas para modificación
- **L** - Liskov Substitution (Sustitución de Liskov). Si S es un subtipo de T, entonces los objetos de tipo T en un programa pueden reemplazarse con objetos de tipo S sin alterar ninguna de las propiedades deseables de ese programa

- **I** – Interface Segregation (Segregación de la interfaz). No se debe obligar a los clientes a depender de métodos que no utilizan
- **D** — Dependency Inversion (Inversión de dependencias). Los módulos de alto nivel no deben depender de los módulos de bajo nivel. Ambos deben depender de la abstracción. Las abstracciones no deben depender de los detalles. Los detalles deben depender de las abstracciones.

La documentación se mantendrá actualizada, ya que el sistema evoluciona con cada iteración/modificación.

Las guías de estilo establecidas en Grupo Oesía se emplean como guía de codificación estándar para mantener la sencillez del código (véanse los documentos ICS06. Estándares de codificación C++ , NOR.DEV.TBT006. Codificación ADA, PCS003. Estándares de codificación Java, PCS025. Estándares de codificación C#). El código se escribirá de tal manera que sea autodocumentado.

La sencillez, la legibilidad y la sostenibilidad siempre se priorizan sobre el código confuso, sin importar cuántas líneas se necesitan para implantar la funcionalidad, lo que permite comprender fácilmente la funcionalidad de cada bloque de código.

Los comentarios sobre cada bloque de código/función son obligatorios y contienen una explicación de los parámetros requeridos, los resultados y una descripción general de la funcionalidad implantada por el bloque de código/función.

Las pruebas de código estático se ejecutan automáticamente en cada iteración para garantizar que se cumplan los requisitos establecidos para la calidad del software.

Dependencias externas

Los marcos y bibliotecas de codificación de terceros también son probados y aprobados por el experto en seguridad del proyecto antes de utilizarlos en el código desarrollado por cualquier empresa del Grupo Oesía.

Al comienzo de cada proyecto, se identificarán y enumerarán los marcos, bibliotecas y componentes de terceros para su análisis. Los desarrollos de terceros que ya se consideren de confianza porque se han utilizado en desarrollos anteriores del Grupo Oesía tendrán preferencia frente a proveedores terceros que no se hayan utilizado previamente en desarrollos del Grupo Oesía; para nuevos desarrollos/proveedores externos, el conjunto completo de pruebas se realizará en bibliotecas/componentes externos seleccionados para comprobar su idoneidad. Los informes de prueba se almacenarán y configurarán para usarlos posteriormente si es necesario.

A los desarrollos de terceros se les aplicarán los estándares de calidad y sencillez definidos para el proyecto (y así se indicará en sus respectivos SOW), donde se considera motivo de rechazo de los colaboradores externos el incumplimiento de los requisitos de calidad y sencillez establecidos en el

proyecto. En caso de que existan incumplimientos inevitables, estos serán documentados y se comunicarán al cliente para su aprobación.

6.4.4 Repositorio de código seguro

El código es tan seguro como los sistemas que se utilizan para crearlo, por lo que es esencial que el repositorio sea lo suficientemente seguro.

El acceso al repositorio de código está protegido con las credenciales proporcionadas por el Grupo Oesía para acceder a cualquier infraestructura de la empresa, por lo que se aplica la misma política de seguridad para las credenciales (seguridad de la contraseña, cambio de contraseña, registro de actividad, etc.). Cualquier actividad que se realice en el repositorio de código fuente se registra (usuario, fecha y recursos a los que se ha accedido) y se documenta obligatoriamente.

Los proyectos pueden seleccionar entre subversión o git (o ambos, según la naturaleza del documento que se debe configurar) como herramienta de configuración.

Los repositorios para los proyectos reservados, en función de su clasificación, se almacenan en salas aisladas cuyo acceso físico está permitido únicamente a quienes trabajan en el proyecto y tienen necesidad de conocer (véanse los documentos MS-03. Manual de políticas de seguridad y PES-09.02. Gestión del acceso de usuarios).

Las máquinas que no están en la misma red con el mismo nivel de clasificación asignado al proyecto no tienen acceso al repositorio de código. Las máquinas externas no asignadas al proyecto no pueden acceder a repositorios distintos a los asignados al proyecto, aunque tengan el mismo nivel de clasificación.

Se realiza una copia de seguridad de forma automática de los repositorios de código de acuerdo con la política del Grupo Oesía (véase el documento **PRO-MP.INFO.6.1 Copias de Respaldo y Recuperación de Información**).

6.4.5 Proteger la canalización de compilación e implementación

La integración, entrega e implementación continuas son los estándares del Grupo Oesía para la compilación, prueba e implementación de sistemas.

Solo el proyecto DevOps (y aquellos en quienes DevOps delega) está autorizado para acceder a los scripts de integración continua del proyecto. El acceso a los servidores y licencias de integración continua se otorga a través de las credenciales corporativas de acuerdo con la política corporativa de renovación y seguridad de credenciales.

La canalización para el proceso de integración continua cumple el estándar establecido para el procedimiento de desarrollo del Grupo Oesía (véase el documento INS.DEV.TBT305.v01. Configuración del proceso de integración continua para proyectos):

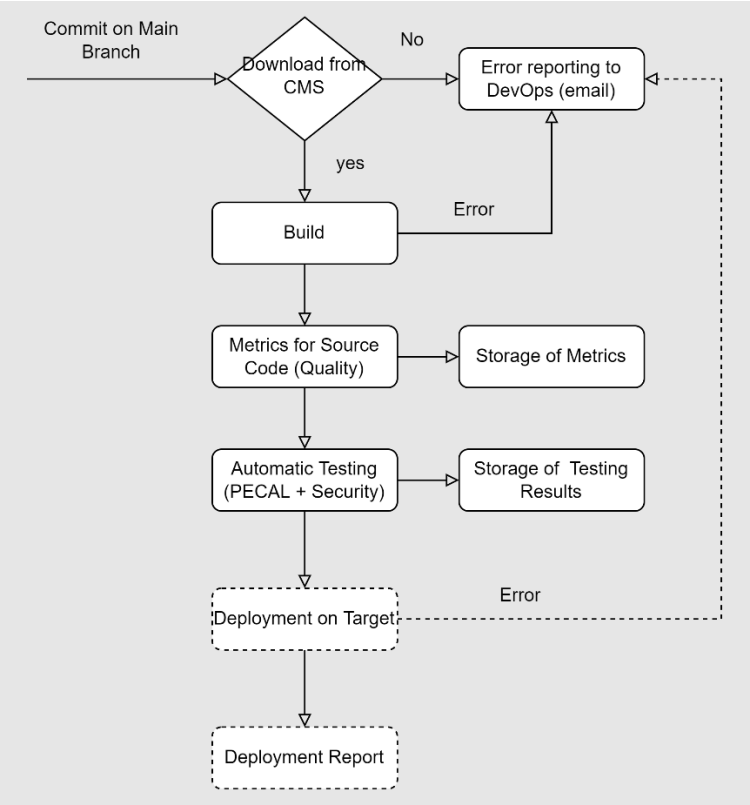

Imagen 1: ciclo de integración continua

Cada commit inicia automáticamente la creación de código, las pruebas de sistema (incluidas las pruebas de casos para los requisitos de seguridad) y las métricas de calidad y se asegura siempre que cada lanzamiento cumpla con los requisitos de seguridad y calidad establecidos para el proyecto.

Cualquier brecha detectada durante las pruebas automáticas se documenta y puede llegar a detener el despliegue de la versión en función de la gravedad de la brecha detectada, según los criterios establecidos para el proyecto y según los criterios del experto en seguridad del proyecto.

La herramienta de código abierto (Jenkins) se emplea para la integración continua de manera que se asegura la capacidad de inspeccionar el código de la herramienta. El acceso a Jenkins está regulado mediante el uso de credenciales corporativas; solo pueden acceder a la máquina Jenkins quienes tienen necesidad de conocer y acceso a la canalización de integración continua.

Por defecto, como parte del proceso de implementación, cada software se firma digitalmente con una firma digital en el ejecutable, programa o archivo de software que se está implementando. El certificado digital garantiza que el software no se ha manipulado y se puede utilizar de forma segura. Solo el responsable técnico del proyecto podrá autorizar la firma del código.

El CSO de la empresa mantiene un inventario con las claves de firma de código, donde indica las firmas que se han generado y dónde se ha instalado/implementado el software.

6.5 Redes y sistemas operativos seguros

6.5.1 Funciones involucradas

- CISO
- Especialista en ciclo de vida de desarrollo seguro
- Ingeniero de proyecto DevSecOps
- Ingeniero de software seguro del proyecto

6.5.2 Requisitos de seguridad

El responsable de seguridad supervisará los requisitos establecidos como criterio común para los sistemas operativos involucrados en el desarrollo e implementaciones del proyecto desarrollado por Grupo Oesía.

El repositorio de requisitos comunes para los sistemas operativos se describe en el documento Requisitos comunes para la securización del sistema operativo.

Como mínimo, se deberán identificar, documentar y validar los siguientes aspectos para los sistemas operativos incluidos en el proyecto

- supervisa que solo estén abiertos los puertos necesarios para las comunicaciones.
- El firmware se actualizará a su última versión. Si por algún motivo se debe congelar la versión del firmware, se deberá elaborar al menos un documento de decisión en el que se indique el motivo por el que no se ha actualizado el firmware a su última versión.
- Desactivación de usuarios predeterminados (y sus contraseñas asociadas)
- No se permitirán configuraciones de depuración en desarrollos implementados para el cliente final.
- Configuración de cortafuegos, equipos IDS, segmentación de redes, etc.

  Métodos de autenticación empleados: políticas de contraseñas establecidas específicamente para el proyecto (fortaleza de las contraseñas, reutilización de contraseñas, periodicidad de cambio de contraseñas, etc.). Las técnicas específicas para garantizar la autenticación desde la perspectiva del código se recogen en el apartado 6.4.2 Requisitos de código. Por defecto, todas las contraseñas estarán cifradas.

  Se elaborará para el proyecto un "mapa de autorización" en el que se indicará el acceso previsto para las funciones establecidas para cada funcionalidad del sistema. Por defecto, a los usuarios (entendidos como personas físicas y/o cualquier otro sistema/aplicación que acceda a las capacidades del sistema) se les asignará el acceso mínimo necesario para llevar a cabo sus responsabilidades. Los permisos se otorgarán por defecto a las funciones, nunca directamente a los usuarios finales.

Como parte de la política general de requisitos de seguridad, toda actividad de acceso, tanto para OS como para la interoperabilidad del sistema (véase 6.4.26.4.2 Requisitos de código), se registra en un registro circular, donde se indica el ID de usuario, la fecha, el resultado de la conexión y el nivel de acceso otorgado, etc. La extensión del registro de actividad vendrá determinada por los requisitos del sistema.

6.6 Desarrollo seguro para hardware

6.6.1 Funciones involucradas

- CISO
- Especialista en ciclo de vida de desarrollo seguro
- Ingeniero de *hardware* seguro del proyecto

6.6.2 Requisitos de seguridad

En el diseño y desarrollo de nuestros productos prestamos especial atención a garantizar que la tecnología empleada en ellos no sea accesible ni pueda ser explotada por partes interesadas no deseadas. El objetivo final de las medidas adoptadas es evitar cualquier acción destinada a degradar la eficacia, acortar la vida útil esperada del sistema o alterar el comportamiento del sistema durante la vida útil esperada del sistema, incluido la retirada del sistema.

Por ello, se han establecido requisitos comunes como criterio común para todos los sistemas desarrollados por el Grupo Oesía. Estos requisitos establecen las actividades de ingeniería de sistemas destinadas a prevenir o retrasar la explotación de tecnologías esenciales o críticas.

Debido a la naturaleza de las técnicas empleadas, en este plan no se puede mencionar ninguna de ellas. Los requisitos seguros para el desarrollo de hardware se enumeran de forma separada en una especificación de requisitos reservada. Ejemplos genéricos que muestran los tipos de opciones disponibles en los requisitos reservados son:

- Recubrimientos opacos delgados no grabables aplicados a obleas semiconductoras.
- Componentes autodestructivos.
- Criptografía para incluir cifrado y descifrado a nivel PL.

Cada proyecto parte de una base de datos común de requisitos de hardware seguro para el desarrollo, tal como se especifica en el documento Requisitos comunes para la securización del sistema operativo, en el que los requisitos de seguridad se describen como una obligación que debe cumplir el hardware desarrollado. En cada proyecto, estos requisitos se ajustan en función de su alcance.

Se pueden establecer pruebas de seguridad adicionales si el responsable de seguridad lo considera necesario para el proyecto; el experto en seguridad del proyecto establece la cobertura y el alcance de estas pruebas.

El experto en seguridad participa siempre en las fases de diseño de cada proyecto con requisitos de seguridad y los diseños del proyecto debe aprobarlos oficialmente el experto en seguridad antes de continuar con el desarrollo, tanto si el proyecto sigue un modelo en cascada como un modelo iterativo.

Los requisitos de seguridad se establecen al comienzo del proyecto y, si para el desarrollo del proyecto se ha elegido el modelo iterativo, los requisitos de seguridad se verifican en cada iteración del proyecto.

6.7 Herramientas y entornos de desarrollo seguros

6.7.1 Funciones involucradas

- CISO
- Ingeniero jefe
- Especialista en ciclo de vida de desarrollo seguro
- Gestor del proyecto

6.7.2 Entornos y herramientas de desarrollo

Los entornos de desarrollo se describen y diseñan durante las primeras fases del proyecto (durante la fase SRR en el caso de proyectos en cascada o se incluyen en las primeras iteraciones en el caso del desarrollo iterativo). Por regla general, se implementan tres entornos diferentes.

- Entorno de desarrollo. Este entorno incluye todas las herramientas de diseño y desarrollo necesarias para el desarrollo del sistema.
- Entorno de preproducción. Este entorno incluye solo artefactos desplegables (SW y HW) y herramientas de prueba. En este entorno no se permiten herramientas de diseño ni de desarrollo. En este entorno se superan todas las pruebas establecidas durante las fases de diseño y desarrollo (incluidas las pruebas de resistencia) que garantizan el correcto funcionamiento del sistema.
- Entorno de producción. En este entorno solo se permiten artefactos de producción probados previamente en el entorno de preproducción, junto con herramientas de supervisión.

Los lenguajes, los marcos (IDE, compiladores) y las pilas de tecnología utilizadas en el entorno de desarrollo los ha aprobado previamente el CISO del Grupo Oesía. Siempre que es posible, se utilizan componentes de seguridad establecidos y bien probados en el entorno de desarrollo en lugar de utilizar otros no aprobados que podrían incorporar nuevas brechas. En caso de que el proyecto

requiera una herramienta/tecnología que no figura en la base de datos de herramientas aprobadas, se inicia el procedimiento dirigido por el ingeniero jefe para analizar y evaluar la aprobación de la herramienta/tecnología solicitada. En este procedimiento se determina si la nueva herramienta/tecnología se incorpora como herramienta/tecnología corporativa o si se restringe únicamente al proyecto en el que se requiere.

Las herramientas, funciones y API utilizadas en el proyecto se actualizan periódicamente de acuerdo con las recomendaciones de CISO y se mejoran de acuerdo con las nuevas actualizaciones y versiones, se resuelven problemas comunes de versiones anteriores, se mantiene actualizado de este modo el entorno de desarrollo y se implementan los últimos controles defensivos.

El seguimiento de protección del entorno de desarrollo se realiza mensualmente en cada entorno de desarrollo seguro para prevenir cualquier fallo/anomalía en el entorno de desarrollo; los fallos detectados se registran y solucionan con la máxima prioridad en las 72 horas siguientes a su detección. En el sistema se registra la trazabilidad del estado y la solución aportada para cada fallo detectado.

El acceso a los entornos de desarrollo siempre está protegido y se accede a través de las credenciales de la empresa, de este modo se garantiza el control sobre cualquier actividad que se realice en el entorno de desarrollo. La política de la empresa establece las funciones y la accesibilidad de las funciones para cada proyecto.

Se realizan controles de auditoría aleatorios sobre los entornos de desarrollo para controlar la seguridad del entorno.

6.8 Almacenamiento y manipulación seguros de datos

6.8.1 Funciones involucradas

- CISO
- Especialista en ciclo de vida de desarrollo seguro
- Gestor del proyecto

6.8.2 Almacenamiento y manipulación de datos

Esta parte **ORG-01-01-Política de Seguridad de la Información,** se ocupa de los siguientes riesgos (véanse también el documento **PRO-MP.INFO.6.1 Copias de Respaldo y Recuperación de Información)**

- acceso no autorizado a los datos, permiso de divulgación de datos, pérdida de información sensible, manipulación de datos o eliminación de datos.

- Empleo de datos maliciosos.
- Pérdida de datos críticos, lo que lleva a la denegación de servicio o pérdida de datos críticos.

Al inicio del proyecto, se identifican los conjuntos de datos y archivos necesarios para el sistema, se clasifican de acuerdo con la criticidad de su contenido y se establecen diferentes niveles de criticidad.

Para cada nivel de criticidad se definirán los requisitos de seguridad del sistema para asegurar la integridad, confidencialidad y disponibilidad requeridas. Estas medidas estarán alineadas y serán coherentes con los permisos otorgados a las diferentes funciones identificadas para el sistema (véase el apartado 6.2. Definición de funciones. Solo las funciones asignadas podrán operar con conjuntos de datos y archivos de acuerdo con los permisos establecidos para cada función.

Los requisitos para la validación de contenido y extensión se definen en el

Garantizar que los datos quedan protegidos por mecanismos de autorización entre entornos mediante la segregación física o lógica y mediante copias de respaldo que aseguren su disponibilidad

7 Registros y Archivo

Se consideran registros de seguridad los siguientes:

Nombre del Registro	Código Formato	Código Registro	Responsable Registro	Tipo de Archivo	Período Mínimo
N/A	N/A	N/A	N/A	N/A	N/A

OESÍA Networks, S.L.

Calle Marie Curie, 19

28251 – Madrid,

Teléfono: 91 309 86 00, Fax: 91 375 82 16

http://www.oesia.com