[logo de la organización]

[nombre de la organización]

POLÍTICA DE DESARROLLO SEGURO

Código:	
Versión:	
Fecha de la versión:	
Creado por:	
Aprobado por:	
Nivel de confidencialidad:	

Commented [AES1]: Se deben completar todos los campos de este documento que estén marcados con corchetes [ ].

Commented [AES2]: Para obtener más información sobre este tema, lea este artículo:

How to integrate ISO 27001 A.14 controls into the system/software development life cycle (SDLC)
https://advisera.com/27001academy/blog/2017/01/24/how-to-integrate-iso-27001-a-14-controls-into-the-system-software-development-life-cycle-sdlc/

Commented [AES3]: El sistema de codificación del documento debe coincidir con el sistema actual de codificación de documentos de la organización. En el caso que no exista ese sistema, se puede eliminar esta línea.

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
	0.1	Advisera	Descripción básica del documento

Tabla de contenido

1. Objetivo, alcance y usuarios

El objetivo de este documento es definir las reglas básicas para desarrollo seguro de software y sistemas.

Este documento se aplica al desarrollo y mantenimiento de todos los servicios, arquitectura, software y sistemas que forman parte del Sistema de Gestión de Seguridad de la Información (SGSI).

Los usuarios de este documento son todos los empleados que trabajan en el desarrollo y mantenimiento de [nombre de la organización].

Commented [AES4]: Incluya el nombre de su organización.

2. Documentos de referencia

- Norma ISO/IEC 27001, cláusulas A.5.33, A.8.11, A.8.25, A.8.26, A.8.27, A.8.28, A.8.29, A.8.30, A.8.31, A.8.32 y A.8.33
- Metodología de evaluación y tratamiento de riesgos
- Política de seguridad para proveedores
- [Política de gestión de cambios] / [Procedimientos de seguridad para el departamento de TI]
- Plan de formación y concienciación

Commented [AES5]: Puede encontrar una plantilla para este documento en la carpeta del Paquete Premium de documentos sobre ISO 27001 e ISO 22301 "06_Evaluacion_y_tratamiento_de_riesgos".

Commented [AES6]: Escoja cuál de estos dos documentos utilizará.

Commented [AES7]: Puede encontrar una plantilla para este documento en la carpeta del Paquete Premium de documentos sobre ISO 27001 e ISO 22301 "11_Formacion_y_concienciacion".

3. Desarrollo seguro y mantenimiento

Commented [AES8]: Como la tecnología que se utiliza es muy

3.1. Evaluación de riesgos para el proceso de desarrollo

Además de la evaluación de riesgos realizada según la Metodología de evaluación y tratamiento de riesgos, el [cargo] debe realizar periódicamente la evaluación de lo siguiente:

Commented [AES9]: Si es necesario, especifique la frecuencia.

- Los riesgos relacionados con el acceso no autorizado al entorno de desarrollo.
- Los riesgos relacionados con los cambios no autorizados sobre el entorno de desarrollo.
- [illegible]

Commented [AES10]: Estas son solo recomendaciones; puede

3.2. Asegurar el entorno de desarrollo

Commented [AES11]: Borrar esta sección si el control A.8.31 se

[Identificar requerimientos internos y externos, describir aquí cómo se restringirá el acceso al entorno de desarrollo únicamente para empleados autorizados, cómo se separará de los entornos de prueba y producción, cómo se realizarán las copias de seguridad.

3.3. Principios para la ingeniería de sistemas seguros

Commented [AES12]: Borrar esta sección si el control A.8.27 se

El [cargo] emitirá procedimientos para la ingeniería de sistemas de información seguros, tanto para el desarrollo de nuevos sistemas como para el mantenimiento de los sistemas existentes; también establecerá los estándares mínimos de seguridad que se deben cumplir.

[redacted]

3.4. Codificación segura

El [cargo] emitirá procedimientos para la codificación segura del sistema de información, tanto para el desarrollo de nuevos sistemas como para el mantenimiento de los sistemas existentes, así como establecer las prácticas mínimas de codificación segura que deberán cumplirse.

[redacted]

3.5. Requerimientos de seguridad

Al adquirir nuevos sistemas de información o al desarrollar o cambiar los vigentes, el [cargo] debe documentar los requerimientos de seguridad en la Especificación de requisitos del sistema de información.

3.6. Requerimientos de seguridad relacionados con redes públicas

El [cargo] es el responsable de definir los controles de seguridad relacionados con la información en los servicios de aplicaciones que se transmiten sobre redes públicas:

- La descripción de los sistemas de autenticación que se usarán.
- [redacted]

El [cargo] es el responsable de la definición de controles para las transacciones en línea, los cuales deben incluir los siguientes:

- Cómo se evitará el direccionamiento erróneo.
- Cómo se evitará la transmisión de datos incompletos.
- [redacted]

3.7. Verificación y prueba de la implementación de requerimientos de seguridad

El [cargo] es el responsable de definir la metodología, responsabilidades y los plazos para verificar si se cumplieron todos los requerimientos de la Especificación de requisitos del sistema de información y si el sistema está listo para producción.

Commented [AES13]: Por ejemplo, lineamientos sobre técnicas de programación (independiente para cada lenguaje de programación), técnicas de autenticación de usuarios, control de sesión segura, validación de datos, etc.

[redacted]

Commented [AES14]: Eliminar este párrafo si el control A.8.30 [redacted]

Commented [AES15]: Eliminar esta sección si el control A.8.28 [redacted]

Commented [AES16]: P.ej. orientación sobre técnicas de [redacted]

Commented [AES17]: Eliminar este párrafo si el control A.8.30 [redacted]

Commented [AES18]: Borrar esta sección si el control A.5.8 se [redacted]

Commented [AES19]: Para saber más sobre este tema, lee este artículo:

[redacted]

Commented [AES20]: O usted también puede definir que este [redacted]

Commented [AES21]: Borrar esta sección si el control A.8.26 se [redacted]

Commented [AES22]: Estas son solo recomendaciones; puede [redacted]

Commented [AES23]: Entre los controles se puede incluir [redacted]

Commented [AES24]: Estas son solo recomendaciones; puede [redacted]

Commented [AES25]: Eliminar esta sección si el control A.8.29 [redacted]

Commented [AES26]: Por ej., ingresos y resultados esperados, [redacted]

Commented [AES27]: Una buena práctica es que realicen las [redacted]

Commented [AES28]: No solo la prueba final una vez finalizado [redacted]

3.8. Repositorio

[Aquí describa dónde se guardan los códigos y todos los demás archivos relacionados con el desarrollo y cómo se protegen del acceso o modificaciones no autorizados]

3.9. Control de versión

[Definir aquí cuál es el sistema de control de versión (números, fechas, etc.) y cómo se aplica en su entorno de desarrollo]

3.10. Control de cambios

Los cambios en el desarrollo y durante el mantenimiento de los sistemas deben ser realizados de acuerdo con [illegible]

3.11. Protección de datos de prueba

Los datos confidenciales, como también los datos que pueden estar relacionados a personas, no deben ser utilizados como datos de prueba. [illegible]

3.12. Formación necesaria en seguridad

El [cargo] define el nivel de habilidades y conocimientos en seguridad para el proceso de desarrollo y le propone al [cargo] cuál es la formación. [illegible]

4. Gestión de registros guardados en base a este documento

[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[Lista de riesgos relacionados al proceso de desarrollo]	Ordenador del [cargo]	[cargo]	Solamente el [cargo] puede acceder a esos archivos.	3 años para los listados que ya no están vigentes.
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

Commented [AES29]: Eliminar esta sección si el control A.8.32 [illegible]

Commented [AES30]: Para obtener más información sobre este tema, lea este artículo: [illegible]

Commented [AES31]: Escoja cuál de estos dos documentos [illegible]

Commented [AES32]: Borrar esta sección si el control A.8.33 se [illegible]

Commented [AES33]: Modifique estos registros para que [illegible]

Commented [AES34]: Modifique estos registros para que [illegible]

5. Validez y gestión de documentos

Este documento es válido hasta el [fecha].

El propietario de este documento es el [cargo], que debe verificar, y si es necesario actualizar, el documento por lo menos una vez al año.

Commented [AES35]: Esto es sólo una recomendación; ajustar

Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:

- Cantidad de incidentes que surgen por fallas en los controles de seguridad creados en los sistemas

6. Apéndices

- Apéndice 1 – Especificación de requisitos del sistema de información

[cargo]
[nombre]

[firma]

Commented [AES36]: Sólo es necesario si el Procedimiento para el control de documentos y registros establece que los documentos en papel deben ser firmados.