[logo de la organización]

[nombre de la organización]

Comment [DK1]: Se deben completar todos los campos de este documento que estén marcados con corchetes [ ].

POLÍTICA DE DESARROLLO SEGURO

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

Comment [DK2]: 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.

©2013 Plantilla para clientes de EPPS services Ltd. www.iso27001standard.com, según Contrato de licencia.

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
10/01/2013	0.1	Dejan Kosutic	Descripción básica del documento

Tabla de contenido

1. OBJETIVO, ALCANCE Y USUARIOS 3

2. DOCUMENTOS DE REFERENCIA 3

3. DESARROLLO Y MANTENIMIENTO SEGURO 3

3.1. EVALUACIÓN DE RIESGOS PARA EL PROCESO DE DESARROLLO 3
3.2. ASEGURAR EL AMBIENTE DE DESARROLLO 3
3.3. PRINCIPIOS DE INGENIERÍA SEGURA 3
3.4. REQUERIMIENTOS DE SEGURIDAD 4
3.5. VERIFICACIÓN Y PRUEBA DE LA IMPLEMENTACIÓN DE REQUERIMIENTOS DE SEGURIDAD 4
3.6. REPOSITORIO 4
3.7. CONTROL DE VERSIÓN 4
3.8. CONTROL DE CAMBIOS 4
3.9. PROTECCIÓN DE DATOS DE PRUEBA 4
3.10. CAPACITACIÓN NECESARIA EN SEGURIDAD 5

4. GESTIÓN DE REGISTROS GUARDADOS EN BASE A ESTE DOCUMENTO 5

5. VALIDEZ Y GESTIÓN DE DOCUMENTOS 5

6. APÉNDICES 6

©2013 Plantilla para clientes de EPPS services Ltd. www.iso27001standard.com, según Contrato de licencia.

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 (ISMS).

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

2. Documentos de referencia

- Norma ISO/IEC 27001, capítulos A.14.1.2, A.14.1.3, A.14.2.1, A.14.2.2, A.14.2.5, A.14.2.6, A.14.2.7, A.14.2.8, A.14.2.9, A.14.3.1
- Metodología de evaluación y tratamiento de riesgos
- Política de seguridad para proveedores
- [Política de gestión de cambios]/[Procedimientos operativos para tecnología de la información y de la comunicación]
- Plan de capacitación y concienciación

Comment [DK3]: Escoja cuál de estos dos documentos utilizará.

3. Desarrollo y mantenimiento seguro

Comment [DK4]: Como la tecnología que se utiliza es muy diferente de una organización a otra, usted necesitará adaptar esta sección de acuerdo a sus circunstancias específicas.

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:

Comment [DK5]: Si es necesario, especifique la frecuencia.

- Los riesgos relacionados con el acceso no autorizado al ambiente de desarrollo.
- Los riesgos relacionados con los cambios no autorizados sobre el ambiente de desarrollo.
- Las vulnerabilidades técnicas de los sistemas de TI utilizados en la organización.
- Los riesgos que puede traer una nueva tecnología si se utiliza en la organización.

3.2. Asegurar el ambiente de desarrollo

Comment [DK6]: Borrar esta sección si el control A.14.2.6 se determinó como no aplicable

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

3.3. Principios de ingeniería segura

Comment [DK7]: Borrar esta sección si el control A.14.2.5 se determinó como no aplicable

El [cargo] emitirá procedimientos para ingeniería segura de sistemas de información, 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.

Comment [DK8]: Por ejemplo, lineamientos sobre técnicas de programación (independiente para cada lenguaje de programación), técnicas de autenticación de usuarios, control de versión seguro, validación de datos, etc.

Abarca todos los niveles de arquitectura: negocio, datos, aplicaciones y tecnología.

©2013 Plantilla para clientes de EPPS services Ltd. www.iso27001standard.com, según Contrato de licencia.

Los mismos principios de ingeniería se aplicarán a los desarrollos externalizados y se incluirán en los contratos, como se determina en la [Política de seguridad para proveedores].

3.4. 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 [Especificación de requerimientos de seguridad] (ver Apéndice).

3.5. 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.
- La descripción de cómo se garantizarán la confidencialidad e integridad de la información.
- La descripción de cómo se garantizarán las acciones de inviolabilidad.

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.
- Cómo se evitará la modificación no autorizada de mensajes.
- Cómo se evitará la duplicación no autorizada de mensajes.
- Cómo se evitará la divulgación no autorizada de datos.

3.6. 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 requerimientos de seguridad y si el sistema está listo para producción.

3.7. 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]

3.8. Control de versión

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

3.9. Control de cambios

Los cambios en el desarrollo y durante el mantenimiento de los sistemas deben ser realizados de acuerdo con [Política de gestión de cambios]/[Procedimientos operativos para tecnología de la información y de la comunicación].

3.10. Protección de datos de prueba

Comment [DK9]: Borrar esta sección si el control A.14.2.7 se determinó como no aplicable

Comment [DK10]: Borrar esta sección si el control A.14.1.1 se determinó como no aplicable

Comment [DK11]: O usted también puede definir qué roles en un trabajo para un equipo de proyecto o similar.

Comment [DK12]: Borrar esta sección si los controles A.14.1.2 y A.14.1.3 se determinaron como no aplicables

Comment [DK13]: Entre los controles se puede incluir firmas digitales, encriptado, sistemas de identificación y autenticación, etc. La aplicación de los controles debe realizarse en conformidad con las leyes y normas.

Comment [DK14]: Borrar esta sección si los controles A.14.2.8 y A.14.29 se determinaron como no aplicables

Comment [DK15]: Por ej., ingresos y resultados esperados, herramientas de análisis de código o escáner de vulnerabilidades.

Esto debe realizarse en un ambiente de pruebas realista.

Comment [DK16]: Una buena práctica es que realicen las pruebas el equipo de desarrollo y un equipo independiente.

Comment [DK17]: No solo la prueba final sino en finalizado el desarrollo sino también durante todo el proceso de desarrollo.

Comment [DK18]: Borrar esta sección si los controles A.14.2.2 y A.14.2.4 se determinaron como no aplicables

Comment [DK19]: Escoja cuál de estos dos documentos utilizará.

Comment [DK20]: Borrar esta sección si el control A.14.3.1 se determinó como no aplicable

©2013 Plantilla para clientes de EPPS services Ltd. www.iso27001standard.com, según Contrato de licencia.

Los datos confidenciales, como también los datos que pueden estar relacionados a personas, no deben ser utilizados como datos de prueba. Las excepciones pueden ser autorizadas solamente por el [cargo], en cuyo caso, el [cargo] debe definir cómo se protegerán esos datos de prueba.

3.11. Capacitación necesaria en seguridad

El [cargo] define el nivel de habilidades y conocimientos en seguridad para el proceso de desarrollo y determina cuál es la capacitación propuesta para el [cargo]. El [cargo] incluye la capacitación correspondiente en el Plan de capacitación y concienciación.

4. Gestión de registros guardados en base a este documento

Nombre del registro	Ubicación de archivo	Persona responsable del archivo	Controles para la protección del registro	Tiempo de retención
[Lista de riesgos relacionados al proceso de desarrollo]	Ordenador de [cargo]	[cargo]	[solo el cargo puede acceder a esos archivos]	3 años para listados que ya no están vigentes
[Procedimientos para ingeniería segura de sistemas de información]	[Intranet de la organización]	[cargo]	[Solamente el cargo puede publicar y editar esos archivos]	3 años para procedimientos que ya no están vigentes
[Planes de prueba]	[Intranet de la organización]	[cargo]	[Solamente el cargo puede publicar y editar esos archivos]	3 años para las pruebas que se han realizado

Comment [DK21]: Adapte el período de esta columna en función de sus necesidades reales.

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.

Comment [DK22]: Esto es sólo una recomendación, ajustar la frecuencia según sea necesario.

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

©2013 Plantilla para clientes de EPPS services Ltd. www.iso27001standard.com, según Contrato de licencia.

6. Apéndices

- Especificación de requerimientos de seguridad

[cargo]
[nombre]

_____

[firma]

Comment [DK23]: Sólo es necesario si el Procedimiento para control de documentos y registros establece que los documentos en papel deben ser firmados.

©2013 Plantilla para clientes de EPPS services Ltd. www.iso27001standard.com, según Contrato de licencia.