Comment [DK1]: Para aprender a completar este documento consulte:

Tutorial en vídeo 'Cómo redactar el Procedimiento para acciones correctivas y preventivas según ISO 27001/ISO 22301' http://www.iso27001standard.com/video-tutorials

[logo de la organización]

Comment [DK2]: Se deben completar todos los campos de este documento que estén marcados con corchetes [ ].

[nombre de la organización]

PROCEDIMIENTO PARA MEDIDAS CORRECTIVAS

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

Comment [DK3]: 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. CORRECCIONES Y MEDIDAS CORRECTIVAS 3

3.1. NO CONFORMIDADES Y CORRECCIONES 3

3.2. MEDIDAS CORRECTIVAS 3

3.3. IMPLEMENTACIÓN DE MEDIDAS CORRECTIVAS 4

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

5. VALIDEZ Y GESTIÓN DE DOCUMENTOS 5

6. APÉNDICES 5

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

1. Objetivo, alcance y usuarios

El objetivo de este procedimiento es describir todas las actividades relacionadas con la iniciación, implementación y mantenimiento de registros de correcciones, como también de medidas correctivas.

Este procedimiento se aplica a todas las actividades implementadas dentro del Sistema de Gestión de Seguridad de la Información (SGSI) Sistema de Gestión de Continuidad del Negocio (SGCN)].

Los usuarios de este documento son todos los empleados de [nombre de la organización].

Comment [DK4]: Se debe insertar esta leyenda en lugar de SGSI en caso que el procedimiento se refiera exclusivamente a la gestión de continuidad del negocio.

2. Documentos de referencia

- Norma ISO/IEC 27001, punto 10,1
- Norma ISO 22301, punto 10.1
- Norma BS 25999-2, punto 6.1
- Política de Seguridad de la Información
- Política de la Continuidad del Negocio
- Procedimiento para auditoría interna
- Procedimiento para gestión de incidentes

Comment [DK5]: Borrar si el procedimiento se refiere sólo a gestión de continuidad del negocio

Comment [DK6]: Borrar esto si usted no implementa continuidad del negocio

Comment [DK7]: Borrar si el procedimiento se refiere sólo a gestión de continuidad del negocio

Comment [DK8]: Borrar esto si usted no implementa continuidad del negocio

Comment [DK9]: Si la documentación es escrita sólo para continuidad del negocio, reemplazar con Plan de respuesta a los incidentes

3. Correcciones y medidas correctivas

3.1. No conformidades y correcciones

Una no-conformidad es todo incumplimiento de los requerimientos de las normas, documentación interna, reglamentos, obligaciones contractuales y de otra clase dentro del SGSI. Las no conformidades pueden ser identificadas durante una auditoría interna o externa, en base a resultados de la revisión por parte de la dirección, luego de incidentes, durante el transcurso normal de las operaciones de negocios o en cualquier otra situación.

Comment [DK10]: o SGCN

Un empleado que detecta una no conformidad debe tomar acciones inmediatamente para controlarla, contenerla y corregirla y para contener sus consecuencias. Si un empleado no es responsable de esa no conformidad debe transmitir la información sobre ella a una persona responsable que pueda corregirla.

3.2. Medidas correctivas

La persona responsable debe evaluar la necesidad de eliminar el origen de la no conformidad y evitar su recurrencia tomando medidas correctivas. La principal diferencia es que las medidas correctivas eliminan la causa de una no-conformidad, mientras que la corrección se enfoca solamente en controlar la no-conformidad y en atender las consecuencias directas.

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

Una medida correctiva puede ser iniciada por cualquier empleado o, cuando sea pertinente, por cualquier cliente, proveedor o socio de la organización. Una medida correctiva puede demandar cambios sobre cualquier documento, proceso o acuerdo dentro del marco del SGSI.

Comment [DK11]: o SGCN

3.3. Implementación de medidas correctivas

Una medida correctiva se implementa de la siguiente forma:

Paso	*Persona responsable de la implementación*
1. Revisión de la no conformidad	Cualquiera con una función dentro del SGSI
2. Determinación de la causa de la no-conformidad	Persona responsable del área donde se ha identificado la no-conformidad
3. Identificar o la no-conformidad ya existía	Persona responsable del área donde se ha identificado la no-conformidad
4. Evaluación de la necesidad de tomar acciones para eliminar la no-conformidad	Persona responsable del área donde se ha identificado la no-conformidad
5. Determinación de las acciones necesarias para eliminar las causas de la no-conformidad y para asegurar que no se produzca nuevamente	Persona responsable del área donde se ha identificado la no-conformidad
6. Implementación de las acciones planificadas	Persona a cargo de la implementación, designada por la persona responsable
7. Revisión para determinar si la acción tomada logró eliminar las causas de la no-conformidad	[cargo]
8. Informar a todas las personas involucradas que se ha implementado la medida correctiva	Persona a cargo de la implementación, designada por la persona responsable
9. Realizar cambios al SGSI si fuera necesario.	La persona que está a cargo de coordinar el SGSI.

Comment [DK12]: o SGCN

Comment [DK13]: Se puede designar a una persona para todas las medidas correctivas (por ejemplo, el Gerente de Seguridad) o la persona responsable puede estar autorizada a designar a una persona cada vez que se inicia una nueva medida correctiva.

La implementación de acciones para regularizar las no-conformidades identificadas durante una auditoría interna generalmente es controlada por el auditor interno.

Comment [DK14]: o SGCN

Comment [DK15]: Por ej., el Jefe de seguridad o el coordinador de continuidad del negocio

Cada uno de los pasos anteriores debe quedar registrado en el formulario de medidas correctivas.

Comment [DK16]: o SGCN

Comment [DK17]: También puede utilizar, por ejemplo, una aplicación de Mesa de ayuda o cualquier otro sistema que use ticket o casos para solucionar determinados problemas.

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

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

Formulario para medidas correctivas	[nombre de la carpeta de archivo, en qué gabinete][nombre de carpeta en Intranet]	[cargo]	Una vez que se han registrado todos los datos, se debe bloquear cualquier agregado o edición.	3 años

Comment [DK18]: Si se guardan los registros en papel

Comment [DK19]: Si se guardan los registros en formato electrónico

Comment [DK20]: Si utilizar una aplicación, especifique el nombre de dicha aplicación.

5. Validez y gestión de documentos

Este documento es válido desde el [fecha]

El propietario de este documento es el [cargo], que [redacted] documento por lo menos una vez al año.

Comment [DK21]: 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 [redacted]
- Cantidad de [redacted]
- cantidad de medidas correctivas tomadas sin haber sido registradas en un formulario designado

6. Apéndices

Comment [DK22]: Borrar esta sección si usted utiliza una aplicación

Apéndice: Formulario para medidas correctivas

[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.