Master Interuniversitario en Seguridad de las TIC (MISTIC)

Trabajo de Final de Máster

Gestión de No Conformidades. Acciones Correctivas y de Mejora

Procedimiento de Gestión de No Conformidades. Acciones Correctivas y de Mejora		
CONTROL DE VERSIONES		
Versión inicial	**Fecha**	
V.1.0	**19/03/2019**	
V.1.1	**20/04/2019**	
Documento elaborado por		
Responsable de actualización		
Versiones Posteriores	**Cambio realizado**	**Fecha**
v.1.0	**Elaboración del documento**	**19/03/2019**
v.1.0	**Definiciones (Apartado 3)**	**20/04/2019**
Estado	**Aprobado por :**	
Etiquetado del documento	**Uso Interno**	

LISTA DE DISTRIBUCIÓN

Este documento ha sido distribuido a los siguientes responsables:

Nombre	Responsabilidad

COPYRIGHT

Tabla de contenido

1. Objeto y campo de aplicación

El presente procedimiento tiene por objeto describir los procedimientos de comunicación relacionados el SGSI. Dichos procedimientos abarcan las comunicaciones de ámbito interno y externo.

El presente documento recoge el procedimiento que describe las acciones a realizar para la gestión de las no conformidades detectadas en el SGSI. En concreto abarca:

- La detección e identificación.
- La evaluación y tratamiento .
- El seguimiento y cierre.

Asimismo, se establece la sistemática para la apertura de acciones correctivas y de mejora necesarias para la eliminación de las causas reales y/o potenciales, respectivamente, que provocan las situaciones de No Conformidad del SGSI.

Este procedimiento aplica a todos los procesos de negocio, documentación del sistema de gestión, activos, y a todos aquellos elementos relacionados con el Sistema de Gestión implantado y que su estado sea “no conforme” con respecto a los requisitos especificados por la organización y/o por las normas de referencias establecidas.

2. Responsabilidades

El Responsable del SGSI, analiza las desviaciones (No Conformidades) registradas en el Informe de No Conformidades, y colabora con la persona que detectó la no conformidad y con los Responsables de Departamento en el establecimiento de las acciones correctivas/de mejora necesarias para la eliminación de las causas que han originado tales desviaciones, siempre que proceda. Igualmente, supervisa la resolución de las situaciones registradas.

La Dirección, en colaboración con el resto de Responsables de Área/ Departamento, analiza las acciones tomadas en la revisión del Sistema de Gestión, pudiendo identificar áreas potenciales de mejora a partir de esta fuente de información.

3. Definiciones

Hallazgos de la auditoría: Resultados de la evaluación de la evidencia de auditoría recopilada frente a los criterios de auditoría. Los hallazgos indican la conformidad o no conformidad, así como las oportunidades de mejora o registrar buenas prácticas.

Tipo de hallazgos de Auditoría:

- **No Conformidad**: Es un incumplimiento de un requisito del sistema, sea este especificado o no. Se conoce como requisito una necesidad o expectativa establecida, generalmente explícita u obligatoria.
    - Tipos de No conformidades:
        - **No Conformidad Mayor**:
            - Incumplimiento de un requisito normativo, propio de la organización,legal y/o seguridad, que vulnera o pone en serio riesgo la integridad del sistema de gestión. Puede corresponder a la no aplicación de una cláusula de una norma (requerida por la organización), el desarrollo de un proceso sin control, ausencia consistente de registros declarados por la organización o exigidos por la norma, o la repetición permanente y prolongada a través del tiempo de pequeños incumplimientos asociados a un mismo proceso o actividad.
        - **No conformidad Menor**:
            - *Desviación mínima en relación con requisitos normativos, propios de la organización y/o legales, estos incumplimientos, son esporádicos, dispersos y parciales y no afecta mayormente la eficiencia e integridad del sistema de gestión.*

- ***Observaciones:*** *Es la manera de* dejar constancia ,en un informe de auditoría, de las oportunidades de mejora, de los riesgos para la calidad que pueden convertirse en no conformidades futuras, o de cualquier otro detalle que haya observado y le parece relevante registrar.

- ***Acciones correctivas****: acciones para eliminar la causa de una no conformidad y para prevenir la recurrencia.*

- ***Oportunidad de mejora****: Detección de una posible actividad, tarea o acción que permite, dentro del proceso de mejora continua, aportar y o contribuir a un incremento de la seguridad.*

4. Desarrollo

4.1. No conformidades

Las no conformidades pueden ser detectadas por cualquier persona que intervenga en el Sistema de Gestión implantado, por el Responsable del SGSI y/o el Comité de Dirección y/o por el equipo auditor.

4.1.1. Gestión de no conformidades

a. Detección e identificación

Cualquier persona que intervenga en el sistema de gestión implantado (empleado y/o contratado) que detecte una no conformidad, deberá proceder a su identificación tan rápido como sea posible, para ello deberá notificar inmediatamente al Responsable del SGSI sobre dicha no conformidad, haciendo uso de cualquier medio: e-mail, teléfono, personalmente, etc., dejando éste en todo caso constancia del hecho mediante e-mail.

El Responsable del SGSI documenta el "Informe de no conformidad" en (**TFM_REG_NC y Acciones Correctivas**), indicando al menos, su fecha de apertura, codificación, tipo de no conformidad (en función del origen), procesos afectados, controles implicados, una descripción y causa raíz de la no conformidad (investigación para identificar el fallo raíz que ha ocasionado).

b. Tratamiento

Tras la detección de una no conformidad y el análisis de su causa se pueden aplicar dos formas de tratamiento que dependerán de la complejidad y/o impacto del problema:

- La primera forma consiste en una solución inmediata a un problema puntual y no repetitivo detectado:
    - El responsable del tratamiento pone en marcha un tratamiento de "choque" mediante la aplicación de una acción positiva inmediata. Dicha acción corregirá el fallo mostrado por la NC, pero no solucionará la causa raíz que dio origen a la misma.

- La segunda forma de tratamiento consiste en adoptar acciones necesarias para eliminar el problema y la posibilidad de que vuelva a ocurrir, estas acciones son denominadas "acciones correctivas".
    - En estos casos se deberá dejar reflejado en el Informe de no conformidad, el número de acción correctiva asociada (para facilitar su seguimiento en el registro de Acciones (**TFM_REG_Acciones**), indicando en su origen NC.

c. Seguimiento y cierre

Tras el tratamiento y llegado el plazo máximo de ejecución establecido anteriormente, el Responsable del SGSI verificará que éste haya sido aplicado con eficacia y en el tiempo estipulado, para ello recogerá todas las evidencias posibles como pruebas de cumplimiento.

Además cumplimentará el apartado correspondiente "seguimiento y cierre" del "informe de no conformidad", indicando el momento de cierre y la eficacia de la misma. Cuando la acción correctiva implantada de cómo resultado no eficaz, se procederá a su cierre e inmediatamente se abrirá una nueva acción correctiva. En la acción correctiva ineficaz se indicará el número de la nueva acción asociada (para facilitar su seguimiento).

4.2. Acciones de mejora

Cuando, a criterio de la Dirección, de un Responsable de Departamento o del Responsable del SGSI, se considere la mejora del SGSI, éstas será gestionadas de igual forma que las acciones correctivas, y registradas en (***FTM_REG_Acciones).***

Las **acciones de Mejora** se originan, en términos generales, como consecuencia de:

- Propuesta de mejora de algún/os aspecto/s del SGSI; puede ser realizada por cualquier persona de la organización debiéndose documentar y remitir al Responsable del SGSI.
- Detección por parte de alguna persona de la organización de un potencial problema o no conformidad que pueda traducirse en un futuro en desviaciones del Sistema de Gestión.
- Como consecuencia de los resultados de las auditorías del sistema, ya sean internas o externas.
- Como consecuencia del resultado de los análisis realizados para la medición de la eficacia y eficiencia del Sistema de Gestión.
- Como consecuencia del estudio o análisis de los procesos (se debe indicar en la acción el proceso o procesos asociados).
- Como resultado de las evaluaciones de riesgo.
- Como mejora para mejorar el cumplimiento de los objetivos del SGSI (se debe indicar el proceso o procesos relacionados para la mejora del objetivo u objetivos).

5. Registros y Archivo

Se consideran registros del SGSI los siguientes:

Nombre del Registro	Responsable registro	Tipo de archivo	Periodo mínimo
TFM_REG_Acciones	Responsable del SGSI	Electrónico	3 años
TFM_NC y Acciones Correctivas	Responsable del SGSI	Electrónico	3 años

6. Referencias

TM_PROC_Procedimiento de Auditorías Internas