Master Interuniversitario en Seguridad de las TIC (MISTIC)

Trabajo de Final de Máster

Procedimiento de Procesos, Roles y Responsabilidades

Procesos, Roles y Responsabilidades		
CONTROL DE VERSIONES		
Versión inicial		**Fecha**
V.1.0		**19/03/2019**
Documento elaborado por		
Responsable de actualización		
Versiones Posteriores	**Cambio realizado**	**Fecha**
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 objeto del presente procedimiento es identificar los procesos del SGSI que soportan los objetivos de seguridad, así como establecer los roles y responsabilidades en todos niveles de la organización.

Este procedimiento es de aplicación a todos los procesos relacionados con el SGSI y a todos los roles que participan en dichos procesos.

2. Responsabilidades

Es responsabilidad de la Dirección para demostrar liderazgo y compromiso respecto al SGSI:

- Garantizar que las políticas y objetivos se establecen y son compatibles con la dirección estratégica de la organización,
- Garantizar la integración de los requisitos del sistema de gestión en los procesos de negocio de la organización,
- Garantizar que los recursos necesarios para el sistema de gestión están disponibles,
- Comunicar la importancia de una gestión eficaz y que se ajuste a los requisitos aplicables.
- Garantizar que el Sistema de gestión logra los resultados deseados,
- Dirección y soporte a las personas para contribuir a la eficacia,
- El fomento de la mejora continua, y
- El apoyo a otras funciones de gestión pertinentes para demostrar su liderazgo y compromiso.

La dirección proporcionar evidencia de su compromiso con el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora mediante:

- El establecimiento de una política de continuidad de negocio y de seguridad de la información.
- Asegurando que se establecen los objetivos y planes de para el Sistema de gestión.
- El establecimiento de funciones, responsabilidades y competencias para la gestión de la continuidad del negocio y seguridad de la información.
- La designación de una o más personas responsables del SGSI, con la autoridad y competencias, que sean responsables de la implementación y mantenimiento (ver Anexo de Roles y responsabilidades).

La Alta Dirección asegura de que las responsabilidades y autoridades para las funciones relevantes se asignan y son comunicadas dentro de la organización.

2.1. Comité de Seguridad

Es responsabilidad del Comité:

- Abordar la Seguridad de la Información desde una perspectiva integrada y conjunta, respecto a toda la Organización.
- Evaluar y aprobar:
    - Una política general de Seguridad de la Información.
    - El análisis de riesgos, así como sus conclusiones y el estado del riesgo asumible por la Dirección.
    - El plan de acción para el tratamiento de los riesgos detectados.
    - Los objetivos de Seguridad de la Información, asegurándose de su cumplimiento.
    - Analizar las incidencias, evaluando sus consecuencias y aprobando medidas correctoras a las mismas.
    - Analizar los resultados de las auditorías internas e independientes.
    - Desarrollar un proceso de mejora continua.

La administración efectiva de la Seguridad de la Información no es sólo un asunto de tecnología, sino un requerimiento de negocio y por ello, se hace imprescindible dotar a la Organización, al igual que en otras disciplinas estratégicas (Financiera, Jurídica, Calidad y Procesos, etc.), de los recursos necesarios para garantizar los objetivos establecidos de acuerdo a los objetivos y las estrategias.

Estos recursos, comienzan por la designación del responsable del Sistema de Gestión de Seguridad de la Información (SGSI).

2.2. Responsable del SGSI

El responsable del SGSI tiene atribuidas las siguientes funciones:

- Disponer de los siguientes recursos y conocimientos:
    - Debe comprender la necesidad de la seguridad de las operaciones en la empresa, y su importancia para la organización.
    - Implementar y verificar la Políticas de Seguridad, y los procedimientos para alcanzar los objetivos del negocio.
- Elaborar planes de propuestas de políticas y procedimientos.
- Realizar, junto a los responsables de las actividades, el análisis de riesgos en el negocio.
- Confeccionar planes de propuestas de mejoras del sistema de gestión.
- Creación de métricas y objetivos de seguridad.
- Comunicación de los resultados del SGSI a la alta dirección.
- Redacción de informes de incidencias.
- Encargarse de las relaciones con partes externas sobre asuntos relacionados con el SGSI.

- Participar en las revisiones del SGSI por la Dirección.
- Realizar la evaluación de seguimiento de los proveedores.
- Actuar como guía del auditor en las auditorías internas y externas.
- Gestionar los procesos de no conformidades, acciones correctivas y de mejora, reclamaciones de los clientes, asegurando el correcto tratamiento, análisis y seguimiento de estos.
- Y demás funciones relacionadas con la implantación y mantenimiento del SGSI.

3. Desarrollo

3.1. Composición del Comité

El **Comité** estará integrado por los siguientes miembros:

- CEO.
- Director de Operaciones.
- Responsable del SGSI
- Responsable de TI

De manera adicional, y según se requiera y acuerde por los miembros permanentes indicados anteriormente, podrán participar otros miembros de carácter temporal, de acuerdo con los temas tratados por el Comité.

De manera posterior a las reuniones, se generarán las actas pertinentes, en las que se recogerá evidencia al menos de los asuntos tratados y los acuerdos alcanzados.

3.2. Reuniones periódicas del Comité

Las reuniones del Comité de Dirección se realizarán **Semestralmente**, aunque se pueden convocar reuniones extraordinarias cuando se considere necesario, bien sea como respuesta a incidentes o cambios organizativos, bien como respuesta a otros aspectos que puedan afectar a la continuidad de las operaciones de la Organización, y sean de carácter urgente.

De manera posterior a las reuniones, se generarán las actas pertinentes, en las cuales se recogerá evidencia al menos de los asuntos tratados y los acuerdos alcanzados.

3.3. Revisión del Sistema de Gestión por la Dirección

La Dirección debe revisar el Sistema completo con una periodicidad mínima anual, aunque puede realizarse mediante una o más reuniones u otras actividades de revisión que considere adecuadas en los distintos Comités de Dirección.

La revisión por la dirección debe incluir la consideración de:

- El estado de las acciones de las revisiones previas por la Dirección.
- Los cambios en los asuntos externos e internos que son relevantes para el sistema de gestión de la continuidad del negocio.
- La información sobre el funcionamiento, incluyendo las tendencias en :
    - las no conformidades y acciones correctivas.
    - resultados sobre la medición y mediciones.
    - resultados de las auditorías.
    - cumplimiento de objetivos.
- Comentarios de las partes interesadas.
- Resultados de la apreciación de riesgos y estado del plan de tratamiento de riesgos.
- Oportunidades de mejora continua.

Los resultados de la revisión por la dirección deben incluir las decisiones relacionadas con las oportunidades de mejora continua y la posible necesidad de cambios en el SGSI. Dichas acciones deberán vincularse con los objetivos del SGSI.

3.4. Procesos y roles del SGSI

La organización ha establecido roles, responsabilidades y ha asignado autoridad para implementar y mantener el SGSI. Dichos roles están repartidos por toda la organización.

Los procesos de alto nivel y los roles con autoridad sobre los mismos se pueden ver en la siguiente tabla.

Proceso	Responsable (R)	Requerido/Informado	Propietario de la gestión (reporta a)
P01. Entendimiento de organización y su contexto. Alcance	Responsable SGSI	Directores de Área Responsables de Servicio	Comité de Seguridad
P02. Evaluación Riesgos Seguridad de la Información	Responsable SGSI	Directores de Área Responsables de Servicio	Comité de Seguridad
P03. Planificación	Responsable SGSI	Directores de Área Responsables de Servicio	Comité de Seguridad
P04. Requisitos Legales, Regulatorios y Contractuales	Responsable Asesoría Jurídica	Responsable SGSI	Comité de Seguridad

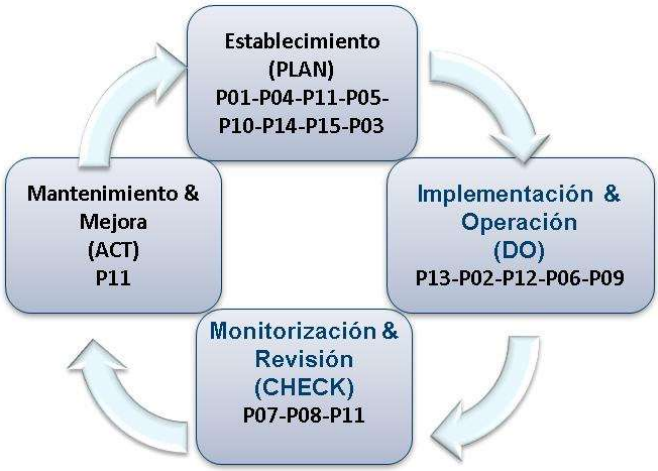
Proceso	Responsable (R)	Requerido/Informado	Propietario de la gestión (reporta a)
P05. Comunicación	Responsable SGSI	Directores de Área Responsables de Servicio	Comité de Seguridad
P06. Incidentes	Responsable SGSI	Directores de Área Responsables de Servicio	Comité de Seguridad
P07. Evaluación y Monitorización/Medición	Responsable SGSI	Directores de Área Responsables de Servicio	Comité de Seguridad
P08. Auditoría Interna	Responsable SGSI	Directores de Área Responsables de Servicio	Comité de Seguridad
P09. Plan de Continuidad	Responsable SGSI	Directores de Área Responsables de Servicio	Comité de Seguridad
P10. Información Documentada	Responsable SGSI	Directores de Área Responsables de Servicio	Comité de Seguridad
P11. Compromiso y liderazgo	Dirección Ejecutiva	Directores de Área Responsables de Servicio Responsable SGSI	Comité de Seguridad
P12.Seguridad en las TIC	Responsable TI	Directores de Área Responsables de Servicio Responsable SGSI	Comité de Seguridad
P13.Gestión de proveedores	Responsable proveedores	Directores de Área Responsables de Servicio Responsable SGSI	Comité de Seguridad
P14. Gestión del personal, roles y responsabilidades	CEO	Directores de Área Responsables de Servicio Responsable SGSI	Comité de Seguridad
P15. Tratamiento de la información	Directores de Área Responsables de Servicio	Dirección Ejecutiva	Comité de Seguridad

Asimismo, el conjunto de responsabilidades asignadas a cada rol se puede ver en la tabla siguiente

La comunicación de dichos roles se realiza, según el caso, de las siguientes formas:

- Comité de Dirección, a los miembros, directores y responsables.
- Personal: Organigrama, curso, política y normativa, intranet etc.

La siguiente imagen muestra el mapa de procesos del SGSI y sus interacciones:



Proceso	Tareas y Responsabilidades	Responsabilidad de (Rol):	Competencias
P09 P05	Revisar y aprobar estrategias de continuidad	Alta Dirección	n/a
P11 P05	Revisión y aprobar la política de seguridad de la información		n/a
P11 P05	Revisar y aprobar Manual de Políticas del SGSI		n/a
P08	Realización plan de auditoría	Auditor independiente	
P08 P05	Realización auditoría interna e informe		
P11 P05	Hacer Revisión por la Dirección	Comité de Dirección	n/a
P11 P05	Establecer acciones de mejora	Comité de Dirección	n/a

Proceso	Tareas y Responsabilidades	Responsabilidad de (Rol):	Competencias
P01	Revisar e incluir nuevos aspectos a regular (legislación y contractual)	Responsable Comercial	Curso de Concienciación seguridad de la información Conocimiento de los procedimientos aplicables
P04	Revisar e incluir nuevos aspectos a regular (legislación y contractual)	Responsable de Auditoria y Procesos	Curso de Concienciación seguridad de la información Conocimiento de los procedimientos aplicables
P11	Revisión Manual de Políticas del SGSI		
P02	Actualización del Análisis de Riesgos		
P06 P05	Tratar incidentes		
P04	Dar soporte al responsable del SGSI sobre el cumplimiento		
P07 P05	Suministrar datos de Indicadores		
P11	Revisión Manual de Políticas del SGSI	Responsable de medios /instalaciones **Responsable SGSI**	Curso de Concienciación seguridad de la información Conocimiento de los procedimientos aplicables
P02	Actualización del Análisis de Riesgos		
P12	Registrar y mantener los accesos físicos del personal		
P06 P05	Tratar incidentes		
P09	Realizar y planes de continuidad de negocio		
P01	Revisión cambios en el alcance. Revisión de contexto.	Responsable de Negocio/ Responsables Áreas	Curso de Concienciación seguridad de la información Conocimiento de los procedimientos aplicables
P04	Revisar e incluir nuevos aspectos a regular (legislación y contractual)		
P15	Clasificar la información		
P14	Informar sobre necesidades de formación.		

Proceso	Tareas y Responsabilidades	Responsabilidad de (Rol):	Competencias
P05			
P15	Informar y autorizar cuando se produce una entrada/salida de soporte que contenga información		
P12	Solicitar alta usuario y permisos		
P06 P05	Tratar incidentes		
P09	Revisar BIAs		
P09	Realizar pruebas del PCN y Contingencias		
P09	Revisar y aprobar estrategias de continuidad		
P09	Realizar planes de continuidad de negocio		
P07 P05	Suministrar datos de Indicadores	**Responsable SGSI**	
P11	Revisión de la política de seguridad de la información		
P02	Actualización del Análisis de Riesgos (incluyendo terceras partes)		
P07 P05	Suministrar datos de Indicadores		
P11	Revisión Manual de Políticas del SGSI	Responsable: **CTO**	Curso de Concienciación seguridad de la información Conocimiento de los procedimientos aplicables
P02	Actualización del Análisis de Riesgos		
P14	Mantener actualizados los puestos y los perfiles exigidos		
P14	Actualización de información y fichas del personal		
P14	Actualización de listados del personal		

Proceso	Tareas y Responsabilidades	Responsabilidad de (Rol):	Competencias
P14	Actualización de curriculums		
P14	Mantener actualizadas Información de activos entregados		
P14	Mantener actualizado un manual de bienvenida, y entregarlo a cada personal nuevo, incluyendo política de seguridad y normativa	Responsable: **CTO**	
P14	Garantizar que se piden y se archivan todos los requisitos de selección de personal		
P06 P05	Tratar incidentes		
P09	Realizar planes de continuidad de negocio		
P07 P05	Suministrar datos de Indicadores		
P14	Asegurar que se realizan las acciones formativas y de concienciación.		
P14	Realizar plan de formación periódico y realizar seguimiento.		
P11	Revisión Manual de Políticas del SGSI	Responsable de TI /**CTO**	Curso de Concienciación seguridad de la información Conocimiento de los procedimientos aplicables
P02	Actualización del Análisis de Riesgos (incluyendo terceras partes)		
P12	Mantenimiento y Actualización del Inventario TIC	**Responsable SGSI**	
P14 P05	Informar sobre necesidades de formación.		
P12	Mantener actualizados accesos asignados por usuario		
P12	Mantener actualizado el registro de mantenimiento de equipos y dispositivos cuando		

Proceso	Tareas y Responsabilidades	Responsabilidad de (Rol):	Competencias
	se produce alguna intervención de mantenimiento		
P12	Realizar procedimiento de borrado seguro, cuando se elimina o se reutiliza un soporte que contiene datos		
P15	Registrar cuando se produce una entrada/salida de soporte que contenga información		
P12	Registrar cambios y aprobaciones		
P12	Registrar cambios acordados y enviados a proveedores		
P12	Revisar eventos y garantizar que se registran en los sistemas		
P12	Realizar y comprobar realización de copias de seguridad		
P12	Documentar y mantener requisitos de seguridad de las aplicaciones		
P12	Registrar y mantener los accesos del personal		
P12	Análisis de vulnerabilidades a máquinas		
P12	Solucionar vulnerabilidades detectadas		
P06	Registrar incidentes		
P06 P05	Tratar incidentes		
P09	Revisar BIAs (análisis de impacto)		
P09	Realizar pruebas del PCN (plan de continuidad de negocio) y Contingencias		
P09 P05	Revisar y aprobar estrategias de continuidad		

Proceso	Tareas y Responsabilidades	Responsabilidad de (Rol):	Competencias
P09	Realizar planes de continuidad de negocio		
P12	Llevar control software y licencias		
P07 P05	Suministrar datos de Indicadores		
P12	Revisión y Actualización de Instrucciones técnicas		
P10	Revisión de manual de Gestión SGSI	**Responsable del SGSI**	Curso de ISO/IEC 27001 Al menos 5 años de experiencia en relación con la seguridad Al menos 5 años de experiencia en relación con las TIC Conocimiento de procedimientos aplicables Curso de Concienciación seguridad de la información
P03	Revisión y planificación de objetivos de seguridad		
P03	Planificación de la evaluación de riesgos		
P11	Revisión de política de seguridad de la información		
P11	Revisión Manual de Políticas del SGSI		
P01	Revisión cambios en el alcance y actualización del manual. Revisión de contexto.		
P06	Actualización del Análisis de Riesgos		
P10	Inclusión de nuevos términos en terminología		
P04	Revisar e incluir nuevos aspectos a regular (legislación y contractual)		
P15	Revisión de marcado y tratamiento de la información con la que se trabaja		
P14 P05	Mantener actualizados los roles y las competencias		
P14 P05	Informar sobre necesidades de formación.		
P14	Hacer seguimiento al plan de formación		

Proceso	Tareas y Responsabilidades	Responsabilidad de (Rol):	Competencias
P06	Registrar incidentes		
P10	Mantener actualizada información documentada		
P07	Registrar NO CONFORMIDADES		
P07	Establecer acciones correctivas		
P07	Mantener plan auditoría anual		
P07 P05	Obtener informe sobre indicadores		
P06 P05	Tratar incidentes	**Equipo SOC**	Equipo de gestión de incidentes
P06 P05	Comunicar incidentes	**Todo el personal**	Conocimiento de procedimientos aplicables Curso de Concienciación seguridad de la información
P15	Marcar la información		
P15	Tratar la información según la normativa		
P13	Evaluación de Proveedores de Servicio	Responsable Proveedores	Curso de Concienciación seguridad de la información Conocimiento de los procedimientos aplicables
P13 P05	Mantener actualizado empresas y contratos con terceras partes.		
P13 P05	Gestionar los cambios en los servicios con proveedores		

4. Registros y Archivo

Nombre del registro	Responsable del registro	Tipo de archivo	Periodo mínimo
Acta de Comité de Dirección de Seguridad	Responsable del	Electrónico	3 años

	SGSI		
TFM_REG_Acciones	Responsable del SGSI	Electrónico	3 años