Sistema de Gestión para la Seguridad de la Información

GARANTÍA Y SEGURIDAD DE LA INFORMACIÓN – CURSO 22-23

Introducción

El objetivo de este trabajo es *elaborar la primera versión de* un Sistema para la Gestión de la Seguridad de la Información (SGSI) para una empresa ficticia. El resultado será un documento en el que lo central será la elaboración del análisis de riesgos y el catálogo de las medidas de seguridad que se deberían implantar, así como los controles para comprobar si se van a tomar o no.

Esta empresa quiere asegurar la disponibilidad, integridad y confidencialidad de la información que maneja. La familia de normativas ISO-27000, en la que se aborda la seguridad de la información, propone los SGSI como una herramienta sencilla de utilizar por cualquier empresa independientemente de su tamaño, puesto que permite establecer normas, procedimientos y controles para disminuir los riesgos en el campo de la información.

La realización de este trabajo supone la realización de las siguientes tareas:

a) se analizará el contexto de la empresa para determinar la situación actual de su sistema de información, incorporando decisiones que el grupo considere oportunas para completar la descripción del contexto aportada en el documento que se aporta para el proyecto.

b) se elaborará un *catálogo de activos*

c) se analizarán las posibles *amenazas* que puedan perjudicar a esos activos.

d) tras esto se hará un *análisis de riesgos* que permitirá establecer

e) una serie de controles y medidas de seguridad con el objetivo de intentar afianzar la seguridad de los elementos del sistema de información.

Para facilitar la realización de este trabajo, se proporcionan cuatro documentos, que se encuentran en la carpeta "*Materiales de trabajo*" del Campus Virtual:

1. El "*Informe de seguridad del sistema*", que describe el contexto de la empresa que se va a analizar y que se deberá completar, y añadir el "*Análisis de Riesgos y Medidas de Seguridad*" que realice el grupo.
2. Una guía para la implantación de un SGSI en la empresa.
3. Una guía de gestión de riesgos.
4. El libro de MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

Fases

Para la realización del proyecto, los alumnos tienen que formar grupos de 3 o 4 personas.

Las fases principales de elaboración del SGSI son las siguientes:

1. **Análisis de la organización**: Comprensión del modelo de negocio, su contexto, su estructura organizativa y las funciones realizadas por su personal y de la información que maneja.
2. **Elaboración del catálogo de activos**: Listado con todos los elementos relevantes de la organización y que se tendrán en cuenta en el SGSI, así como la valoración de los mismos en función de la importancia que tienen para el funcionamiento de la empresa.
3. **Elaboración del listado de amenazas**: Análisis de las amenazas a las que están expuestos los activos anteriores.
4. **Evaluación y gestión de riesgos**: Estudiar los riesgos a los que están expuestos los activos en función de las amenazas que pueden sufrir, su probabilidad y el daño que pueden ocasionar.
5. **Propuesta de salvaguardas y controles**: Listado con una serie de salvaguardas que permitan disminuir el riesgo que corren los activos

Según se vayan cubriendo las fases anteriores, habrá que ir elaborando el "*Informe de seguridad*"

definitivo y que habrá que entregar en el Campus Virtual: Partiendo de un modelo de informe "inicial" (que se proporciona), hay que completarlo en el análisis de contexto, realizar el análisis de riesgos del sistema objetivo y un plan de salvaguardas razonado para el mismo.

Además, cada grupo tiene que elaborar una breve presentación sobre su trabajo de no más de 20 transparencias, cada una de 20 segundos (400 segundos en total) en la que la parte central será el análisis de riesgos y el plan de salvaguardas propuestas.

Hitos

ENTREGA	Hito	Descripción
28-nov-2022	Presentación del trabajo a realizar	Se presenta el trabajo a realizar y las fases
18-dic-2022	Informe con el SGSI	Se entregará el informe completo: descripción completa revisada del sistema objetivo, el análisis de riesgos, descripción de las medidas de seguridad.
01-dic-2022 **12-dic-2022**	Seguimiento del trabajo	El profesor revisa con cada grupo el estado de avance, sobre trabajo realizado hasta ese momento.
19-dic-2022 **22-dic-2022**	Defensa oral del informe presentado	Cada grupo realizará una presentación oral del informe de hasta 10 minutos de duración a toda la clase.

Objetivos

Con la realización de este trabajo se pretende que los estudiantes alcancen los siguientes objetivos:

- Asimilar de forma activa los conceptos fundamentales sobre los que se asienta el análisis de riesgos de seguridad.
- Ser capaz de realizar un análisis de riesgos de un sistema informático de complejidad media-baja.
- Ser capaz de interpretar los resultados del análisis de riesgos y aplicarlo a la mejora de la seguridad de los sistemas.
- Ser capaz de colaborar en un grupo reducido para definir y seguir una metodología de trabajo adecuada a los objetivos que se persiguen.
- Elaborar una documentación correcta del trabajo realizado.
- Ser capaz de comunicar adecuadamente a público técnico el trabajo desarrollado.

Evaluación

La evaluación del trabajo seguirá los criterios que se indican a continuación. Para cada uno se refleja, en puntos sobre el total, su peso relativo en términos de la calificación global.

2pt El seguimiento de la actividad del grupo realizada por el profesor, para valorar tanto la metodología como el ritmo de trabajo y el cumplimiento de las diversas metas del trabajo. Esta parte de la calificación podrá ser diferente para cada miembro del grupo.

10pt El análisis de riesgos se corresponde con la descripción del proyecto y aporta un catálogo adecuado de controles y medidas, estando justificadas todas las decisiones.

8pt El informe está escrito de forma precisa, correcta y clara, se ajusta a las instrucciones de la plantilla y es completo.

Bibliografía

Asociación Española de Normalización y Certificación (2014). Normativa ISO/IEC 27000
http://www.iso27000.es/iso27000.html
[Consulta: 29-11-2021].

INTECO -actualmente INCIBE- (2009): Implantación de un SGSI en la empresa. Guia_apoyo_SGSI_v0_1_RevisionINTECO. Guías de INTECO, 25 de noviembre. Disponible en: https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf
[Consulta: 29-11-2021].

International Organization for Standarization (2018). ISO31000:2018 – Sistemas de Gestión de Riesgos y Seguridad
https://www.iso.org/iso-31000-risk-management.html
[Consulta: 29-11-2021].

Ministerio de Hacienda y Administraciones Públicas (2012). MAGERIT. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Versión 3.0. Libro I.
https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html
[Consulta: 29-11-2021].