Módulo Teórico-Práctico

Actividad en contexto

Módulo
Teoría de Seguridad de la Información
Nombre de la entrega
La política de seguridad del papel a la acción
Nivel académico
Especialización
Tipo de entrega
Análisis de un caso práctico

Nota

Tenga en cuenta que el tutor le indicará qué herramienta requiere y qué estrategia deberá desarrollar para evidenciar su participación individual en un trabajo colaborativo.

DESCRIPCIÓN **DE LA ACTIVIDAD**

En esta actividad se presenta un caso práctico para que el estudiante analice la situación y proponga un plan de sensibilización para el conocimiento y aplicación de la política de seguridad en el entorno planteado.

CASO O PROBLEMA

Datalatina es una firma latinoamericana dedicada al aseguramiento, gestión de riesgos, calidad y seguridad de sistemas de información.

El personal de consultores y docentes de esta firma cuenta con las principales certificaciones internacionales asociadas al alcance de sus tareas, las cuales han sido emitidas por prestigiosas organizaciones académicas, como ISACA, PMI, DRI, entre otras. Esto, sumado a la vasta experiencia generada a través de más de 30 años de compromiso con el cliente, hace de Datalatina una empresa líder en las soluciones que ofrece.

Las tres líneas de negocio de Datalatina son: soluciones, *software* y capacitación.

Línea de soluciones: provee consultoría y capacitación sobre buen gobierno corporativo, con referentes como COSO y gobierno de TI con COBIT; gestión integral de riesgo y auditoría; gestión de riesgos de lavado de activos y financiamiento terrorista; gestión de seguridad de la información; gestión de continuidad del negocio, tomando como referencia la norma ISO 22301; hacking ético; cumplimiento y legislación; y soluciones personalizadas.

Línea de *software*: Datalatina utiliza el software Meycor; ha desarrollado aplicaciones para el gobierno de TI con Cobit, seguridad de la información ISO 27001 y gestión de riesgo corporativo alineado con la Norma ISO 3100.

Línea de capacitación: es un centro autorizado por ISACA para la capacitación y certificación en ISA, CISM, CGEIT, CRISC, CISSP y DRI.

Datalatina es certifcada ISO/IEC 27001, lo cual asegura la calidad en términos de seguridad según dicho estándar y cuenta con importantes clientes a nivel mundial, además, trabaja a través de representantes en diferentes países.

» Política de seguridad de la información de Datalatina

La dirección de la firma reconoce la importancia de identificar y proteger sus activos de información evitando la destrucción, la divulgación, modificación y utilización no autorizada de toda información relacionada con clientes, empleados, precios, bases de conocimiento, manuales, casos de estudio, códigos fuente, estrategia, gestión, y otros conceptos; además, comprometiéndose a desarrollar, implantar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información (SGSI).

La seguridad de la información se caracteriza por la preservación de:

A. Su confidencialidad, asegurando que solo quienes estén autorizados pueden acceder a la información.

B. Su integridad, asegurando que la información y sus métodos de proceso son exactos y completos.

C. Su disponibilidad, asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran.

La seguridad de la información se consigue implantando un conjunto adecuado de controles, tales como políticas, prácticas, procedimientos, estructuras organizativas y funciones de software. Estos controles han sido establecidos para garantizar que se cumplen los objetivos específicos de seguridad de la empresa.

» Es política de Datalatina que:

1. Se establezcan anualmente objetivos en relación con la seguridad de la información.
2. Se desarrolle un proceso de análisis del riesgo y, de acuerdo con su resultado, se implementen las acciones correspondientes con el fin de tratar los riesgos que se consideren inaceptables, según los criterios establecidos en el Manual de Gestión.

3. Se establezcan los objetivos de control y los controles correspondientes, en virtud de las necesidades que en materia de riesgos surjan del proceso de análisis de riesgos manejado.
4. Se cumpla con los requisitos del negocio, legales o reglamentarios, y las obligaciones contractuales de seguridad.
5. Se brinde concientización y entrenamiento en materia de seguridad de la información a todo el personal.
6. Se establezcan los medios necesarios para garantizar la continuidad del negocio de la empresa.
7. Se sancione cualquier violación a esta política y a cualquier política o procedimiento del SGSI.
8. Todo empleado es responsable de registrar y reportar las violaciones a la seguridad, confirmadas o sospechadas.
9. Todo empleado es responsable de preservar la confidencialidad, integridad y disponibilidad de los activos de información en cumplimiento de la presente política y de las políticas y procedimientos inherentes al sistema de gestión de la seguridad de la información.
10. El jefe de seguridad de la información es responsable directo del mantenimiento de esta política a través de brindar consejo y guía para su implementación, así como también de investigar toda violación reportada por el personal.

PLANTEAMIENTO **DE LA ACTIVIDAD**

De acuerdo con la información anterior, realice las siguientes actividades:

1. Defina la política de seguridad para Datalatina, según la estructura vista en el Escenario 5.
2. Proponga un plan de implementación y desarrollo de política que contenga lo siguiente:
   a. Objetivos del SGSI
   b. Definición de alto nivel del alcance y marco de referencia para el SGSI
   c. Procedimientos y controles que apoyan la política

d. Definición de roles y responsabilidades

e. Indicación de alto nivel de alcance y límite a nivel físico de TICS y de organización.

3. Definir un plan de sensibilización para la implementación de la política de seguridad.

Item de la estructura	Descripción
Introducción	Indicación general de la temática del documento, donde se justifique de manera clara la realización del programa de sensibilización.
Objetivos	Responder a la pregunta sobre qué se espera lograr con el plan. Se deben redactar en infinitivo de manera general.
Alineación a política	Se debe indicar cómo el programa de sensibilización se encuentra alineado con la política de seguridad. Debe incluir las políticas generales y específicas.
Alcance	Se debe indicar quiénes, cuántos y cómo se verán beneficiados con el programa.
Roles y responsabilidades	Definición del equipo de trabajo con indicación de perfiles, roles y responsabilidades dentro del plan.
Metas	Orientadas a los indicadores de cumplimiento. Deben ser medibles. Deben partir de los objetivos.
Definición de audiencia	Segmentar al público objetivo con el fin de mejorar la eficiencia.
Definición de temáticas	Los temas dependerán de la política y de la definición del SGSI.
Actividades de sensibilización programadas	Se deben indicar las tareas puntuales, quién las realiza, cómo y su respectiva duración.
Materiales y recursos	Son los instrumentos de sensibilización. Debe indicarse el tipo, el tiempo que permanecerá visible y sus objetivos. Algunos tipos son afiches, folletos, protectores de pantalla, recordatorios, presentaciones y planes de capacitación.
Duración	Se debe indicar la duración completa del plan. Se propone que no sea inferior a 6 meses, dependiendo de la complejidad de la política.
Definición de evaluación	Mencionar los indicadores de calidad del programa, medios para la evaluación, frecuencia, etc.
Conclusiones	A partir de los resultados de la evaluación se deben indicar las conclusiones sobre el programa, orientadas al cumplimiento de metas y objetivos.
Plan de mejora	Proponer planes de mejora de acuerdo con los resultados obtenidos.