GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN

INTRODUCCIÓN Y ANTECEDENTES

La gestión de los incidentes de seguridad es un aspecto muy importante para lograr el mejoramiento continuo de la seguridad de la información de cualquier compañía, el principal inconveniente es que muchas organizaciones o empresas no lo utilizan adecuadamente. La gestión de incidentes en la seguridad de la información es de gran importancia para una empresa ya que se encarga de mejorar la seguridad en la compañía y así tener en cuenta que la revisión continua de la información o de algún sistema es muy importante ya que además de seguridad garantiza la disponibilidad, la integridad y la confidencialidad de la información con la que cuenta la organización. La gestión es la norma o bien reglas de recomendaciones con las advertencias de ciertos eventos que puedan ocurrir al momento de un ataque además de ver cuáles son los puntos más débiles en los cuales se tendría que mejorar. También verifica los procedimientos y responsabilidades que se deberían de asignar a la gestión de incidentes en la seguridad.
Si la compañía no dispone de ningún sistema de reporte de eventos o la debilidad de la seguridad en algunos momentos, es necesario implementar los procedimientos adecuados para que todos los empleados y terceras personas involucrados en la información con la que cuenta la empresa puedan reportar los diferentes tipos de eventos o debilidades que puede tiene un impacto en la seguridad. Para esto es necesario tener un control o una respuesta a los incidentes en caso de presentarse. Por esta razón er importante monitorizar y controlar los eventos que vallan surgiendo en la compañía con el objetivo de tener evidencias sólidas y legales para cualquier procedimiento o acción legal que se pueda realizar es por ello que la gestión de incidentes de la seguridad de la información es importante para la empresa.

OBJETIVOS

El objetivo que se persigue con la comunicación de los eventos que se presenten relacionados con la seguridad de la información, es el de garantizar que las causas, los tratamientos y la solución de dichos eventos sirvan para la implementación de acciones correctivas y preventivas oportunas en casos similares que pudieran presentarse en un futuro. Para lograrlo se deben implementar los canales apropiados que garanticen la agilidad en la comunicación de los eventos de seguridad que pudieran presentarse y permitir que los usuarios reporten las debilidades encontradas o que crean que pueden utilizarse para poner en riesgo la seguridad de la información. Estos sistemas pueden apoyarse en los desarrollos que se tengan alrededor de las mesas de ayuda y las estrategias de gestión de solicitudes para atender inconvenientes de tipo tecnológico en la compañía.
Además de tener una herramienta para la gestión de incidentes es necesario establecer las responsabilidades y los procedimientos de gestión para asegurar una respuesta rápida, efectiva y ordenada a los incidentes en la seguridad de información. Estos procesos deben contribuir al logro de la mejora continua en la evaluación y monitoreo de los incidentes en la seguridad de información.

GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN Y MEJORAS

Deberían establecerse las responsabilidades y procedimientos para manejar los eventos y debilidades en la seguridad de información de una manera efectiva y una vez que hayan sido comunicados. Se debería aplicar un proceso de mejora continua en respuesta para monitorear, evaluar y gestionar en su totalidad los incidentes en la seguridad de información. Cuando se requieran evidencias, éstas deben ser recogidas para asegurar el cumplimiento de los requisitos legales. Debería establecerse el informe formal de los eventos y de los procedimientos de escalado. Todos los empleados, contratistas y terceros deberían estar al tanto de los procedimientos para informar de los diferentes tipos de eventos y debilidades que puedan tener impacto en la seguridad de los activos organizacionales. Se les debería exigir que informen de cualquier evento o debilidad en la seguridad de información lo más rápido posible y al punto de contacto designado.

Responsabilidades y procedimientos. Se deberían establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.

Notificación de los eventos de seguridad de la información. Los eventos de seguridad de la información se deberían informar lo antes posible utilizando los canales de administración adecuados.

Notificación de puntos débiles de la seguridad. Se debería requerir anotar e informar sobre cualquier debilidad sospechosa en la seguridad de la información en los sistemas o servicios tanto a los empleados como a contratistas que utilizan los sistemas y servicios de información de la organización.

Valoración de eventos de seguridad de la información y toma de decisiones. Se deberían evaluar los eventos de seguridad de la información y decidir su clasificación como incidentes.

Respuesta a los incidentes de seguridad. Se debería responder ante los incidentes de seguridad de la información en atención a los procedimientos documentados.

Aprendizaje de los incidentes de seguridad de la información. Se debería utilizar el conocimiento obtenido del análisis y la resolución de incidentes de seguridad de la información para reducir la probabilidad y/o impacto de incidentes en el futuro.

Recopilación de evidencias. La organización debería definir y aplicar los procedimientos necesarios para la identificación, recopilación, adquisición y preservación de la información que puede servir de evidencia.

FUENTES DE BIBLIOGRAFICAS

- http://gestiondeincidenciasenlaseguridad.blogspot.com/
- https://www.isotools.com.co/iso-27001-gestionar-incidencias-seguridad-informacion/
- https://iso27002.wiki.zoho.com/13Incidentes.html
- https://www.isotools.com.co/iso-27001-gestionar-incidencias-seguridad-informacion/