MNEMO

Anexo 16

Ciclo de deming

GESTIÓN DE INCIDENTES

Dentro de esta área se localizan los siguientes objetivos y principios, controles y posibles mediciones asociadas:

A5.24	Planificación y preparación de la gestión de incidentes de seguridad de la información
Objetivo	La organización debería planificar y prepararse para la gestión de incidentes de seguridad de la información definiendo, estableciendo y comunicando procesos, roles y responsabilidades de gestión de incidentes de seguridad de la información.
Principios	Garantizar una respuesta rápida, eficaz, coherente y ordenada a los incidentes de seguridad de la información, incluida la comunicación de los eventos de seguridad de la información. Especificar y gestionar la seguridad de la información para el uso de los servicios en la nube. 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. Las revisiones post-incidentes y los casos de estudio para incidentes serios, tales como fraudes, ilustran los puntos débiles de control, identifican oportunidades de mejora y conforman por sí mismos un mecanismo eficaz de concienciación en seguridad.

A5.24	Planificación y preparación de la gestión de incidentes de seguridad de la información
Información	Establezca y dé a conocer una hotline (generalmente, el helpdesk habitual de TI) para que la gente pueda informar de incidentes, eventos y problemas de seguridad. Los incidentes de seguridad de la información pueden trascender las fronteras de la organización y del país. Para responder a estos incidentes, es beneficioso coordinar la respuesta y compartir la información sobre estos incidentes con organizaciones externas, según corresponda. En la serie ISO/IEC 27035 se ofrecen orientaciones detalladas sobre la gestión de incidentes de seguridad de la información.
Medición	Estadísticas del helpdesk de TI, con análisis sobre el número y tipos de llamadas relativas a seguridad de la información (p. ej., cambios de contraseña; porcentaje de preguntas acerca de riesgos y controles de seguridad de la información respecto al total de preguntas). A partir de las estadísticas, cree y publique una tabla de clasificación por departamentos (ajustada según el número de empleados por departamento), mostrando aquellos que están claramente concienciados con la seguridad, frente a los que no lo están

A5.25	Evaluación y decisión sobre eventos de seguridad de la información
Objetivo	La organización debe evaluar los eventos de seguridad de la información y decidir si deben categorizarse como incidentes de seguridad de la información.
Principios	Garantizar la categorización y priorización efectiva de los eventos de seguridad de la información.

A5.25	Evaluación y decisión sobre eventos de seguridad de la información
	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. Las revisiones post-incidentes y los casos de estudio para incidentes serios, tales como fraudes, ilustran los puntos débiles de control, identifican oportunidades de mejora y conforman por sí mismos un mecanismo eficaz de concienciación en seguridad.
Información	Establezca y dé a conocer una hotline (generalmente, el helpdesk habitual de TI) para que la gente pueda informar de incidentes, eventos y problemas de seguridad. Debe acordarse un esquema de categorización y priorización de los incidentes de seguridad de la información para la identificación de las consecuencias y la prioridad de un incidente. El esquema debe incluir los criterios para categorizar los eventos como incidentes de seguridad de la información. El punto de contacto debe evaluar cada incidente de seguridad de la información utilizando el esquema acordado. La serie ISO/IEC 27035 ofrece más orientaciones sobre la gestión de incidentes.
Medición	Estadísticas del helpdesk de TI, con análisis sobre el número y tipos de llamadas relativas a seguridad de la información (p. ej., cambios de contraseña; porcentaje de preguntas acerca de riesgos y controles de seguridad de la información respecto al total de preguntas).

A5.25	Evaluación y decisión sobre eventos de seguridad de la información
	A partir de las estadísticas, cree y publique una tabla de clasificación por departamentos (ajustada según el número de empleados por departamento), mostrando aquellos que están claramente concienciados con la seguridad, frente a los que no lo están

A5.26	Respuesta a incidentes de seguridad de la información
Objetivo	Los incidentes de seguridad de la información deben responderse de acuerdo con los procedimientos documentados.
Principios	Garantizar una respuesta eficiente y eficaz a los incidentes de seguridad de la información. 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. Las revisiones post-incidentes y los casos de estudio para incidentes serios, tales como fraudes, ilustran los puntos débiles de control, identifican oportunidades de mejora y conforman por sí mismos un mecanismo eficaz de concienciación en seguridad.
Información	Establezca y dé a conocer una hotline (generalmente, el helpdesk habitual de TI) para que la gente pueda informar de incidentes, eventos y problemas de seguridad. La organización debe establecer y comunicar los procedimientos de respuesta a incidentes de seguridad de la información a todas las partes interesadas pertinentes.

A5.26	Respuesta a incidentes de seguridad de la información
	A los incidentes de seguridad de la información debe responder un equipo designado con la competencia necesaria (véase 5.24). La serie ISO/IEC 27035 proporciona más orientación sobre la gestión de incidentes.
Medición	Porcentaje de incidentes de seguridad de la información sobre el total de incidentes. Porcentaje de los incidentes de seguridad de la información revisados y probados sobre el total de los incidentes documentados. Porcentaje de los incidentes de seguridad de la información investigados. Porcentaje de respuestas a incidentes canalizados de acuerdo con las actividades previamente identificadas.

A5.27	Aprendiendo de los incidentes de seguridad de la información
Objetivo	El conocimiento obtenido de los incidentes de seguridad de la información debería usarse para fortalecer y mejorar los controles de seguridad de la información.
Principios	Reducir la probabilidad o las consecuencias de futuros incidentes. 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.

A5.27	Aprendiendo de los incidentes de seguridad de la información
	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. Las revisiones post-incidentes y los casos de estudio para incidentes serios, tales como fraudes, ilustran los puntos débiles de control, identifican oportunidades de mejora y conforman por sí mismos un mecanismo eficaz de concienciación en seguridad.
Información	Establezca y dé a conocer una hotline (generalmente, el helpdesk habitual de TI) para que la gente pueda informar de incidentes, eventos y problemas de seguridad. La organización debe establecer procedimientos para cuantificar y controlar los tipos, volúmenes y costes de los incidentes de seguridad de la información. La información obtenida de la evaluación de los incidentes de seguridad de la información debe utilizarse para a) mejorar el plan de gestión de incidentes, incluyendo los escenarios y procedimientos de incidentes (véase 5.24); b) identificar los incidentes recurrentes o graves y sus causas para actualizar la evaluación de riesgos de seguridad de la información de la organización y determinar e implementar los controles adicionales necesarios para reducir la probabilidad o las consecuencias de futuros incidentes similares. Los mecanismos para permitirlo incluyen la recopilación, cuantificación y seguimiento de la información sobre los tipos, volúmenes y costes de los incidentes; c) mejorar la concienciación y la formación de los usuarios (véase el apartado 6.3) proporcionando ejemplos de lo que puede ocurrir, cómo responder a esos incidentes y cómo evitarlos en el futuro. La serie ISO/IEC 27035 proporciona más orientación.

A5.27	Aprendiendo de los incidentes de seguridad de la información
Medición	Estadísticas del helpdesk de TI, con análisis sobre el número y tipos de llamadas relativas a seguridad de la información (p. ej., cambios de contraseña; porcentaje de preguntas acerca de riesgos y controles de seguridad de la información respecto al total de preguntas). A partir de las estadísticas, cree y publique una tabla de clasificación por departamentos (ajustada según el número de empleados por departamento), mostrando aquellos que están claramente concienciados con la seguridad, frente a los que no lo están

A5.28	Recolección de evidencia
Objetivo	La organización debería establecer e implementar procedimientos para la identificación, recopilación, adquisición y preservación de evidencia relacionada con eventos de seguridad de la información.
Principios	Garantizar una gestión coherente y eficaz de las pruebas relacionadas con los incidentes de seguridad de la información a efectos de acciones disciplinarias y 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.

A5.28	Recolección de evidencia
Información	Establezca y dé a conocer una hotline (generalmente, el helpdesk habitual de TI) para que la gente pueda informar de incidentes, eventos y problemas de seguridad. Deben desarrollarse y seguirse procedimientos internos cuando se traten pruebas relacionadas con eventos de seguridad de la información a efectos de acciones disciplinarias y legales. Deberán tenerse en cuenta los requisitos de las diferentes jurisdicciones para maximizar las posibilidades de admisión en las jurisdicciones pertinentes. En general, estos procedimientos para la gestión de las pruebas deben proporcionar instrucciones para la identificación, la recogida, la adquisición y la conservación de las pruebas de acuerdo con los diferentes tipos de medios de almacenamiento, dispositivos y estado de los dispositivos (es decir, encendidos o apagados). Por lo general, las pruebas deben recogerse de manera que sean admisibles en los tribunales nacionales correspondientes o en otro foro disciplinario. La norma ISO/IEC 27037 proporciona definiciones y directrices para la identificación, recogida, adquisición y conservación de pruebas digitales. La serie ISO/IEC 27050 se ocupa del descubrimiento electrónico, que implica el tratamiento de la información almacenada electrónicamente como prueba.
Medición	Porcentaje de evidencias colectadas sobre la cantidad de incidentes de seguridad de la información. Porcentaje de evidencias de incidentes de seguridad de la información resguardadas sobre la totalidad de las evidencias resguardadas.

A6.8	Notificaciones de eventos de seguridad de la información
Objetivo	La organización debe proporcionar un mecanismo para que el personal informe los eventos de seguridad de la información observados o sospechados a través de los canales apropiados de manera oportuna.
Principios	Apoyar la notificación oportuna, coherente y eficaz de los eventos de seguridad de la información que puedan ser identificados por el personal. 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. Las revisiones post-incidentes y los casos de estudio para incidentes serios, tales como fraudes, ilustran los puntos débiles de control, identifican oportunidades de mejora y conforman por sí mismos un mecanismo eficaz de concienciación en seguridad.
Información	Establezca y dé a conocer una hotline (generalmente, el helpdesk habitual de TI) para que la gente pueda informar de incidentes, eventos y problemas de seguridad. Todo el personal y los usuarios deben ser conscientes de su responsabilidad de informar sobre los eventos de seguridad de la información tan pronto como sea posible con el fin de prevenir o minimizar el efecto de los incidentes de seguridad de la información. Se debe aconsejar al personal y a los usuarios que no intenten probar las presuntas vulnerabilidades de la seguridad de la información. Probar las vulnerabilidades puede interpretarse como

A6.8	Notificaciones de eventos de seguridad de la información
	un posible mal uso del sistema y también puede causar daños al sistema o servicio de información, y puede corromper u ocultar las pruebas digitales. En última instancia, esto puede dar lugar a la responsabilidad legal de la persona que realiza las pruebas. Consulte la serie ISO/IEC 27035 para obtener información adicional.
Medición	Estadísticas del helpdesk de TI, con análisis sobre el número y tipos de llamadas relativas a seguridad de la información (p. ej., cambios de contraseña; porcentaje de preguntas acerca de riesgos y controles de seguridad de la información respecto al total de preguntas). A partir de las estadísticas, cree y publique una tabla de clasificación por departamentos (ajustada según el número de empleados por departamento), mostrando aquellos que están claramente concienciados con la seguridad, frente a los que no lo están