MNEMO

Anexo 15

Ciclo de Deming

RELACIÓN CON PROVEEDORES

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

A5.19	Seguridad de la información en las relaciones con los proveedores
Objetivo	Deben definirse e implementarse procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con el uso de los productos y/o o servicios proveídos por terceros.
Principios	Mantener un nivel acordado de seguridad de la información en las relaciones con los proveedores. Todos los requisitos de seguridad de la información deben ser establecidos y acordados con cada proveedor que pueda acceder, procesar, almacenar, la información de la organización que así se haya acordado.
Información	Se debe documentar a que información y que requisitos de seguridad deben ser habilitados para que terceras partes accedan a la información. Estos acuerdos incluirán requisitos para abordar la seguridad de la información y el riesgo asociado a los servicios de tecnología de las comunicaciones. Los proveedores con una gestión inadecuada de la seguridad de la información pueden poner en peligro la información. Deben determinarse y aplicarse controles para gestionar el acceso del proveedor a la información y otros activos asociados. Por ejemplo, si hay una necesidad especial de confidencialidad de la información, se pueden utilizar acuerdos de no divulgación o técnicas criptográficas. Otro ejemplo son los riesgos de protección de datos personales cuando el acuerdo con el proveedor implica la transferencia de información o el acceso a ella a través de las fronteras. La organización debe ser consciente de que la

A5.19	Seguridad de la información en las relaciones con los proveedores
	responsabilidad legal o contractual de proteger la información sigue siendo de la organización.
Medición	Porcentaje de conexiones con terceras partes que han sido identificadas, evaluadas en cuanto a su riesgo y estimadas como seguras.

A5.20	Abordar la seguridad de la información dentro de los acuerdos con proveedores
Objetivo	Los requisitos de seguridad de la información relevantes deben establecerse y acordarse con cada proveedor en función del tipo de relación con el proveedor.
Principios	Mantener un nivel acordado de seguridad de la información en las relaciones con los proveedores. Todos los requisitos de seguridad de la información deben ser establecidos y acordados con cada proveedor que pueda acceder, procesar, almacenar, la información de la organización que así se haya acordado.
Información	Se debe documentar a que información y que requisitos de seguridad deben ser habilitados para que terceras partes accedan a la información. Estos acuerdos incluirán requisitos para abordar la seguridad de la información y el riesgo asociado a los servicios de tecnología de las comunicaciones. Los acuerdos con los proveedores deben establecerse y documentarse para garantizar que existe un claro entendimiento entre la organización y el proveedor respecto a las obligaciones de ambas partes de cumplir con los requisitos pertinentes de seguridad de la información.

A5.20	Abordar la seguridad de la información dentro de los acuerdos con proveedores
	Los acuerdos pueden variar considerablemente para las diferentes organizaciones y entre los diferentes tipos de proveedores. Por lo tanto, se debe tener cuidado de incluir todos los requisitos pertinentes para abordar los riesgos de seguridad de la información. Para más detalles sobre los acuerdos con proveedores, véase la serie ISO/IEC 27036. Para los acuerdos de servicios en la nube, véase la serie ISO/IEC 19086.
Medición	Porcentaje de conexiones con terceras partes que han sido identificadas, evaluadas en cuanto a su riesgo y estimadas como seguras.

A5.21	Gestión de la seguridad de la información en la cadena de suministro de las TIC
Objetivo	Deben definirse e implementarse procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de TIC.
Principios	Mantener un nivel acordado de seguridad de la información en las relaciones con los proveedores Todos los requisitos de seguridad de la información deben ser establecidos y acordados con cada proveedor que pueda acceder, procesar, almacenar, la información de la organización que así se haya acordado.
Información	Se debe documentar a que información y que requisitos de seguridad deben ser habilitados para que terceras partes accedan a la información. Estos acuerdos incluirán requisitos para abordar la seguridad de la información y el riesgo asociado a los servicios de tecnología de las comunicaciones.

A5.21	Gestión de la seguridad de la información en la cadena de suministro de las TIC
	Se aconseja a las organizaciones que trabajen con los proveedores para entender la cadena de suministro de las TIC y cualquier asunto que tenga un efecto importante en los productos y servicios que se proporcionan. La organización puede influir en las prácticas de seguridad de la información de la cadena de suministro de TIC dejando claro en los acuerdos con sus proveedores los asuntos que deben ser tratados por otros proveedores en la cadena de suministro de TIC. Las TIC deben adquirirse de fuentes fiables. La fiabilidad del software y el hardware es una cuestión de control de calidad. Aunque generalmente no es posible que una organización inspeccione los sistemas de control de calidad de sus proveedores, puede hacer juicios fiables basados en la reputación del proveedor. Consulte la norma ISO/IEC 27036-3 para obtener más detalles, incluida la orientación para la evaluación de riesgos. Las etiquetas de identificación de software (SWID) también pueden ayudar a lograr una mejor seguridad de la información en la cadena de suministro, al proporcionar información sobre la procedencia del software. Véase la norma ISO/IEC 19770-2 para más detalles.
Medición	Porcentaje de conexiones con terceras partes que han sido identificadas, evaluadas en cuanto a su riesgo y estimadas como seguras.

A5.22	Seguimiento, revisión y gestión de cambios de los servicios de proveedores
Objetivo	La organización debe monitorear, revisar, evaluar y gestionar con regularidad los cambios en las prácticas de seguridad de la información de los proveedores y la prestación de servicios.
Principios	Mantener un nivel acordado de seguridad de la información y de prestación de servicios conforme a los acuerdos con los proveedores Las organizaciones deben controlar regularmente, la revisión y la prestación de servicios de servicios de auditoría. Se debería evitar la exposición de datos sensibles en entornos de prueba.
Información	Deben asegurarse un seguimiento y revisión de los servicios prestados por los proveedores, revisando que las condiciones de seguridad y los acuerdos se están cumpliendo. Así mismo se ha de verificar que los incidentes de seguridad de la información y los problemas se gestionan adecuadamente El seguimiento, la revisión y la gestión de los cambios de los servicios de los proveedores deben garantizar el cumplimiento de las condiciones de seguridad de la información de los acuerdos, la gestión adecuada de los incidentes y problemas de seguridad de la información y que los cambios en los servicios de los proveedores o en la situación empresarial no afecten a la prestación de los servicios. Garantizar que el proveedor mantiene una capacidad de servicio suficiente, junto con planes viables diseñados para garantizar el mantenimiento de los niveles de continuidad del servicio acordados tras fallos importantes del servicio o catástrofes (véanse los puntos 5.29, 5.30, 5.35, 5.36 y 8.14). La responsabilidad de la gestión de las relaciones con los proveedores debe asignarse a una persona o equipo designado. Deben ponerse a disposición de los proveedores los conocimientos técnicos y los recursos suficientes para supervisar que se cumplen los requisitos del acuerdo, en particular los relativos a la seguridad

A5.22	Seguimiento, revisión y gestión de cambios de los servicios de proveedores
	de la información. Deben tomarse las medidas adecuadas cuando se observen deficiencias en la prestación del servicio.
Medición	Porcentaje de sistemas evaluados de forma independiente como totalmente conformes con los estándares de seguridad básica aprobados, respecto a aquellos que no han sido evaluados, no son conformes o para los que no se han aprobado dichos estándares