MNEMO

Anexo 6

ASPECTOS ORGANIZATIVOS

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

A5.2	Roles y responsabilidades de seguridad de la información
Objetivo	Los roles y responsabilidades de seguridad de la información deben definirse y asignarse de acuerdo con las necesidades de la organización.
Principios	La Dirección debería establecer de manera precisa los roles, autoridad, responsabilidad dentro de la Seguridad de la Información. Se debería establecer una estructura de gestión con objeto de iniciar y controlar la implantación de la seguridad de la información dentro de la Organización. El órgano de dirección debería aprobar la política de seguridad de la información, asignar los roles de seguridad y coordinar y revisar la implantación de la seguridad en toda la Organización. Si fuera necesario, en la Organización se debería establecer y facilitar el acceso a una fuente especializada de consulta en seguridad de la información. Deberían desarrollarse contactos con especialistas externos en seguridad, que incluyan a las administraciones pertinentes, con objeto de mantenerse actualizado en las tendencias de la industria, la evolución de las normas y los métodos de evaluación, así como proporcionar enlaces adecuados para el tratamiento de las incidencias de seguridad. Debería fomentarse un enfoque multidisciplinario de la seguridad de la información, que, por ejemplo, implique la cooperación y la colaboración de directores, usuarios, administradores, diseñadores de aplicaciones, auditores y el equipo de seguridad con expertos en

A5.2	Roles y responsabilidades de seguridad de la información
	áreas como la gestión de seguros, la gestión de riesgos y en general en todos los proyectos que se desarrollen dentro de la organización independientemente de su naturaleza.
Información	La definición de los roles y responsabilidades deben ser realizadas en concordancia con la política de seguridad de la información y políticas sobre temas específicos relacionados dentro de los aspectos de desarrollo de la organización, a nivel administrativo y operativo relacionado con seguridad de la información. Conjuntamente con la designación de los roles y controles se deben definir los niveles de autoridad de cada rol. Toda la organización debe conocer quienes asumen los roles y responsabilidades dentro del SGSI Dependiendo del tamaño y de los recursos de una organización, la seguridad de la información puede cubrirse con funciones específicas o con funciones adicionales a las existentes. Reproduzca la estructura y tamaño de otras funciones corporativas especializadas, como Legal, Riesgos y Compliance.
Medición	Cumplimiento de los nombramientos donde se asignen los roles y responsabilidades, adicionalmente a los roles naturales que realizan las personas a quienes se les ha asignado estos roles y las responsabilidades, Porcentaje de funciones/unidades organizativas para las cuales se ha implantado una estrategia global para mantener los riesgos de seguridad de la información por debajo de umbrales explícitamente aceptados por la dirección. Porcentaje de empleados que han (a) recibido y (b) aceptado formalmente, roles y responsabilidades de seguridad de la información.

A5.3	Segregación de deberes
Objetivo	Deben segregarse los deberes y las áreas de responsabilidad en conflicto.
Principios	Las funciones y áreas de responsabilidad deben segregarse para reducir la posibilidad de que se produzcan modificaciones no autorizadas o no intencionadas o usos indebidos de los activos de la organización. Se debería establecer una estructura de gestión con objeto de iniciar y controlar la implantación de la seguridad de la información dentro de la Organización. Debería fomentarse un enfoque multidisciplinario de la seguridad de la información, que, por ejemplo, implique la cooperación y la colaboración de directores, usuarios, administradores, diseñadores de aplicaciones, auditores y el equipo de seguridad con expertos en áreas como la gestión de seguros, la gestión de riesgos y en general en todos los proyectos que se desarrollen dentro de la organización independientemente de su naturaleza.
Información	La segregación de funciones y áreas de responsabilidad tiene como objetivo separar las funciones conflictivas entre diferentes personas para evitar que una persona ejecute por sí misma posibles funciones conflictivas. La organización debe determinar qué funciones y áreas de responsabilidad deben separarse
Medición	Porcentaje de funciones/unidades organizativas para las cuales se ha implantado una estrategia global de segregación para mantener los riesgos de seguridad de la información por debajo de umbrales explícitamente aceptados por la dirección. Porcentaje de empleados que han (a) recibido y (b) aceptado formalmente, roles y responsabilidades de seguridad de la información.

A5.5	Contacto con las autoridades
Objetivo	La organización debería establecer y mantener contacto con las autoridades pertinentes.
Principios	Deben mantenerse los contactos apropiados con las autoridades pertinentes. Garantizar un flujo de información adecuado con respecto a la seguridad de la información entre la organización y las autoridades legales, reglamentarias y de supervisión pertinentes.
Información	Se debería establecer una estructura de gestión con objeto de iniciar y controlar la implantación de la seguridad de la información dentro de la Organización. La organización debe especificar cuándo y quién debe ponerse en contacto con las autoridades (por ejemplo, las fuerzas de seguridad, los organismos reguladores, las autoridades de supervisión) y cómo se deben notificar oportunamente los incidentes de seguridad de la información identificados. Los contactos con las autoridades también deben servir para facilitar la comprensión de las expectativas actuales y futuras de estas autoridades (por ejemplo, las normas de seguridad de la información aplicables). Deberían desarrollarse contactos con especialistas externos en seguridad, que incluyan a las administraciones pertinentes, con objeto de mantenerse actualizado en las tendencias de la industria, la evolución de las normas y los métodos de evaluación, así como proporcionar enlaces adecuados para el tratamiento de las incidencias de seguridad. Debería fomentarse un enfoque multidisciplinario de la seguridad de la información, que, por ejemplo, implique la cooperación y la colaboración de directores, usuarios, administradores, diseñadores de aplicaciones, auditores y el equipo de seguridad con expertos en áreas como la gestión de seguros, la gestión de riesgos y en general

A5.5	Contacto con las autoridades
	en todos los proyectos que se desarrollen dentro de la organización independientemente de su naturaleza.
Medición	Número de actualizaciones de los datos de contacto de las Autoridades y Contactos externos relacionados con las actividades de la organización. Número de documentos, correos, e información intercambiada con las Autoridades, contactos externos definidos y fuentes de información.

A5.6	Contacto con grupos de interés especial
Objetivo	La organización debería establecer y mantener contacto con grupos de intereses especiales u otros foros especializados en seguridad y asociaciones profesionales.
Principios	Deben mantenerse los contactos apropiados con grupos de interés especial, u otros foros y asociaciones profesionales especializados en seguridad, para garantizar un flujo de información adecuado con respecto a la seguridad de la información. Se debería establecer una estructura de gestión con objeto de iniciar y controlar la implantación de la seguridad de la información dentro de la Organización. El órgano de dirección debería aprobar la política de seguridad de la información, asignar los roles de seguridad y coordinar y revisar la implantación de la seguridad en toda la Organización. Si fuera necesario, en la Organización se debería establecer y facilitar el acceso a una fuente especializada de consulta en seguridad de la información. Deberían desarrollarse contactos con especialistas externos en seguridad, que incluyan a las administraciones pertinentes, con objeto de mantenerse

A5.6	Contacto con grupos de interés especial
	actualizado en las tendencias de la industria, la evolución de las normas y los métodos de evaluación, así como proporcionar enlaces adecuados para el tratamiento de las incidencias de seguridad. Debería fomentarse un enfoque multidisciplinario de la seguridad de la información, que, por ejemplo, implique la cooperación y la colaboración de directores, usuarios, administradores, diseñadores de aplicaciones, auditores y el equipo de seguridad con expertos en áreas como la gestión de seguros, la gestión de riesgos y en general en todos los proyectos que se desarrollen dentro de la organización independientemente de su naturaleza.
Información	La pertenencia a grupos o foros de interés especial debe considerarse como un medio para: a) mejorar los conocimientos sobre las mejores prácticas y mantenerse al día con la información de seguridad pertinente; b) asegurarse de que la comprensión del entorno de seguridad de la información está actualizada c) recibir avisos tempranos de alertas, avisos y parches relativos a ataques y vulnerabilidades d) Acceder al asesoramiento especializado en seguridad de la información; e) compartir e intercambiar información sobre nuevas tecnologías, productos, servicios, amenazas o vulnerabilidades f) proporcionar puntos de enlace adecuados cuando se trate de incidentes de seguridad de la información (véanse los puntos 5.24 a 5.28).
Medición	Número de actividades realizadas con y en Foros especializados. Número de participación de empleados en foros, seminarios y webinarios relacionados con la Seguridad de la Información.

A5.8	Seguridad de la información en la gestión de proyectos
Objetivo	La seguridad de la información debería ser integrada en la gestión de proyectos
Principios	La seguridad de la información debe tratarse dentro de la gestión de proyectos, independientemente de la naturaleza del proyecto. Garantizar que los riesgos de seguridad de la información relacionados con los proyectos y los resultados se abordan de forma eficaz en la gestión de proyectos a lo largo del ciclo de vida de los mismos. Dentro de los sistemas de información se incluyen los sistemas operativos, infraestructuras, aplicaciones de negocio, aplicaciones estándar o de uso generalizado, servicios y aplicaciones desarrolladas por los usuarios. El diseño e implantación de los sistemas de información que sustentan los procesos de negocio pueden ser cruciales para la seguridad. Los requisitos de seguridad deberían ser identificados y consensuados previamente al desarrollo y/o implantación de los sistemas de información. Todos los requisitos de seguridad deberían identificarse en la fase de recogida de requisitos de un proyecto y ser justificados, aceptados y documentados como parte del proceso completo para un sistema de información. Se debería establecer una estructura de gestión con objeto de iniciar y controlar la implantación de la seguridad de la información dentro de la Organización. Debería fomentarse un enfoque multidisciplinario de la seguridad de la información, que, por ejemplo, implique la cooperación y la colaboración de directores, usuarios, administradores, diseñadores de aplicaciones, auditores y el equipo de seguridad con expertos en áreas como la gestión de seguros, la gestión de riesgos y en general en todos los proyectos que se desarrollen dentro de la organización independientemente de su naturaleza.

A5.8	Seguridad de la información en la gestión de proyectos
Información	Involucre a los "propietarios de activos de información" en evaluaciones de riesgos a alto nivel y consiga su aprobación de los requisitos de seguridad que surjan. Si son realmente responsables de proteger sus activos, es en interés suyo el hacerlo bien. Esté al tanto de las novedades sobre vulnerabilidades comunes o actuales en aplicaciones e identifique e implemente las medidas protectoras o defensivas apropiadas. Numerosas referencias ofrecen orientación sobre la implementación, como, p. ej., OWASP. La norma ISO/IEC 27005 ofrece orientación sobre el uso de los procesos de gestión de riesgos para identificar los controles para cumplir con los requisitos de seguridad de la información.
Medición	Porcentaje de sistemas y aplicaciones corporativas para los que los "propietarios" adecuados han: (a) sido identificados, (b) aceptado formalmente sus responsabilidades, (c) llevado a cabo -o encargado- revisiones de accesos y seguridad de aplicaciones, basadas en riesgo y (d) definido las reglas de control de acceso basadas en roles. Porcentaje de funciones/unidades organizativas para las cuales se ha implantado una estrategia global para mantener los riesgos de seguridad de la información por debajo de umbrales explícitamente aceptados por la dirección. Porcentaje de empleados que han (a) recibido y (b) aceptado formalmente, roles y responsabilidades de seguridad de la información.

A8.1, A6.7	Dispositivos Móviles y Teletrabajo
Objetivo	Para garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.
Principios	Garantizar la seguridad de la información cuando el personal trabaja a distancia. Los usuarios deben asegurarse que el equipo desatendido tiene la protección adecuada. Para proteger la información contra los riesgos introducidos por el uso de dispositivos de punto final del usuario La política y el apoyo a las medidas de seguridad debe adoptarse para gestionar los riesgos introducidos por el uso de dispositivos móviles, así como para garantizar que se implementan las medidas de seguridad de cara a proteger la información de acceso, y aquella tratada o almacenados en sitios de teletrabajo.
Información	Haga inventario de conexiones de red y flujos de información significativos con terceras partes, evalúe sus riesgos y revise los controles de seguridad de información existentes respecto a los requisitos. ¡Esto puede dar miedo, pero es 100% necesario! Considere exigir certificados en ISO/IEC 27001:2022 a los PARTNERS más críticos, tales como outsourcing de-TI, proveedores de servicios de seguridad TI, etc.
Medición	Porcentaje de conexiones con terceras partes que han sido identificadas, evaluadas en cuanto a su riesgo y estimadas como seguras.