MNEMO

ANEXO 13

SEGURIDAD EN LAS COMUNICACIONES

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

A8.20	Seguridad de las redes
Objetivo	Las redes y los dispositivos de red deberían estar asegurados, gestionados y controlados para proteger la información en los sistemas y aplicaciones.
Principios	Proteger la información en las redes y sus instalaciones de procesamiento de información de apoyo contra el compromiso a través de la red. La gestión de la seguridad de las redes, las cuales pueden cruzar las fronteras de la organización, exige la atención a los flujos de datos, implicaciones legales, monitoreo y la protección; para esto es importante establecer acuerdos de nivel de servicio tanto cuando son gestionados por la organización como si son servicios tercerizados. Podrían ser necesarios controles adicionales con el fin de proteger la información sensible que pasa por las redes públicas. Adicional, es importante que los grupos de servicios de información, los usuarios y los sistemas de información sean segregados en redes distintas
Información	Prepare e implante estándares, directrices y procedimientos de seguridad técnicos para redes y herramientas de seguridad de red como IDS/IPS (detección y prevención de intrusiones), gestión de vulnerabilidades, etc. La organización debe asegurarse de que se aplican los controles de seguridad adecuados al uso de las redes virtualizadas. Las redes virtualizadas también abarcan las redes definidas por software (SDN, SD-WAN). Las redes virtualizadas pueden ser deseables desde el punto de vista de la seguridad, ya que pueden permitir la

A8.20	Seguridad de las redes
	separación lógica de la comunicación que tiene lugar a través de las redes físicas, en particular para los sistemas y aplicaciones que se implementan utilizando la computación distribuida.
Medición	Número de incidentes de seguridad de red identificados en el mes anterior, dividido por categorías de leve / importante / grave, con análisis de tendencias y descripción comentada de todo incidente serio y tendencia adversa.

A8.21	Seguridad de los servicios de red
Objetivo	Los mecanismos de seguridad, los niveles de servicio y los requisitos de servicio de los servicios de red deberían ser identificados, implementados y monitorizados
Principios	Garantizar la seguridad en el uso de los servicios de red. La gestión de la seguridad de las redes, las cuales pueden cruzar las fronteras de la organización, exige la atención a los flujos de datos, implicaciones legales, monitoreo y la protección; para esto es importante establecer acuerdos de nivel de servicio tanto cuando son gestionados por la organización como si son servicios tercerizados. Podrían ser necesarios controles adicionales con el fin de proteger la información sensible que pasa por las redes públicas. Adicional, es importante que los grupos de servicios de información, los usuarios y los sistemas de información sean segregados en redes distintas.
Información	Prepare e implante estándares, directrices y procedimientos de seguridad técnicos para redes y herramientas de seguridad de red como IDS/IPS (detección y prevención de intrusiones), gestión de vulnerabilidades, etc.

A8.21	Seguridad de los servicios de red
	Los servicios de red incluyen el suministro de conexiones, servicios de red privada y soluciones de seguridad de red gestionadas, como cortafuegos y sistemas de detección de intrusiones. Estos servicios pueden ir desde un simple ancho de banda no gestionado hasta complejas ofertas de valor añadido. En la norma ISO/IEC 29146 se ofrecen más orientaciones sobre un marco para la gestión del acceso.
Medición	Número de incidentes de seguridad de red identificados en el mes anterior, dividido por categorías de leve / importante / grave, con análisis de tendencias y descripción comentada de todo incidente serio y tendencia adversa.

A8.22	Segregación de redes
Objetivo	Los grupos de servicios de información, los usuarios y los sistemas de información deberían estar segregados en las redes de la organización
Principios	Dividir la red en límites de seguridad y controlar el tráfico entre ellos en función de las necesidades de la empresa. La gestión de la seguridad de las redes, las cuales pueden cruzar las fronteras de la organización, exige la atención a los flujos de datos, implicaciones legales, monitoreo y la protección; para esto es importante establecer acuerdos de nivel de servicio tanto cuando son gestionados por la organización como si son servicios tercerizados. Podrían ser necesarios controles adicionales con el fin de proteger la información sensible que pasa por las redes públicas. Adicional, es importante que los grupos de servicios de información, los usuarios y los sistemas de información sean segregados en redes distintas.

A8.22	Segregación de redes
Información	Prepare e implante estándares, directrices y procedimientos de seguridad técnicos para redes y herramientas de seguridad de red como IDS/IPS (detección y prevención de intrusiones), gestión de vulnerabilidades, etc. La organización debe considerar la posibilidad de gestionar la seguridad de las grandes redes dividiéndolas en dominios de red independientes y separándolas de la red pública (es decir, Internet). Los dominios pueden elegirse en función de los niveles de confianza, criticidad y sensibilidad (por ejemplo, dominio de acceso público, dominio de escritorio, dominio de servidor, sistemas de bajo y alto riesgo), a lo largo de las unidades organizativas (por ejemplo, recursos humanos, finanzas, marketing) o alguna combinación (por ejemplo, dominio de servidor que se conecta a múltiples unidades organizativas). La segregación puede hacerse utilizando redes físicamente diferentes o utilizando redes lógicas diferentes. Las redes a menudo se extienden más allá de los límites de la organización, ya que se forman asociaciones empresariales que requieren la interconexión o el uso compartido de instalaciones de procesamiento de información y de redes. Estas extensiones pueden aumentar el riesgo de acceso no autorizado a los sistemas de información de la organización que utilizan la red, algunos de los cuales requieren protección de otros usuarios de la red debido a su sensibilidad o criticidad.
Medición	Número de incidentes de seguridad de red identificados en el mes anterior, dividido por categorías de leve / importante / grave, con análisis de tendencias y descripción comentada de todo incidente serio y tendencia adversa.

A5.14	Transferencia de la información
Objetivo	Reglas de transferencia de la información, procedimientos o acuerdos deberían ser implementados para todos los tipos de instalaciones para la transferencia dentro de la organización y entre la organización y otras partes relacionadas.
Principios	Mantener la seguridad de la información transferida dentro de una organización y con cualquier parte externa interesada. Se deberían realizar los intercambios sobre la base de una política formal de intercambio de información tanto interna como eterna, según los acuerdos de intercambio y cumplir con la legislación correspondiente. Se deberían establecer procedimientos y normas para proteger la información y los medios físicos que contienen información en tránsito. Se debería efectuar la documentación y revisión regular de los acuerdos de confidencialidad.
Información	Estudie canales de comunicaciones alternativos y "preautorizados", en especial direcciones de e-mail secundarias por si fallan las primarias o el servidor de correo, y comunicaciones offline por si caen las redes. La organización debe establecer y comunicar a todas las partes interesadas una política específica sobre la transferencia de información. Las normas, procedimientos y acuerdos para proteger la información en tránsito deben reflejar la clasificación de la información en cuestión. Cuando la información se transfiera entre la organización y terceros, deben establecerse y mantenerse acuerdos de transferencia (incluida la autenticación del receptor) para proteger la información en todas sus formas en tránsito (véase 5.10). Deben disponerse de controles diseñados para proteger la información transferida contra la interceptación, el acceso no autorizado, la copia, la modificación, el desvío, la destrucción y la

A5.14	Transferencia de la información
	denegación de servicio, incluidos los niveles de control de acceso acordes con la clasificación de la información en cuestión y cualquier control especial que sea necesario para proteger la información sensible, como el uso de técnicas criptográficas (véase 8.24).
Medición	Porcentaje de enlaces de terceras partes para los cuales se han (a) definido y (b) implementado satisfactoriamente los requisitos de seguridad de la información.

A6.6	Acuerdos de confidencialidad o de no divulgación
Objetivo	Los acuerdos de confidencialidad o de no divulgación que reflejan las necesidades de la organización para la protección de la información deberían ser identificados, documentados, revisados regularmente y firmados por el personal y otras partes interesadas pertinentes.
Principios	Mantener la confidencialidad de la información a la que puede acceder el personal o partes externas. Se deberían realizar los intercambios sobre la base de una política formal de intercambio de información tanto interna como eterna, según los acuerdos de intercambio y cumplir con la legislación correspondiente. Se deberían establecer procedimientos y normas para proteger la información y los medios físicos que contienen información en tránsito. Se debería efectuar la documentación y revisión regular de los acuerdos de confidencialidad.
Información	Estudie canales de comunicaciones alternativos y "preautorizados", en especial direcciones de e-mail secundarias por si fallan las

A6.6	Acuerdos de confidencialidad o de no divulgación
	primarias o el servidor de correo, y comunicaciones offline por si caen las redes. El verificar canales de comunicación alternativos reducirá el estrés en caso de un incidente real. La organización debe tener en cuenta el cumplimiento de los acuerdos de confidencialidad y no divulgación para la jurisdicción a la que se aplican (véase 5.31, 5.32, 5.33, 5.34). Los requisitos de los acuerdos de confidencialidad y no divulgación deben revisarse periódicamente y cuando se produzcan cambios que influyan en estos requisitos. Los acuerdos de confidencialidad y no divulgación protegen la información de la organización e informan a los firmantes de su responsabilidad de proteger, utilizar y divulgar la información de manera responsable y autorizada.
Medición	Porcentaje de enlaces de terceras partes para los cuales se han (a) definido y (b) implementado satisfactoriamente los requisitos de seguridad de la información.