MNEMO

Anexo 17

CONTINUIDAD DE NEGOCIO

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

A5.29	Seguridad de la información durante la interrupción
Objetivo	La organización debe planificar cómo mantener la seguridad de la información a un nivel apropiado durante la interrupción.
Principios	Proteger la información y otros activos asociados durante la interrupción. Se debería implantar un proceso de gestión de continuidad del negocio para reducir, a niveles aceptables, la interrupción causada por los desastres y fallos de seguridad (que, por ejemplo, puedan resultar desastres naturales, accidentes, fallas de equipos o acciones deliberadas) mediante una combinación de controles preventivos y de recuperación. Este proceso debería identificar los procesos críticos de negocio e integrar los requisitos de gestión de la seguridad de información para la continuidad del negocio con otros requisitos de continuidad relacionados con dichos aspectos como operaciones, proveedores de personal, materiales, transporte e instalaciones. Se deberían analizar las consecuencias de los desastres, fallas de seguridad, pérdidas de servicio y la disponibilidad del servicio y desarrollar e implantar planes de contingencia para asegurar que los procesos del negocio se pueden restaurar en los plazos requeridos las operaciones esenciales. La seguridad de información debería ser una parte integral del plan general de continuidad del negocio y de los demás procesos de gestión dentro de la organización. La gestión de la continuidad del negocio debería incluir adicionalmente al proceso de evaluación de controles para la identificación y reducción de riesgos, limitar las consecuencias de incidencias dañinas y asegurar la reanudación a tiempo de las operaciones esenciales.

A5.29	Seguridad de la información durante la interrupción
Información	Considere la gestión de continuidad de negocio como un proceso con entradas procedentes de diversas funciones (alta dirección, TI, operaciones, RRHH, etc.) y actividades (evaluación de riesgos, etc.). Asegure la coherencia y concienciación mediante personas y unidades organizativas relevantes en los planes de continuidad de negocio. Deberían llevarse a cabo las pruebas pertinentes (tales como pruebas sobre el papel, simulacros, pruebas de failover, etc.) para: (a) mantener los planes actualizados, (b) aumentar la confianza de la dirección en los planes y (c) familiarizar a los empleados relevantes con sus funciones y responsabilidades bajo condiciones de desastre. En el contexto de la planificación de la continuidad del negocio y de la continuidad de las TIC, puede ser necesario adaptar los requisitos de seguridad de la información en función del tipo de interrupción, en comparación con las condiciones operativas normales. Como parte del análisis del impacto en el negocio y de la evaluación de riesgos realizada en el marco de la gestión de la continuidad del negocio, deben considerarse y priorizarse las consecuencias de la pérdida de confidencialidad e integridad de la información, además de la necesidad de mantener la disponibilidad. La información sobre los sistemas de gestión de la continuidad del negocio se puede encontrar en las normas ISO 22301 e ISO 22313. En la norma ISO/TS 22317 se ofrecen más orientaciones sobre el análisis del impacto en el negocio (BIA).
Medición	Porcentaje de planes de continuidad de negocio en cada una de las fases del ciclo de vida (requerido / especificado / documentado / probado). Porcentaje de unidades organizativas con planes de continuidad de negocio que han sido adecuadamente (a) documentados y (b) probados mediante test apropiados en los últimos 12 meses