ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.

INTRODUCCIÓN Y ANTECEDENTES

Reaccionar a la interrupción de actividades del negocio y proteger sus procesos críticos frente a desastres o grandes fallos de los sistemas de información.

OBJETIVOS

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 de 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, controles para la identificación y reducción de riesgos, limitar las consecuencias de incidencias dañinas y asegurar la reanudación a tiempo de las operaciones esenciales.

Continuidad de la seguridad de la información

Se deberían determinar los requisitos de seguridad de la información al planificar la continuidad de los procesos de negocio y la recuperación ante desastres.

La organización debería establecer, documentar, implementar y mantener procesos, procedimientos y cambios de implementación para mantener los controles de seguridad de la información existentes durante una situación adversa.

Si los controles de seguridad no pueden continuar resguardando la información ante situaciones adversas, se deberían establecer, implementar y mantener otros controles para mantener un nivel aceptable de seguridad de la información.

Las organizaciones deberían verificar la validez y la efectividad de las medidas de continuidad de la seguridad de la información regularmente, especialmente cuando cambian los sistemas de información, los procesos, los procedimientos y los controles de seguridad de la información, o los procesos y soluciones establecidas para la gestión de la continuidad de negocio.

Planificación de la continuidad de la seguridad de la información

La continuidad de seguridad de la información se debería incluir en os sistemas de gestión de la continuidad del negocio.

La norma busca que los activos de la organización siempre estén disponibles, y cuando no pueda estarlo, su tiempo de disponibilidad sea mínimo para no afectar las operaciones criticas del negocio.

Control: determinar requisitos o circunstancias para que se cumpla la seguridad de la información y continuidad ante situaciones adversas

Implantación de la continuidad de la seguridad de la información

Interpretar, establecer, documentar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa
Implementación
Contar con:
Estructura adecuada para prepararse, gestionar, mitigar.
Contar con el personal idóneo
Desarrollar y probar planes de respuesta y control documentos para mantener la seguridad de la información.

Verificación, revisión y evaluación de la continuidad de la seguridad de la información

Verificar los planes y controles implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.
Implementación
Revisar los procedimientos que han sufrido cambios en la organización y que pueden afectar el plan de negocio y la seguridad de la información

Redundancias

Se deberían considerar los componentes o arquitecturas redundantes cuando no se pueda garantizar el nivel de disponibilidad requerido por las actividades de la organización a través de arquitecturas sencillas típicas o los sistemas existentes se demuestren insuficientes.

Se deberían probar los sistemas de información redundantes para garantizar que la conmutación funcione adecuadamente.

Disponibilidad de instalaciones para el procesamiento de la información: Se debería implementar la suficiente redundancia en las instalaciones de procesamiento de la información y en correspondencia con los requisitos de disponibilidad.