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

Continuidad de la seguridad de la información
Tiene como objetivo asegurar que la continuidad de la seguridad de la información debería ser integrada en los sistemas de gestión de la continuidad de negocio de la organización

Planificación de la continuidad de la seguridad de la información
La organización debería determinar sus requisitos de seguridad de la información y la continuidad de la gestión de seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.

Una organización debería determinar si la continuidad de la seguridad de la información está incluida dentro del proceso de gestión de continuidad del negocio o en el proceso de gestión de recuperación ante desastres. Deberían determinarse los requisitos de seguridad de la información al planificar la continuidad del negocio y la recuperación ante desastres.

Si no existe una planificación formal de continuidad del negocio y de recuperación ante desastres, la gestión de seguridad de la información debería asumir que los requisitos de seguridad de la información siguen siendo los mismos en situaciones adversas, en comparación con las condiciones de funcionamiento normales. Alternativamente, una organización podría realizar un análisis de impacto en el negocio para aspectos de seguridad de la información con el fin de determinar los requisitos de seguridad de la información aplicables a las situaciones adversas.

Implementación de la continuidad de seguridad de la información
La organización debería establecer, documentar, implementar y mantener los procesos, procedimientos y controles para garantizar el nivel necesario de continuidad de seguridad de la información durante una situación adversa. nveniencia, adecuación y eficacia del sistema de gestión de seguridad de la información.

Una organización debería asegurarse de que:

a) se establezca una adecuada estructura de gestión para estar preparados para, mitigar y responder a un evento disruptivo utilizando personal con la autoridad, experiencia y competencia necesarias;

b) se designe personal de respuesta a incidentes con la responsabilidad, autoridad y competencia necesarias para gestionar un incidente y mantener la seguridad de la información;

c) se desarrollen y aprueben los planes documentados, los procedimientos de respuesta y recuperación, detallando cómo la organización va a gestionar un evento disruptivo y mantener su seguridad de la información en un nivel predeterminado, basado en los objetivos de continuidad de seguridad de la información aprobados por la gestión.

De acuerdo con los requisitos de continuidad de la seguridad de la información, la organización debería establecer, documentar, implementar y mantener:

a) los controles de seguridad de la información dentro de los procesos, procedimientos y sistemas de apoyo y herramientas de continuidad del negocio o de recuperación ante desastres;

b) los procesos, procedimientos y cambios de implementación para mantener los controles de seguridad de la información existentes duante una situación adversa;

c) los controles compensatorios para los controles de seguridad de la información que no pueden ser mantenidos durante una situación adversa.

Verificar, revisar y evaluar la continuidad de la seguridad de la información
La organización debería verificar a intervalos regulares los controles de continuidad de la información establecidos e implementados a fin de asegurarse de que sean válidos y efectivos durante situaciones adversas.

Los cambios organizacionales, técnicos, de procedimiento y de proceso, ya sea en un contexto operacional o de continuidad, pueden conducir a cambios en los requisitos de continuidad de seguridad de la información. En tales casos, la continuidad de los procesos, procedimientos y controles para la seguridad de la información deberían revisarse frente a estos requisitos cambiados.

Las organizaciones deberían verificar su gestión de la continuidad de la seguridad de la información:

a) haciendo uso y probando la funcionalidad de los procesos, procedimientos y controles de continuidad de la seguridad de la información para asegurarse de que sean coherentes con los objetivos de continuidad de seguridad de la información;

b) haciendo uso y probando el conocimiento y la rutina para operar los procesos, procedimientos y controles de continuidad de la seguridad de la información para asegurarse de que su desempeño sea coherente con los objetivos de continuidad de seguridad de la información;

c) revisando la validez y eficacia de las medidas de continuidad de la seguridad de la información cuando los sistemas de información, los procesos, procedimientos y controles de seguridad de la información o los procesos de gestión de continuidad del negocio/gestión de recuperación ante desastres y las soluciones cambian.

Redundancias
Tiene como objetivo el asegurar la disponibilidad de los recursos de procesamiento de información

Disponibilidad de recursos de procesamiento de información
Los recursos de procesamiento de la información deberían ser implementados con redundancia suficiente para cumplir los requisitos de disponibilidad.

Las organizaciones deberían identificar los requisitos del negocio para la disponibilidad de los sistemas de información. Cuando la disponibilidad no puede ser garantizada mediante la arquitectura de sistemas existente, deberían considerarse componentes o las arquitecturas redundantes.

Cuando corresponda, los sistemas de información redundantes deberían probarse para asegurarse de que el cambio, en caso de falla, de un componente a otro funcione según lo previsto.