Facultad de Ingeniería y Arquitectura
Departamento de Electrónica e Informática

Examen final de Administración de Riesgos Informáticos.
Ciclo 01-2024

Nombre: Andrés Josué Mendoza Alvarado

Fecha: 5 de julio de 2024 Carné: 00305422

1. Proponga una solución a la siguiente pregunta. Puede incluir un diagrama conceptual en el desarrollo de su respuesta:

¿Qué elementos, subprocesos, eventos y perfiles identifica como comunes o dependientes en la implementación de los tres grandes procesos: gestión de continuidad del negocio, la gestión de riesgos y la gestión de seguridad informática?, es decir, ¿estos tres grandes procesos convergen en algún punto, uno necesita del otro para su implementación, comparten algún objetivo, o bien su relación e implementación es totalmente excluyente uno del otro?

La interrelación entre la Gestión de Continuidad del Negocio, la Gestión de Riesgos y la Gestión de Seguridad Informática es fundamental para garantizar la resiliencia y seguridad de una organización. Estos tres procesos no solo comparten objetivos comunes, sino que también dependen y se complementan mutuamente a través de subprocesos y eventos comunes. A continuación, se detallan las dependencias y convergencias específicas que ilustran cómo estos procesos se entrelazan para crear un marco integral de gestión empresarial.

Dependencias y Convergencias

Compartición de Objetivos:
- Protegen la disponibilidad e integridad de procesos e información crítica.
- Dependen de la identificación y mitigación de riesgos para evitar interrupciones.
- La seguridad informática es esencial para mitigar riesgos relacionados con la información.

Perfiles que Participan en los Procesos

- **Gerente de Continuidad del Negocio**: Desarrolla y mantiene planes de continuidad del negocio, realizando análisis de impacto y pruebas de recuperación, y participa en la identificación y mitigación de riesgos.
- **Responsable de Seguridad de la Información**: Implementa políticas y procedimientos de seguridad, protege la información crítica, gestiona incidentes de seguridad, y colabora en la identificación y mitigación de riesgos.
- **Gerente de Riesgos**: Identifica, evalúa y clasifica los riesgos, implementa acciones de mitigación, y verifica la reducción de los riesgos, participando en todos los procesos: Gestión de Continuidad del Negocio, Gestión de Riesgos y Gestión de Seguridad Informática.

Subprocesos Comunes:

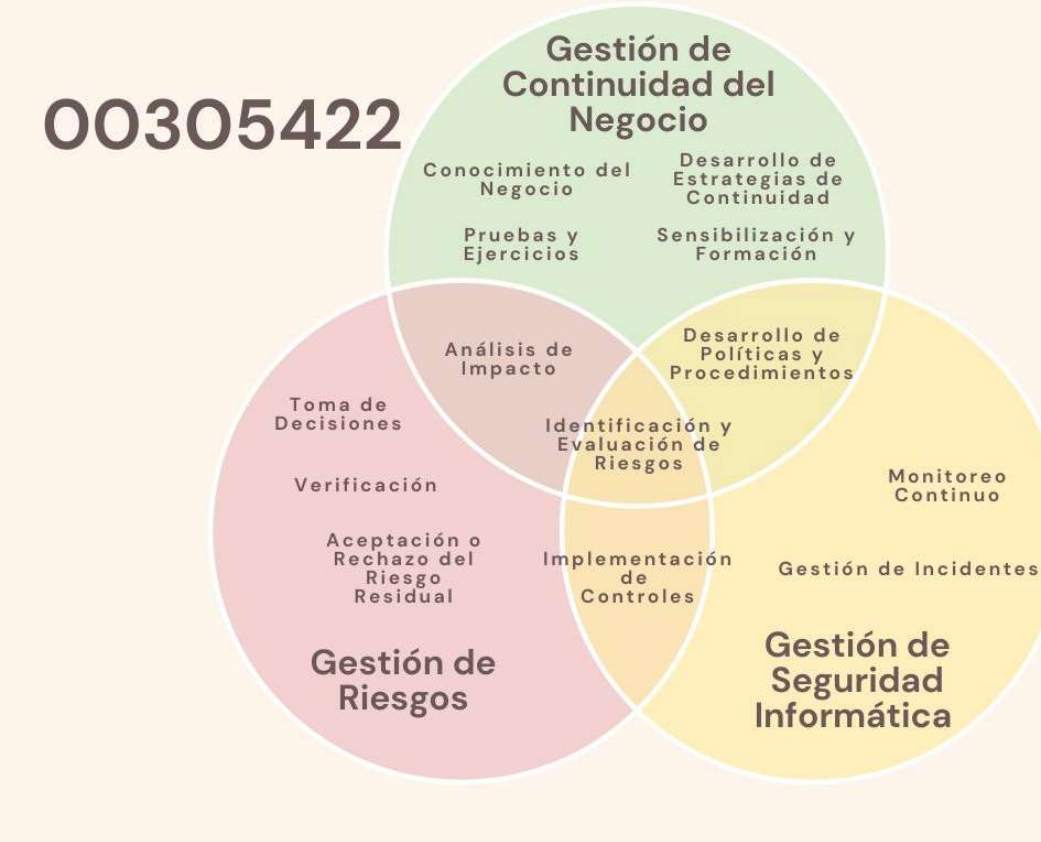
- **Evaluación de Riesgos**: Crucial en los tres procesos.

- **Desarrollo de Políticas y Procedimientos**: Necesario para la Gestión de Continuidad del Negocio y la Gestión de Seguridad Informática.
- **Implementación de Controles**: Fundamental en la Gestión de Riesgos y la Gestión de Seguridad Informática.
- **Análisis de Impacto**: Común en Gestión de Continuidad del Negocio y Gestión de Riesgos.

Eventos Comunes:

- **Incidentes de Seguridad**: Impactan en todos los procesos.
- **Desastres Naturales**: Requieren evaluación de riesgos y medidas de seguridad.

Diagrama de Venn Ilustrando los subprocesos comunes de los tres procesos:



2. **¿Cuál es la diferencia entre evaluar-analizar riesgos y gestionar riesgos? Desarrolle su respuesta.**

Evaluar y analizar riesgos implica identificar y comprender los riesgos potenciales que pueden afectar a una organización, cuantificando su probabilidad e impacto. Este proceso resulta en una lista de riesgos clasificados y priorizados, proporcionando una base sólida para la toma de decisiones. Por otro lado, gestionar riesgos se refiere a desarrollar e implementar estrategias para mitigar, transferir, aceptar o eliminar estos riesgos identificados. Aunque ambos procesos están intrínsecamente conectados y se complementan, la principal diferencia radica en su enfoque: evaluar y analizar se centra en la identificación y entendimiento, mientras que gestionar se enfoca en la acción y control de los riesgos. Ambos comparten el objetivo común de minimizar el impacto negativo de los riesgos en la organización, pero lo hacen en etapas diferentes del proceso de gestión de riesgos.