GOBERNANZA

- **1. Strategy**
  - La estrategia define la visión y los objetivos a largo plazo del programa de ciberseguridad. Implica el desarrollo de planes que alineen las iniciativas de seguridad con la misión de la organización.
- **2. Business Alignment**
  - Esta sección asegura que las políticas y procesos de seguridad estén en sintonía con las metas del negocio. Se trata de integrar la seguridad en la toma de decisiones empresariales para maximizar el valor.
- **3. Risk Management**
  - Un enfoque sistemático para identificar, evaluar y mitigar los riesgos de seguridad. Esto incluye la implementación de prácticas que minimicen el impacto de las amenazas y vulnerabilidades.:
- **4. Program Frameworks**
  - Los marcos de programas proporcionan estructuras para la gestión de la ciberseguridad:
    - NIST CSF: Marco del NIST para la gestión de la ciberseguridad, enfocado en la identificación, protección, detección, respuesta y recuperación..
    - ISO 27000: Normativa internacional que detalla los requisitos para un sistema de gestión de seguridad de la información.
- **5. Control Frameworks**
  - Los marcos de control son guías que ayudan a las organizaciones a implementar controles de seguridad efectivos:
    - NIST 800-53: Conjunto de controles de seguridad para sistemas de información federales..
    - CIS Controls: Conjunto de mejores prácticas para la defensa cibernética.
- **6. Program Structure**
  - Define cómo se organizarán y gestionarán los programas de ciberseguridad dentro de la organización.
- **7. Roles and Responsibilities**
  - Establece las funciones y responsabilidades de cada miembro del equipo de seguridad, asegurando que todos comprendan su papel en la gestión de riesgos.
- **8. Workforce Planning**
  - Se refiere a la planificación de recursos humanos necesarios para implementar y mantener los programas de ciberseguridad de manera efectiva.
- **9. Resource Management**
  - Gestión eficiente de los recursos tecnológicos y humanos necesarios para la ciberseguridad.
- **10. Data Classification**
  - Proceso de categorizar datos según su sensibilidad y el impacto que tendría su exposición.
- **11. Security Policy**
  - Conjunto de directrices que establecen cómo se debe manejar y proteger la información sensible.
- **12. Creating a Security Culture**
  - Fomentar una cultura organizacional que priorice la seguridad en todos los niveles, involucrando a todos los empleados.
- **13. Security Training**
  - Awareness Training: Capacitación general sobre seguridad para todos los empleados.
  - Role-Based Training: Capacitación especializada basada en el rol del empleado dentro de la organización.
- **14. Metrics and Reporting**
  - Establecimiento de métricas para evaluar la eficacia del programa de ciberseguridad y generar reportes que informen a la alta dirección
- **15. Program Management**
  - Gestión general del programa de ciberseguridad, asegurando que se cumplan los objetivos y se ajusten las estrategias según sea necesario.
- **16. IT Portfolio Management**
  - Gestión de todos los activos tecnológicos en términos de su seguridad y alineación con la estrategia de ciberseguridad.
- **17. Communications Plan**
  - Estrategias para comunicar la importancia de la seguridad y mantener informados a los interesados.
- **18. Change Management**
  - Proceso para gestionar cambios en la infraestructura de TI de manera segura, minimizando riesgos.
- **19. Board Communications**
  - Establecimiento de un canal de comunicación claro entre el equipo de seguridad y la junta directiva, asegurando que los temas de ciberseguridad sean tratados a nivel ejecutivo. Esta estructura de gobernanza es esencial para construir una base sólida en la gestión de la ciberseguridad, permitiendo a las organizaciones protegerse contra amenazas y cumplir con las regulaciones aplicables.

fundamental para establecer un marco de seguridad que garantice la alineación con los objetivos del negocio y la gestión de riesgos

Presented with xmind AI