TECNICATURA UNIVERSITARIA EN CIBERSEGURIDAD

AUDITORÍAS DE SEGURIDAD DE LA INFORMACIÓN

Unidad II – Trabajo práctico N°1

Profesor: Marcelo Daniel Rossetti

Alumno: Balbuena Atar Dante Gabriel

Tucumán, Tafí Viejo – octubre 2024

Contenido

1. Introducción

La creciente preocupación por los ciberataques y los rescates exigidos a las empresas ha llevado a un aumento en la demanda de una sólida estrategia de seguridad de la información. Como Técnico en Seguridad de la Información, propongo llevar a cabo una auditoría integral de seguridad para evaluar y mejorar la postura de seguridad de la empresa RMD. Esta auditoría se basará en buenas prácticas reconocidas y marcos normativos, como la ISO 27002.

La empresa RMD de logística internacional con sede central en CABA (Ciudad Autónoma de Buenos Aires, Argentina) y sucursales en Asunción (Paraguay), Rosario (Santa Fe Argentina), Salta (Salta, Argentina) y Santa Rosa (La Pampa, Argentina).
La empresa cuenta con una plantilla de 100 empleados.
Caso II-1-1:
Un titular de la Empresa RMD está preocupado por el estado de su organización en función de los relatos de Ciberataques y pedidos de rescate que sufren empresas en las ciudades donde operan. Estos relatos llegan por medios de comunicación locales y/o referencias de empresarios cercanos.
Cuáles serían sus primeros tres (3) pasos al ser consultado como T.U.C.?
Indique el objetivo de cada paso.
Realice una descripción de cada paso a seguir.

2. Desarrollo

Propuesta de Auditoría de Seguridad de la Información

Fecha: 03/10/2024

De: Balbuena Atar Dante Gabriel
Cargo: Técnico en Seguridad de la Información
Para: [Nombre del Titular]
Cargo: [Cargo del Titular]
Empresa: RMD de Logística Internacional
Sede Central: CABA, Argentina

Objetivos de la Auditoría

1. Identificar Vulnerabilidades: Detectar debilidades en la seguridad de la información que puedan ser explotadas por atacantes.
2. Evaluar la Conformidad Normativa: Comparar las prácticas actuales de seguridad de la información de RMD con los estándares internacionales aplicables.
3. Definir un Plan de Acción: Proporcionar recomendaciones concretas para mitigar riesgos y mejorar la seguridad de la información.

Pasos a Seguir

Paso 1: Realizar una Entrevista Inicial

- Objetivo: Identificar las preocupaciones específicas del empresario sobre la seguridad de la información y comprender el contexto operativo de RMD.
- Descripción:
    - Preparar un conjunto de preguntas para la entrevista.
    - Realizar la entrevista, documentando las inquietudes y preocupaciones del titular.
    - Ejemplos de preguntas a realizar:
        - ¿Qué medidas de seguridad se están utilizando actualmente?
        - ¿Han sufrido incidentes de seguridad previos?
        - ¿Qué activos considera más críticos?
        - ¿tiene clientes de otros países?
        - ¿Qué medidas de seguridad se viene aplicando?

Paso 2: Evaluar el Marco Normativo y de Buenas Prácticas

- Objetivo: Identificar marcos normativos aplicables y evaluar el estado actual de la empresa respecto a las buenas prácticas de seguridad de la información.
- Descripción:
    - Investigar las normativas y estándares relevantes, como la ISO 27002.

- Establecer una lista de controles sugeridos por estos marcos.
- Evaluar las prácticas actuales de RMD y su alineación con las mejores prácticas del sector.

Paso 3: Realizar una Evaluación de Riesgos Preliminar

- Objetivo: Identificar y priorizar los riesgos asociados a la seguridad de la información en RMD.
- Descripción:
  - Identificar los activos críticos de información.
  - Evaluar las posibles vulnerabilidades en la infraestructura actual.
  - Clasificar los riesgos identificados en función de su probabilidad e impacto.

3.Conclusiones y siguientes pasos

La auditoría de seguridad de la información proporcionará una visión clara de la postura de seguridad de RMD, permitiendo identificar áreas de mejora y desarrollar un plan de acción para mitigar riesgos. Después de completar los pasos iniciales, se presentará una propuesta formal que incluirá recomendaciones específicas y un plan para la implementación de mejoras.

Agradecimiento

Agradezco la oportunidad de colaborar con RMD y espero poder contribuir a fortalecer la seguridad de la información en su organización.

Atentamente,

---
cel:
Mail:
firma y aclaración:

4. Referencias

National Institute of Standards and Technology. (2020). Controles de seguridad y privacidad para sistemas y organizaciones federales de información (SP 800-53, Rev. 5). https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
European Union Agency for Cybersecurity. (s.f.). Publicaciones de ENISA. https://www.enisa.europa.eu/publications
INCIBE. (s.f.). Auditoría de sistemas. https://virtual.ugr.edu.ar/pluginfile.php/466644/mod_resource/content/1/auditoria-sistemas-INCIBE.pdf
National Institute of Standards and Technology. (s.f.). Marco para mejorar la ciberseguridad de infraestructuras críticas. https://www.nist.gov/cyberframework
Este documento sigue las normas de citación y referencias de la *Publication Manual of the American Psychological Association* (7ª ed.).