TECNICATURA UNIVERSITARIA EN CIBERSEGURIDAD

AUDITORÍAS DE SEGURIDAD DE LA INFORMACIÓN

Trabajo practico N° 2: Propuesta de auditoría Externa para la Empresa “RMD”

Profesor: Marcelo Daniel Rossetti

Alumno: Balbuena Atar Dante Gabriel

Tucumán, Tafí Viejo – octubre 2024

Índice

1. Introducción y Contacto Inicial ..... pág. 3
2. Descripción del Servicio de Auditoría ..... pág. 3
    - Fase 1: Evaluación de Políticas y Documentación de Seguridad
    - Fase 2: Inspección de Prácticas Operativas y Evaluación en Campo
3. Determinación de Necesidades y Alcance ..... pág. 3
    - Áreas de Enfoque
4. Estimación de Duración y Costos ..... pág. 3
    - Duración
    - Costo Total
5. Asignación de Recursos del Equipo de Auditoría ..... pág. 4
    - Roles y Responsabilidades
6. Ejecución de Actividades y Cronograma ..... pág. 4
    - Actividades Diarias y Objetivos
7. Informe Final ..... pág. 5
    - Informe Ejecutivo
    - Informe Técnico
    - Matriz de Riesgos
8. Consideraciones Finales ..... pág. 5
9. Referencias ..... pág. 6

1. Introducción y Contacto Inicial

- Un representante del área comercial se contactará con el cliente para comprender sus necesidades y expectativas en profundidad. A partir de esta comunicación preliminar, se definirá un plan de auditoría externa personalizado que responda a los requerimientos específicos del cliente.
- Tras la aceptación de la propuesta inicial, el equipo de auditores coordinará una agenda con el cliente para iniciar el servicio. La auditoría comenzará con una entrevista preliminar con el representante designado de RMD, lo que permitirá identificar con claridad los objetivos, el contexto y la situación actual en cuanto a la seguridad de la información de la empresa.

2. Descripción del Servicio de Auditoría

- En base a las necesidades de RMD, proponemos un servicio integral de auditoría externa, estructurado en dos fases clave:

Fase	Descripción
Fase 1 - Evaluación de Políticas y Documentación de Seguridad	Análisis exhaustivo de documentos y políticas, incluyendo políticas de acceso, gestión de redes y protocolos de respuesta ante incidentes.
Fase 2 - Inspección de Prácticas Operativas y Evaluación en Campo	Revisión de prácticas operativas de seguridad, con enfoque en sistemas críticos y cumplimiento de controles según ISO 27002 y políticas internas.

3. Determinación de Necesidades y Alcance

- En el primer encuentro, se realizará una entrevista con el referente designado en RMD para obtener una comprensión precisa de sus metas y necesidades. Esta reunión permitirá adaptar el alcance de la auditoría, asegurando que se cubran las áreas prioritarias para la organización.
- **Áreas de Enfoque**: Durante la auditoría, se analizarán los sistemas críticos de gestión, las prácticas de seguridad operativas y las herramientas de comunicación, como correo electrónico y Telegram.

4. Estimación de Duración y Costos

- Para garantizar un proceso detallado y eficiente, la auditoría está planificada para realizarse en una semana de cinco días:

Fase del servicio	Duración	Costo Estimado (USD)
Fase 1 - Evaluación Documental	2 días (14 horas)	$6,000
Fase 2 - Evaluación de Prácticas	3 días (21 horas)	$8,500
Total	5 días / 35 horas	$14,500

5. Asignación de Recursos del Equipo de Auditoría

- Basándonos en los requerimientos de RMD, el equipo estará compuesto por:

Rol	Experiencia	Certificaciones	Habilidades Clave	Responsabilidades
Auditor Principal	12 años	ISO 27001 Auditor Líder, CISSP	Liderazgo, Análisis de Riesgos, Evaluación de Controles	Dirigir el proceso de auditoría y garantizar cumplimiento de estándares
Especialista Técnico Sr	5 años	Microsoft Certified: Azure Security, CompTIA Security+	Seguridad en Nube, Evaluación de Red, Soporte Técnico Avanzado	Soporte técnico avanzado y evaluación de prácticas operativas
Asistente de Auditoria	4 años	Especialización en Gestión de Riesgos	Recopilación de Datos, Análisis de Vulnerabilidades, Documentación de Hallazgos	Relevamiento de datos y verificación de seguridad

6. Ejecución de Actividades y Cronograma

- Las actividades se llevarán a cabo de acuerdo con un cronograma organizado que asegure una cobertura completa de todas las áreas clave:

Actividad	Objetivo principal	Dia estimado
Reunión de apertura	Introducción del equipo, revisión de objetivos y cronograma	Día 1 (mañana)
Entrevista preliminar de requisitos	Entender en profundidad las metas y preocupaciones de RMD	Día 1 (tarde)
Validación de documentación previa	Revisión inicial de políticas y procedimientos	Día 2 (mañana)
Evaluación documental completa	Análisis detallado de seguridad de documentos	Día 2 (tarde)
Inspección de procesos operativos	Verificación de prácticas diarias en seguridad	Día 3 (mañana)
Recolección de evidencias	Identificación de áreas de mejora y recopilación de pruebas	Día 3 (tarde)
Evaluación de cumplimiento con ISO 27002	Contraste de prácticas actuales con controles de ISO 27002	Día 4

Sesión de Retroalimentación Intermedia	Presentación de hallazgos preliminares	Día 5 (mañana)
Reunión de Cierre	Explicación detallada de hallazgos y recomendaciones	Día 5 (tarde)
Elaboración del informe final	Documentación de hallazgos, vulnerabilidades, fortalezas y plan de acción	Tras la auditoría

7. Informe Final

- **Informe Ejecutivo**: Resumen dirigido a la gerencia con los puntos clave, conclusiones y áreas críticas de mejora por ejemplo las no conformidades.
- **Informe Técnico**: Detalle técnico de vulnerabilidades, fortalezas y recomendaciones prácticas para mitigar riesgos, incluyendo una **Matriz de Riesgos** para priorizar los hallazgos de acuerdo a probabilidad e impacto. Se respaldará cada vulnerabilidad con evidencia específica y referencia normativa.

  Ejemplo de matriz de riesgo:

Vulnerabilidad Detectada	Probabilidad	Impacto	Prioridad
Ausencia de políticas de seguridad	Alta	Alto	Prioridad Alta
Configuración insegura en VPN	Media	Alto	Prioridad Media
Uso de herramientas de comunicación sin cifrado	Alta	Medio	Prioridad Media
Falta de monitoreo de accesos	Baja	Alto	Prioridad Baja

Consideraciones Finales

Esta propuesta de auditoría se ajusta a las características y necesidades específicas de la empresa RMD, ofreciendo un análisis exhaustivo y un plan de auditoría estructurado. Al finalizar el proceso, el equipo proporcionará recomendaciones prácticas y un Plan de Implementación de Medidas Correctivas para los próximos seis meses. Estas recomendaciones están diseñadas no solo para mitigar riesgos inmediatos, sino también para fortalecer a largo plazo la postura de seguridad de RMD en un entorno de amenazas creciente.
Implementar estas medidas ayudará a:

- **Aumentar la Resiliencia Operativa** frente a ciberataques.
- **Mejorar la Conformidad Regulatoria** con normativas internacionales como ISO 27001.
- **Optimizar el Control y Monitoreo de Accesos** para reducir vulnerabilidades.

Este enfoque integral permitirá a RMD desarrollar una cultura de seguridad sostenida y

escalable.

Referencias

International Organization for Standardization. (2013). *ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems - Requirements.* ISO.

Universidad del Gran Rosario. (2024). *Material UIII* [Archivo PDF]. UGRvirtual.

Rossetti, M. D. (2024). *Encuentro Auditorías UIII, 10/10/24 18hs* [Video]. UGR (Universidad del Gran Rosario). https://us02web.zoom.us/rec/play/tB_FmSZ0XCHYae9yCtegZA0hiY1Bn8Zb3V7SFRXfaCjB4ZZgNSrGzu_Xwx51qHcY_h20x0ovJ4-8-5z3.OxF42sUxVFrzTlSl?canPlayFromShare=true&from=share_recording_detail&continueMode=true&componentName=rec-play&originRequestUrl=https%3A%2F%2Fus02web.zoom.us%2Frec%2Fshare%2FMap3AhAKR7-NiRDKc2TsIqjOjIIuwIIUe4ti5uSyaVI83JjxeIVkRge3WN3fmd15.dgjki2CtLUaJ2khk

Este documento sigue las normas de citación y referencias de la *Publication Manual of the American Psychological Association* (7ª ed.).