



AUDITORIA DE SISTEMAS INFORMÁTICOS

PLAN DE TRABAJO PARA UNA AUDITORÍA EN LA EMPRESA WIN

Docente: Ing. Miguel Ángel Del Pozo Mata

Lima, 2024

Plan de Auditoría para Win

1. Introducción a la Planificación de Auditoría

La planificación de la auditoría es una etapa esencial para evaluar y mejorar los sistemas y procesos de la empresa. Este plan detalla los pasos para auditar el **Sistema de Gestión de Seguridad de la Información (SGSI)** de Win.

1.1. Responsables

- Líder de Auditoría: Pachas Johan
- Especialista de TI: Sebastian Yauri
- Auditoría de Cumplimiento y Normativa: John Doe

1.2. Documentos Base

- Políticas y procedimientos internos de Win.
- Constitución Política del Perú.
- Legislación y regulaciones locales aplicables.
- Informes de auditorías previas.
- Manual del SGSI de Win.
- Políticas de Seguridad de la Información.
- Plan de Continuidad del Negocio.
- Registros de incidentes de seguridad y gestión de accesos.

2. Componentes del Plan

2.1. Objetivos de la Auditoría, Unidades y Procesos a Auditar

- Objetivos:
 - Evaluar la seguridad física y lógica de los puntos de acceso y centro de datos.
 - Asegurar el cumplimiento de las políticas internas y regulaciones externas.
 - Evaluar la alineación de las políticas internas con los objetivos estratégicos de la organización.
 - Examinar los procedimientos para la gestión de accesos y credenciales.
 - Asegurar la integridad y disponibilidad de las aplicaciones críticas para la operación.
- Alcances de las unidades y Procesos a Auditar

La empresa Auditorías PTJYSS, se encargará de realizar una auditoría a la empresa Win Internet Perú, de la fecha del 30 de noviembre del 2024 al 21 de diciembre del 2024, con la finalidad de evaluar una parte fundamental de la empresa, la cual será la gestión y funcionamiento de sus aplicaciones críticas, asegurando que cumplan con los estándares de calidad, seguridad y eficiencia requeridos.

La auditoría cubrirá una evaluación integral de los sistemas de información, centrada en la infraestructura que soporta las aplicaciones, el control de accesos y la gestión de usuarios. Se analizarán las medidas de seguridad lógica implementadas para proteger las aplicaciones y los procedimientos de backup y recuperación ante desastres asociados a estas plataformas.

Además, se revisarán en detalle los procesos relacionados con la operación y mantenimiento de las aplicaciones críticas, incluyendo el análisis de logs, la gestión de incidentes y las pruebas de vulnerabilidades. Se auditarán las principales instalaciones tecnológicas de Win Internet Perú, garantizando que los sistemas asociados a las aplicaciones críticas estén alineados con las mejores prácticas y normativas vigentes.

2.2. Composición del Grupo Auditor

Johan Pachas - Líder de Auditoría

Johan cuenta con experiencia obtenida de una participación constante en proyectos de auditoría así como certificaciones en CISA, ISO 27001 Lead Auditor y PMP, comprendiendo las diversas políticas de seguridad, gestión de riesgos y aseguramiento de calidad en aplicaciones. Sus funciones son planificación y supervisión de auditorías, evaluación de controles y presentación de resultados detallados a la alta dirección de Win Internet Perú. Asimismo, es responsable de garantizar la precisión, eficacia y continuidad de los procesos de auditoría, supervisar la implementación de las recomendaciones, validar la documentación generada, y realizar un seguimiento exhaustivo de las acciones correctivas propuestas.

Sebastian Yauri - Especialista de TI

Sebastian cuenta con certificaciones **CompTIA Network+ y Microsoft Certified: Azure Solutions Architect Expert**, y tiene una sólida experiencia en la administración de redes, configuración de sistemas y soporte técnico avanzado. Sus funciones incluyen la evaluación técnica de infraestructuras de TI, diagnóstico de problemas en sistemas y redes, y supervisión de la implementación de soluciones tecnológicas.

Sus principales responsabilidades son garantizar la continuidad operativa de los sistemas auditados, documentar configuraciones clave, identificar áreas de mejora en la infraestructura tecnológica y colaborar en la implementación de recomendaciones técnicas.

John Doe - Auditor de Cumplimiento y Normativa

Mariana posee certificaciones **ISO 27001 Lead Implementer y CISA**, con amplia experiencia en auditorías de cumplimiento regulatorio y evaluación de políticas corporativas. Sus funciones incluyen analizar normativas legales y regulatorias aplicables, revisar las políticas internas de la organización y realizar auditorías documentales para verificar la conformidad con estándares internacionales de seguridad.

Sus responsabilidades principales son identificar desviaciones respecto a las normativas, preparar informes detallados de cumplimiento, asesorar en la implementación de mejoras y asegurar que los procesos internos estén alineados con las mejores prácticas y las exigencias legales vigentes.

2.3. Recursos a solicitar

Categoría	Equipo	Modelo	Aplicación
Computadora personal	Laptop	Dell XPS 15 (12ª Gen Intel Core i7)	Ejecutar herramientas de análisis de aplicaciones y generación de informes.
Recopilación de Datos	Unidad Flash USB	Kingston DataTraveler 100 G3 (64GB)	Almacenar registros, logs y resultados de auditoría.
Recopilación de Datos	Smartphone	Samsung Galaxy S23	Captura de evidencia visual, grabaciones y acceso remoto a aplicaciones.
Recopilación de Datos	Cuaderno	Cuaderno A4	Registrar observaciones, hallazgos y notas de entrevistas.
Software Especializado	Licencia de herramientas	Burp Suite Professional, OWASP ZAP	Análisis de vulnerabilidades y pruebas de seguridad en aplicaciones.
Lugar de Trabajo	Sala de reuniones	-	Realizar análisis, reuniones y entrevistas con el equipo auditado.
Conexión a Internet	Router	TP-Link Archer AX73	Garantizar conectividad segura durante las pruebas en aplicaciones en la nube.
Alimentación	-	-	Proveer al equipo durante sesiones extendidas de auditoría.

2.3. Programación

Fechas: Del 30 de noviembre del 2024 al 21 de diciembre del 2024.

Horarios: De 9:00 AM a 5:00 PM

Duración: 3 semanas

Métodos de Auditoría: Entrevistas, revisión documental, pruebas de control, observación directa

Fecha	Día	Hora	Actividad	Responsables
30 de noviembre	Sábado	10:00 - 13:00	Reunión de apertura y planificación inicial	Johan Pachas, Sebastian Yauri, John Doe
1 de diciembre	Domingo	12:00 - 15:00	Revisión de políticas de seguridad de la información	Sebastian Yauri, John Doe
2 de diciembre	Lunes	09:00 - 12:00	Evaluación de riesgos asociados a las aplicaciones	Johan Pachas, John Doe
3 de diciembre	Martes	10:00 – 13:00	Análisis de arquitectura de aplicaciones críticas	Sebastian Yauri
6 de diciembre	Viernes	09:00 - 12:00	Evaluación de la gestión de vulnerabilidades en aplicaciones	Sebastian Yauri
7 de diciembre	Sábado	14:00 – 16:00	Análisis de configuración y seguridad de la base de datos	Johan Pachas
8 de diciembre	Domingo	09:00 – 11:00	Revisión de procedimientos de respaldo y recuperación	John Doe
9 de diciembre	Lunes	10:00 – 12:00	Auditoría de medidas de seguridad de las aplicaciones	Johan Pachas, Sebastian Yauri
12 de diciembre	Jueves	09:00 - 12:00	Revisión de logs de seguridad y monitoreo de aplicaciones	Sebastian Yauri
13 de diciembre	Viernes	14:00 – 17:00	Pruebas de penetración en aplicaciones críticas	Sebastian Yauri
14 de diciembre	Sábado	09:00 - 12:00	Revisión de gestión de accesos a aplicaciones críticas	John Doe
15 de diciembre	Domingo	09:00 – 12:00	Inspección de infraestructuras tecnológicas y redes de aplicaciones	Johan Pachas
16 de diciembre	Lunes	10:00 –	Verificación de	John Doe

		12:00	cumplimiento de normativas de seguridad	
19 de diciembre	Jueves	09:00 – 11:00	Análisis de incidentes de seguridad relacionados con aplicaciones	Sebastian Yauri
20 de diciembre	Viernes	10:00 – 12:00	Preparación de informes preliminares de hallazgos	Johan Pachas, John Doe
21 de diciembre	Sábado	09:00 – 11:00	Reunión de cierre y presentación de resultados finales	Johan Pachas, Sebastian Yauri, John Doe

3. Adaptación a Imprevistos para Auditoría de Aplicaciones

- Las evaluaciones programadas de la arquitectura y seguridad de las aplicaciones podrían reprogramarse si surgen problemas técnicos o interrupciones en los sistemas. Esto incluiría una nueva planificación de pruebas de penetración o análisis de vulnerabilidades para asegurar que no se afecten las operaciones de las aplicaciones críticas.
- En caso de identificar áreas adicionales de riesgo, como vulnerabilidades no anticipadas en las aplicaciones o infraestructuras de TI, el alcance de la auditoría se ampliará para incluir estas nuevas áreas. Esto podría implicar la revisión de sistemas adicionales, la inclusión de nuevas pruebas de seguridad o el análisis de aplicaciones no consideradas inicialmente.
- Dependiendo de los resultados preliminares obtenidos durante las primeras fases de la auditoría, se podrán ajustar las metodologías de análisis. Por ejemplo, si se identifican debilidades significativas en las configuraciones de seguridad de las aplicaciones, se podrán implementar enfoques adicionales como el análisis de código fuente o pruebas más profundas en las interfaces de usuario.
- Mantendremos una comunicación constante con todas las partes interesadas, incluyendo la alta dirección y los equipos de desarrollo de aplicaciones. Esto garantizará que cualquier cambio en la planificación o el alcance se comunique de manera efectiva y oportuna.
- El plan de auditoría se ajustará de forma continua según se presenten desafíos imprevistos o cambios en el entorno de las aplicaciones auditadas. Las estrategias de auditoría se actualizarán para abordar cualquier nueva amenaza identificada y para asegurar que todas las áreas críticas sean evaluadas de manera exhaustiva.

4. Fase 1

4.1. Análisis del Contexto Organizacional para el SGSI

- Evaluar los principios fundamentales de Win Internet Perú, como su misión, visión y metas estratégicas, para validar que el SGSI esté alineado con los objetivos de la empresa.
- Identificar a los grupos de interesados y realizar entrevistas estructuradas , tales como líderes de la empresa, personal de alto cargo, clientes y socios comerciales.
- Utilizar un modelo de madurez para diagnosticar el estado actual de la seguridad de la información en la empresa y como los empleados son conscientes de ello.
- Recopilar y revisar documentos relevantes, como políticas internas, reportes operativos y estudios del sector, con el único objetivo de conocer el contexto actual de Win Internet Perú.
- Investigar factores internos y externos que puedan influir en la seguridad de la información, como cambios tecnológicos, normativas legales o tendencias del mercado.
- Realizar un análisis integral del contexto actual de la empresa usando marcos como PESTEL, con el principal objetivo de prever oportunidades y amenazas que puedan impactar el SGSI.

4.2. Compromiso de la Alta Dirección

- Analizar los mensajes y acciones de los líderes de Win Internet Peru, como comunicados oficiales, emails o su participación activa en la planificación de la seguridad, para evidenciar el compromiso al SGSI.
- Establecer indicadores clave (KPIS) para medir a la alta dirección, como recursos asignados o iniciativas lideradas.
- Evaluar el nivel de implicación de la dirección en los procesos de SGSI, así como la asignación de responsabilidades.
- Documentar evidencias del impacto de este compromiso en los trabajadores de Win Internet Peru , como el cumplimiento normativo y la confianza de los clientes.

4.3. Evaluación de la Planificación

- Revisar los documentos relacionados con la planificación del SGSI, asegurándose de que estos establezcan objetivos claros, plazos definidos y responsabilidades específicas.

- Analizar si las estrategias de seguridad contemplan aspectos esenciales, como la protección de datos sensibles y la respuesta ante incidentes de seguridad.
- También considerar ejercicios de simulación y revisar si la eficacia de los planes de acción frente a posibles incidentes de seguridad.
- Examinar la coherencia entre los objetivos del SGSI y los planes estratégicos de la empresa, identificando cualquier desajuste o área que necesite ajustes.
- Evaluar la pertinencia de los indicadores utilizados para medir el éxito de los objetivos del SGSI y proponer métricas más relevantes si es necesario.

4.4. Gestión de Riesgos: Identificación, Análisis, Evaluación y Tratamiento

- Comprobar la existencia y el uso de un sistema documentado que identifique los activos críticos, posibles amenazas y las vulnerabilidades relacionadas a la empresa Win Internet Perú.
- Incorporar software especializado para identificar y monitorear riesgos de forma más eficiente y en tiempo real usando los datos de la empresa Win Internet Perú.
- Analizar la metodología empleada para evaluar riesgos, y validar que esta sea acorde a los estándares reconocidos o normas propuestas y sea adecuada para la operación de la empresa.
- Revisar la frecuencia con la que se actualizan los riesgos identificados, especialmente en respuesta a cambios internos o externos en el entorno de la organización.
- Examinar la efectividad de las estrategias o propuestas implementadas para mitigar los riesgos o recuperación en caso de que ocurran desastres.

4.5. Implementación y Operación del SGSI

- Corrobora que la documentación previa respalda la implementación del SGSI, usando procedimientos, registros y manuales operativos.
- También proponer la inclusión del personal en revisiones periódicas para identificar problemas prácticos y soluciones efectivas ante posibles amenazas.
- Verificar posibles observaciones previas de los trabajadores y entrevistas con los empleados para confirmar que los procesos definidos en el SGSI se están llevando a cabo correctamente.
- Sugerir los programas de formación y sensibilización para garantizar que todo el personal de Win Internet Perú sea consciente sobre el tema y su importancia.

- Concluir con la verificación de puntos débiles que serán utilizadas para mejorar el desempeño a futuro.

4.6. Mantenimiento y Mejora Continua del SGSI

- Analizar las acciones correctivas y preventivas implementadas en el SGSI, asegurándose de que éstas resuelvan efectivamente las no conformidades detectadas.
- Crear un espacio o reuniones para que los empleados sugieran ideas innovadoras para mejorar la seguridad de la información y recompensarlos en caso sus ideas aporten progreso a la empres.
- Revisar informes de auditorías internas y externas para identificar patrones que puedan indicar áreas recurrentes de mejora.
- Proponer nuevas herramientas, tecnologías o prácticas para optimizar la capacidad de la organización de mantener y evolucionar su SGSI.

4.7. Auditorías Internas y Supervisión del SGSI

- Examinar los informes de auditorías anteriores, verificando si las recomendaciones emitidas se han implementado de manera efectiva.
- Diseñar un sistema de retroalimentación que permita a los auditores futuros identificar oportunidades de mejora y priorizarlas. De esta manera garantizaremos la mejora continúan en nuestro SGSI.
- Verificar si todo el personal encargado de las auditorías tiene la experiencia y habilidades necesarias para llevar a cabo revisiones.
- Identificar oportunidades para mejorar la calidad y el alcance de las auditorías internas, como la integración de herramientas automatizadas para el seguimiento de indicadores clave.
- Recopilar y documentar hallazgos relevantes .Además, ofrecer sugerencias prácticas para fortalecer la gestión del SGSI y fomentar una cultura de mejora continua.

Fase 2: Verificación e Implementación del SGSI en Win Internet Perú

5.1. Verificar que lo Documentado en la Fase 1 se Realiza Efectivamente

- Implementar auditorías internas entre departamentos con la misma metodología para validar la implementación de políticas.
- Utilizar herramientas tecnológicas que permitan verificar la conformidad de las prácticas diarias con las políticas documentadas.
- Entrevistas Grupales: Realizar focus groups con diferentes niveles de empleados para identificar percepciones y brechas en la implementación.
- Asegurar que los proyectos en curso cumplen con las normativas del SGSI, por ejemplo la expansión de cobertura o implementación de fibra óptica en nuevos distritos.
- Recopilar las observaciones sobre la documentación en la Fase 1.
- Pruebas de Campo: Realizar simulaciones específicas para evaluar la respuesta operativa a escenarios previstos en las políticas.

5.2. Comprobación del Alcance del SGSI

- Validar el alcance del SGSI planteado en la documentación previa.
- Verificar si el SGSI incluye controles para proveedores clave que interactúan con los sistemas de Win Internet Perú.
- Confirmar que los activos críticos de Win Internet Perú sean considerados en el plan.
- Realizar entrevistas con usuarios clave para asegurar que los activos críticos han sido correctamente identificados desde su perspectiva.
- Validar que dispositivos conectados en la red están contemplados en el alcance del SGS
- Añadir los activos que fueron omitidos en el proceso anterior.

5.3. Comprobación de la Política

- Formular entrevistas de forma periódica para la evaluación a los empleados sobre su comprensión del tema de seguridad.
- Estructurar la política actual y validar que se usen referencias a amenazas encontradas, como posibles incidencias.
- Verificar que los nuevos empleados reciben capacitación sobre la política desde su ingreso a la empresa.
- Evaluar si los clientes están informados sobre las políticas de seguridad relevantes para su interacción con la empresa
- Evaluar los usos de los canales de comunicación que usan los empleados.

5.4. Revisión de la Gestión de Activos

- Revisar la gestión de los activos y su listado en todas las etapas de su ciclo de vida, desde la adquisición hasta su disposición final.
- Generar un inventario de toda la infraestructura crítica, como antenas, servidores, routers y cableado.
- Listar los activos críticos están etiquetados de manera visible, tanto física como digitalmente, para facilitar su seguimiento.
- Confirmar que nuevos activos tecnológicos adquiridos recientemente han sido incorporados en el inventario.
- Considerar el uso de herramientas que generen reportes automáticos sobre activos registrados.

5.5. Revisión de la Gestión de los Incidentes de Seguridad de la Información

- Realizar pruebas controladas, como ataques DDoS simulados, para evaluar la respuesta del equipo de seguridad
- Revisar el inventario actual y su organización
- Organizar simulacros para evaluar cómo el personal responde a incidentes simulados en tiempo real.
- Crear documentación acerca de posibles activos no identificados en Win Perú.

5.6. Revisión de la Gestión de la Continuidad del Negocio

- Verificar la existencia y funcionalidad de planes para contingencias específicas, como desastres naturales que afecten la infraestructura
- Verificar que las copias de seguridad se realizan y prueban regularmente.
- Asegurar que el plan de continuidad del negocio se alinea con los objetivos estratégicos y operativos.
- Incorporar escenarios específicos como cortes masivos de internet o ataques dirigidos a infraestructura.

5.7. Revisión del Cumplimiento

- Asegurar que Win Internet Perú cumple con regulaciones nacionales como la Ley de Protección de Datos Personales y normas de OSIPTEL
- Programar auditorías externas periódicas para evaluar el cumplimiento de regulaciones locales e internacionales.
- Verificar que los acuerdos con terceros incluyen cláusulas relacionadas con la seguridad de la información.
- Implementar sesiones de capacitación para personal clave sobre nuevas regulaciones y normativas.
- Crear un sistema de alertas para notificar cambios legales que puedan impactar al SGSI.

5.8. Cierre de la Auditoría del SGSI

- Presentar los hallazgos preliminares a las partes interesadas antes del informe final.
- Proponer un cronograma para implementar recomendaciones estratégicas basadas en la auditoría.
- Invitar a empleados de todos los niveles a sesiones donde se explique el impacto de los resultados del SGSI.
- Asegurar la validación oficial del informe final por parte de la alta dirección y responsables clave.

6. Conformidad del Plan de Auditoría

Este plan fue revisado y aprobado el 30 de noviembre de 2024 por el Gerente General de Win Internet Perú, Eduardo Zagazeta, junto al Vicepresidente de Operaciones Comerciales, Víctor Jauregui Hoyle, y el Gerente de TI, Carlos Oliveros. La ejecución del plan está programada para iniciarse el 5 de diciembre de 2024.