Plan de pruebas de auditoría (sede Barcelona)

1. Introducción

Objetivo:

Este plan define las pruebas que se harán para comprobar que los controles de seguridad, los procesos y las normas internas se cumplen correctamente en la sede de Barcelona.

Alcance:

Se revisarán sistemas, redes, dispositivos, políticas de seguridad y procesos clave que usa el equipo de Consultoría y Atención al Cliente, que son los departamentos que trabajan en esta sede.

Tipo de auditoría:

Auditoría interna, realizada por el equipo de TI de la empresa junto con un auditor designado.

2. Normativas y criterios de auditoría

- **Normas aplicables:** ISO 27001, RGPD y políticas internas de seguridad de la empresa.
- **Políticas y procedimientos internos:** gestión de accesos, uso de VPN, protección de datos de clientes.
- **Requisitos legales:** cumplimiento de la Ley de Protección de Datos (LOPDGDD).

3. Alcance de las pruebas

- **Sistemas:** portátiles y tablets de consultores y soporte técnico.
- **Redes y dispositivos:** Firewall local, red interna, VPN que conecta con la sede central.
- **Servidores:** acceso remoto a los servidores de la sede central (Madrid), aparte de los propios de la sede de Barcelona - CISCO y NAS.
- **Procesos clave:** gestión de accesos, copias de seguridad, uso de VPN, control de actualizaciones y respuesta ante incidentes.
- **Políticas y controles:** revisar que se cumplan políticas de contraseñas, cifrado de dispositivos y uso de antivirus.

4. **Equipo de auditoría**

Nombre	Cargo	Rol en la auditoría
Jorge Torres	Técnico de Seguridad TI	Realiza escaneos, pruebas de vulnerabilidades y simulaciones de ataques autorizados
Aníbal Giordani	Administrador de sistemas	Recopila logs, configuraciones y valida resultados técnicos
Elisabeth Ild	Responsable de consultoría	Coordina entrevistas, encuestas y verifica procesos operativos
Pablo Agudelo	Auditor técnico	Supervisa la ejecución técnica, revisa configuraciones avanzadas y valida hallazgos críticos

5. **Metodología de las pruebas**

Tipos de pruebas:

- **Pruebas documentales:** revisar políticas, inventarios de dispositivos y registros de accesos.
- **Pruebas técnicas:** escaneo de vulnerabilidades, comprobar configuraciones del firewall y revisión de logs.
- **Entrevistas:** hablar con personal de soporte técnico y consultores para confirmar cómo aplican los procedimientos.
- **Pruebas funcionales:** comprobar que la VPN funciona bien, que los backups se hacen y que se cumplen las políticas de acceso.

Metodologías de referencia: OWASP, NIST SP 800-115.

6. **Planificación y cronograma**

Fase	Fecha estimada	Duración
Revisión documental	5 - 6 de agosto	2 días
Pruebas técnicas	7 - 8 de agosto	2 días

Entrevistas	9 de agosto	1 día
Análisis y reporte preliminar	10 - 12 de agosto	3 días

7. **Detalle de pruebas específicas**

Ver archivo Excel adjunto para el detalle organizado.

8. **Procedimientos de documentación**

Todos los resultados se registrarán en plantillas de evidencias. Las capturas de pantalla y logs se guardarán en carpetas seguras con acceso restringido. Cada evidencia se adjuntará al informe final.

9. **Gestión de hallazgos**

Cualquier problema detectado se documentará con nivel de criticidad: bajo, medio, alto. Se validarán todos los hallazgos antes de incluirlos en el informe. Si se detecta algo crítico, se comunicará de inmediato al responsable de Consultoría.

10. **Coordinación y comunicación**

Reuniones diarias para revisar avances. Comunicación directa con Pablo Agudelo (punto de contacto) para resolver dudas. El equipo firmará un compromiso de confidencialidad y cumplirá la normativa de protección de datos.

Control de cambios

Si se cambia alguna prueba, se registrará la versión del plan y se justificará la razón. Los cambios se aprobarán por Jorge Torres (responsable de Seguridad TI).

Buenas prácticas

Las pruebas no afectarán la operativa diaria. Se avisará con antelación a los usuarios implicados. Se mantendrá una copia firmada del plan como parte de la documentación de la auditoría.

Aviso legal

Las pruebas técnicas sólo se harán en equipos y redes autorizados. Se respeta la ley y la privacidad de todos los empleados.