Matriz de Riesgos e Implementación de Controles de TI

Introducción y Propósito del Informe

El presente documento constituye el reporte técnico formal de seguimiento a la **Matriz de Riesgos y Controles de TI** de Telecafé Ltda. Este informe tiene como objetivo demostrar ante la auditoría el control y la mitigación efectiva de las debilidades tecnológicas identificadas sobre los activos de información institucionales.

A través de la aplicación de los controles del estándar internacional ISO 27001 y las directrices del MSPI (MinTIC), este informe consolida las evidencias que transforman los riesgos teóricos en una operación supervisada bajo la metodología PHVA (Planificar-Hacer-Verificar-Actuar).

Metodología de Priorización del Riesgo

Escala de Riesgo Inherente: Calculada mediante el cruce de Probabilidad (1 a 5) e Impacto (1 a 5).

- **Riesgo Crítico (Nivel 16-25):** Requiere atención inmediata y controles mensuales estrictos.
- **Riesgo Alto (Nivel 11-15):** Requiere gestión proactiva y monitoreo periódico de infraestructura.
- **Riesgo Moderado (Nivel 6-10):** Se mitiga mediante directivas y configuraciones estándar.

Matriz de Seguimiento Operativo (Riesgos Críticos y Altos)

A continuación, se consolidan los activos prioritarios extraídos de la matriz corporativa, el nivel de riesgo detectado, el control implementado y el estado de la evidencia almacenada en el repositorio interno:

Activo de Información	Vulnerabilidad Identificada	Riesgo Inherente	Control ISO 27001 Ejecutado	Frecuencia de Revisión	Evidencia de Soporte
Servidor DA	Actualizaciones faltantes, configuración incorrecta de sistemas.	CRÍTICO (25)	**A.6.8:** Evaluación y decisión sobre eventos de seguridad de la información.	Mensual	Logs de eventos de servidor y alertas de parches.
Servidor Páginas Web	Desactualizaciones y código vulnerable expuesto.	CRÍTICO (20)	**A.8.23:** Filtrado WEB y restricción de recursos no autorizados.	Mensual	Políticas de bloqueo activas en Fortigate.
Firewall & Antivirus	Falta de firmas de nuevos virus y	MODERADO (8)	**A.5.33:** Protección de registros y políticas de seguridad comunicadas.	Mensual	Consola Cloud Antivirus e

Activo de Información	Vulnerabilidad Identificada	Riesgo Inherente	Control ISO 27001 Ejecutado	Frecuencia de Revisión	Evidencia de Soporte
	políticas débiles de red.				informe de firmas actualizadas.
Cámaras IP	Acceso no autorizado por uso de contraseñas predeterminadas.	CRÍTICO (25)	**A.5.36:** Cumplimiento con políticas, reglas y estándares para seguridad.	Mensual	Directiva de cambio de claves por defecto aplicada.
Suite de Gmail	Phishing y falta de autenticación de dos factores (MFA).	MODERADO (10)	**A.5.33:** Robustecimiento de autenticación de accesos corporativos.	Mensual	Reporte de porcentaje de usuarios con MFA en consola Google.
Servidor de Backup	Conexiones inseguras y falta de redundancia de almacenamiento.	ALTO (12)	Monitoreo sistemático de copias de seguridad de datos institucionales.	Mensual	Logs de ejecución exitosa diaria/semanal de respaldos.
Sistema de Gestión Documental	Falta de cifrado de documentos y control de acceso inadecuado (Privacidad).	CRÍTICO (20)	Restricción lógica de acceso basada en roles del personal (Ley 1581).	Mensual	Matriz de permisos lógicos aprobada por área administrativa.

Organización de Evidencias en Repositorio Interno

Para facilitar las tareas de verificación de la auditoría, las evidencias físicas, técnicas y administrativas se encuentran estructuradas de forma restringida en el plan de continuidad del negocio del área de TI.

- **Políticas de TI y de seguridad de la información y Gobierno de TI:** Contiene el Programa de TI 2026, los documentos rectores aprobados (TEI-PRO-23, TEI-PRO-24) y actas de comités.
- **Riesgos y Seguridad de la Información:** Contiene esta matriz, reportes de logs extraídos de Fortigate, capturas de consolas de antivirus y auditorías de MFA de Google Workspace.
- **Soporte, Mantenimiento y Continuidad:** Hojas de vida de servidores, switches, bitácoras de mantenimiento de UPS, plantas eléctricas e históricos de la mesa de ayuda.
- **Capacitación y Cumplimiento Legal:** Listados de asistencia, memorandos de socialización de políticas de seguridad de la información y autorizaciones de tratamiento de datos personales (Ley 1581).

Conclusión.

A través de la aplicación de estos controles mensuales, Telecafé Ltda. logra reducir el nivel de riesgo inicial de un estado **"Crítico" o "Alto"** a un riesgo residual tolerable de

nivel **"Moderado" o "Bajo"**. Este informe demuestra que la Oficina de TI realiza un seguimiento técnico riguroso que resguarda la confidencialidad, integridad y disponibilidad de la infraestructura y los datos de la entidad.