Universidad de Palermo

TRABAJO FINAL DE GRADO

DIC 2025

MODELO INTEGRADO DE GESTIÓN DE CIBERSEGURIDAD Y TRANSFORMACIÓN DIGITAL PARA PEQUEÑAS PYMES DE SERVICIOS ADMINISTRATIVOS

ANTONELLA LUCIANA PIVA - 0134961 -
LIC. EN CIBERSEGURIDAD

TUTOR: BÁRBARA AYXA SIBLER

TRABAJO FINAL DE GRADO

INTRODUCCIÓN Y OBJETIVOS

MARCO TEORICO

METODOLOGIA

CASO DE ESTUDIO

RESULTADOS

PLAN DE MEJORA

CONCLUCION Y CIERRE

Idea → mejorar la seguridad en pymes de carácter administrativo

Problema → falta de recursos, procesos y cultura en ciberseguridad

Propuesta → modelo práctico e integrado adaptado a Pequeñas Pymes de Servicios Administrativos



TRABAJO FINAL DE GRADO

INTRODUCCIÓN Y OBJETIVOS

MARCO TEORICO

METODOLOGIA

CASO DE ESTUDIO

RESULTADOS

PLAN DE MEJORA

CONCLUCION Y CIERRE

Fundamentos conceptuales

El modelo se apoya en normas y marcos internacionales aplicados a la realidad de pequeñas PyMEs:

ISO/IEC 27001

ISO 31000: Gestión de Riesgos

Ley 25.326: Protección de Datos Personales.



NIST Cybersecurity Framework.



TRABAJO FINAL DE GRADO

INTRODUCCIÓN Y OBJETIVOS

MARCO TEORICO

METODOLOGIA

CASO DE ESTUDIO

RESULTADOS

PLAN DE MEJORA

CONCLUCION Y CIERRE

Componentes del modelo:

Categorías:

- Controles físicos (2)
- Acceso y autenticación (6)
- Respaldo y continuidad (7)
- Normativos y organizacionales (16)
- Concientización y cultura (1)



Pilar	ID	Control	Ejemplo	Acción esperada o evidencia	Categoría	Norma de Origen
Identificar	1	Mantener un inventario consolidado y actualizado de activos tecnológicos	Registro de computadoras, notebooks, teléfonos móviles corporativos y sistemas de	Planilla o sistema centralizado con el listado de activos, versiones, responsables y estado actual (alta,	Controles normativos y organizacionales + Controles físicos	ISO/IEC 27001:2022 A.5.9 / A.5.10 / A.5.11
Proteger	6	Implementar gestión segura de credenciales (contraseñas robustas, políticas de rotación	Uso de claves de al menos 8 caracteres, combinando letras, números y símbolos; adopción	Evidencia de configuración en sistemas, políticas o procedimientos internos que definan los requisitos	Controles de acceso y autenticación	ISO/IEC 27001:2022 A.5.15 / A.5.17
Detectar	19	Monitorear los accesos y actividades en sistemas críticos mediante la revisión periódica de registros (logs) y	Revisión de accesos a sistemas de gestión administrativa, correo corporativo o almacenamiento en la nube;	Reportes o registros de revisiones realizadas, capturas de configuración de alertas activadas y evidencia de acciones de	Controles de acceso y autenticación	ISO/IEC 27001:2022 — A.8.15 / A.8.16
Responder	25	Contar con un protocolo formal de respuesta a incidentes de seguridad que describa los pasos internos de	Ante un caso de phishing, ransomware o interrupción de un servicio crítico, el protocolo indica responsables, tiempos	Ante un caso de phishing, ransomware o interrupción de un servicio crítico, el protocolo indica responsables, tiempos de respuesta	Controles normativos y organizacionales + Controles de concientización y cultura	ISO/IEC 27001:2022 — A.5.24 / A.5.25 / A.5.26 / A.5.27 / A.5.33 / Ley 25.326 (Art. 6 — Deber de
Recuperar	30	Contar con un plan de continuidad operativa que contemple los escenarios críticos más probables y	Cortes de luz, caída de internet, indisponibilidad del sistema principal o interrupción de servicios	Documento formal del plan, firmado y actualizado, que detalle escenarios, responsables, tiempos de recuperación, medidas	Controles de respaldo y continuidad	ISO/IEC 27001:2022 — A.5.29 / A.5.30 / A.5.33 + ISO 31000 (Gestión de continuidad)

TRABAJO FINAL DE GRADO

INTRODUCCIÓN Y OBJETIVOS

MARCO TEORICO

METODOLOGIA

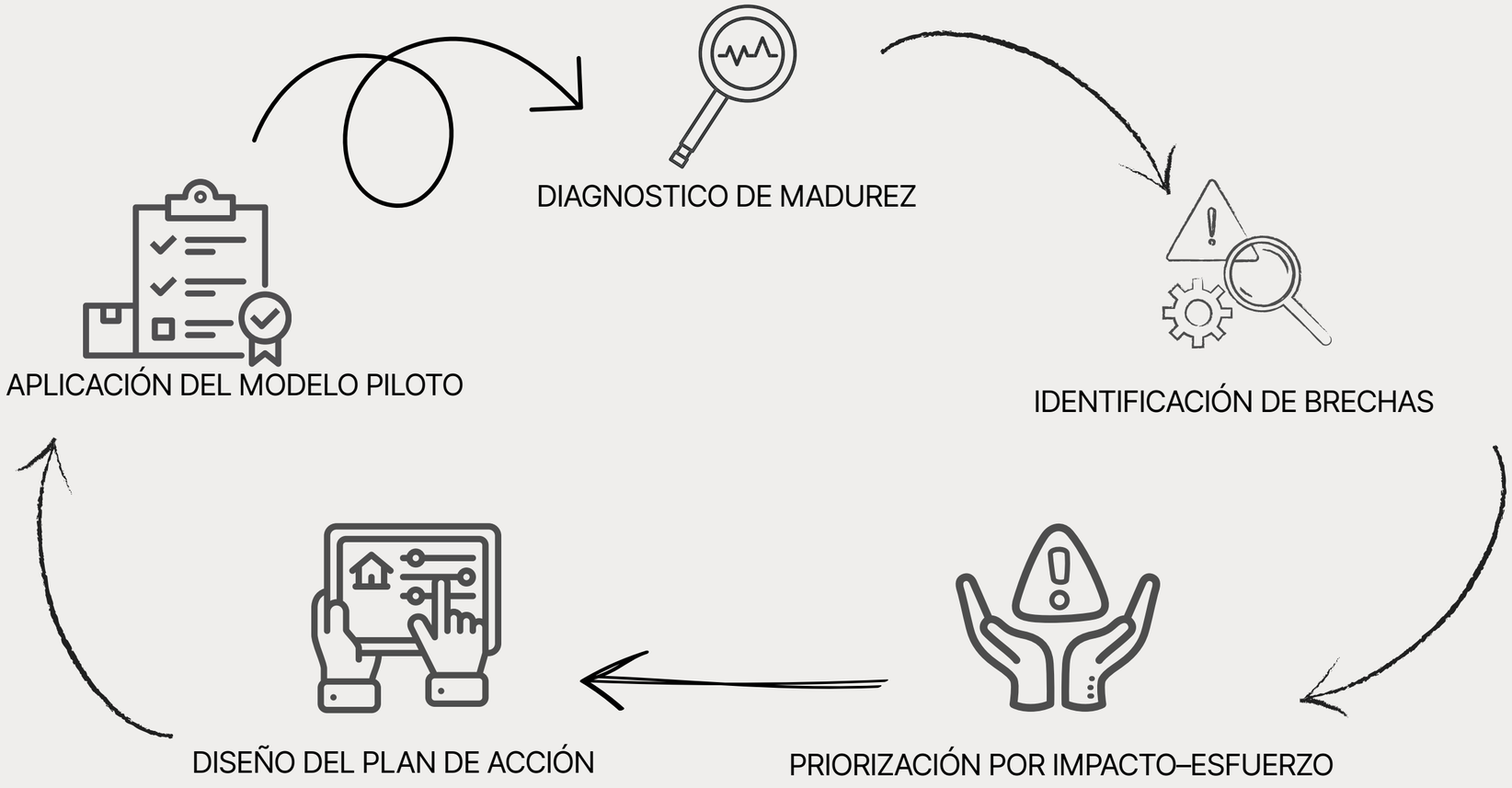
CASO DE ESTUDIO

RESULTADOS

PLAN DE MEJORA

CONCLUCION Y CIERRE

Se diseñó un modelo práctico basado en un análisis de brechas (Gap Analysis) adaptado a pequeñas PyMEs de servicios administrativos.



TRABAJO FINAL DE GRADO

INTRODUCCIÓN Y OBJETIVOS

MARCO TEORICO

METODOLOGIA

CASO DE ESTUDIO

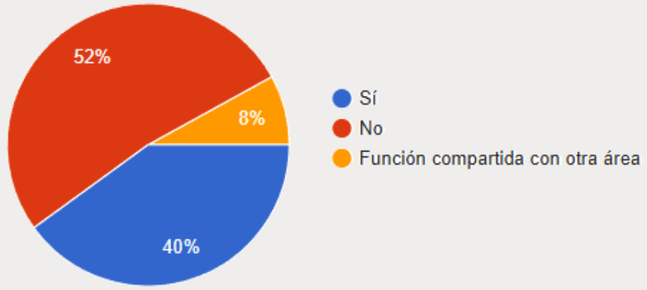
RESULTADOS

PLAN DE MEJORA

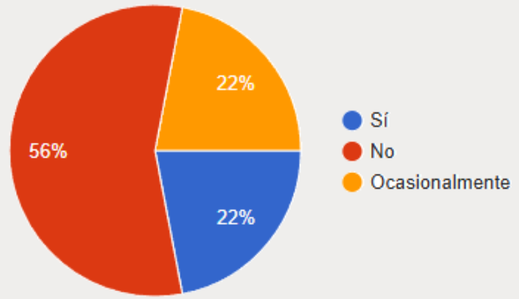
CONCLUCION Y CIERRE

Resultados de la encuesta a PyMEs

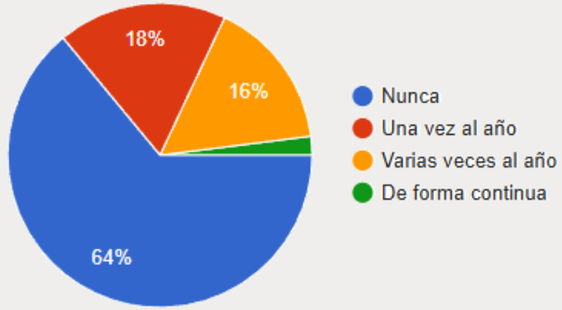
4. ¿La empresa cuenta con una persona responsable de ciberseguridad o seguridad de la información?



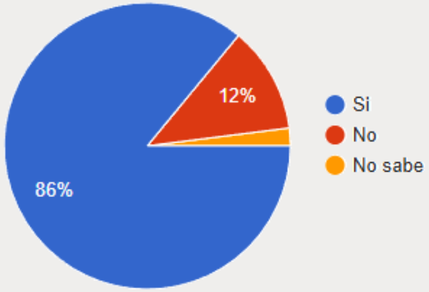
8. ¿Se realizan auditorías o revisiones internas sobre seguridad de la información o gestión de riesgos?



5. ¿Se realizan capacitaciones o charlas sobre ciberseguridad (phishing, contraseñas, redes sociales)?



11. ¿La empresa trata datos personales de clientes, proveedores o empleados?
(Ejemplos: nombre, DNI, correo electrónico, teléfono, dirección, CUIL/CUIT, cuenta bancaria, firma, etc.)



TRABAJO FINAL DE GRADO

INTRODUCCIÓN Y OBJETIVOS

MARCO TEORICO

METODOLOGIA

CASO DE ESTUDIO

RESULTADOS

PLAN DE MEJORA

CONCLUCION Y CIERRE

Caso de Estudio:





- Villa Ballester - San Martin
- Empresa familiar fundada en 1991, dedicada a administración y comercialización de propiedades.
- 3 personas activas

TRABAJO FINAL DE GRADO

INTRODUCCIÓN Y OBJETIVOS

MARCO TEORICO

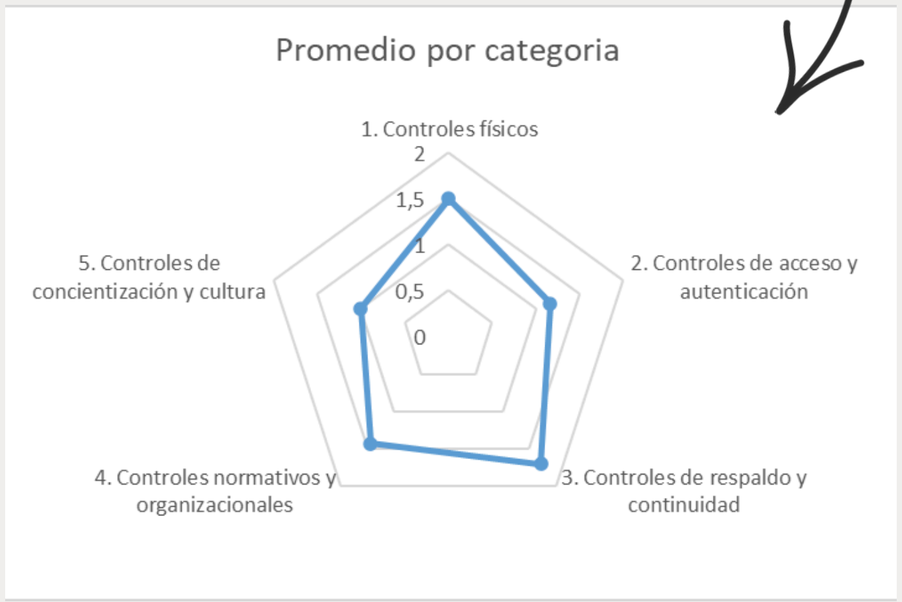
METODOLOGIA

CASO DE ESTUDIO

RESULTADOS

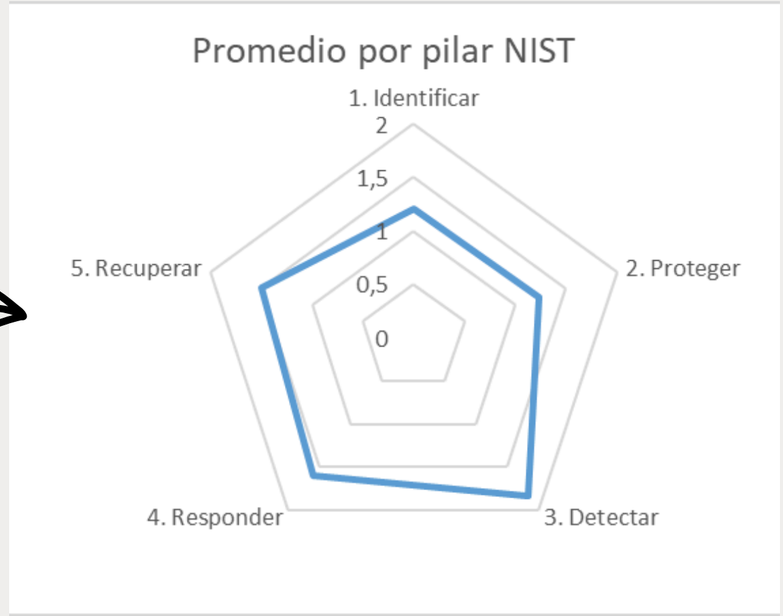
PLAN DE MEJORA

CONCLUCION Y CIERRE



Dominio	Inicial
1. Controles físicos	1,5
2. Acceso y autenticación	1,17
3. Respaldo y continuidad	1,71
4. Normativos y organizacionales	1,44
5. Concientización y cultura	1

Dominio	Inicial
1. Identificar	1,2
2. Proteger	1,23
3. Detectar	1,83
4. Responder	1,6
5. Recuperar	1,5



TRABAJO FINAL DE GRADO

INTRODUCCIÓN Y OBJETIVOS

MARCO TEORICO

METODOLOGIA

CASO DE ESTUDIO

RESULTADOS

PLAN DE MEJORA

CONCLUCION Y CIERRE

Pilar	ID	Acción de mejora	Plazo recomendado	Costo	Prioridad
Identificar	1	Elaborar inventario consolidado de dispositivos (PCs y celulares).	1 mes	Bajo	Inmediata
Proteger	7	Activar el doble factor de autenticación (2FA) en cuentas de Google Workspace, homebanking y redes sociales corporativas.	1 mes	Bajo	Inmediata
Proteger	12	Habilitar bloqueo automático de pantalla y establecer contraseña de inicio en todos los dispositivos.	1 mes	Bajo	Inmediata
Proteger	17	Documentar cada baja en un registro o checklist de salida.	1 mes	Bajo	Inmediata
Detectar	19	Activar las alertas automáticas de seguridad en Google Workspace y revisar notificaciones de inicio de sesión sospechoso.	1 mes	Bajo	Inmediata
Detectar	20	Capacitar al personal sobre cómo identificar y reportar correos o mensajes sospechosos.	1 mes	Bajo	Inmediata
Detectar	24	Suscribirse a boletines de seguridad de AFIP, Banco Central, Microsoft y Google.	1 mes	Bajo	Inmediata
Responder	27	Elaborar una lista actualizada de contactos de emergencia (soporte técnico, banco, proveedores, asesor legal).	1 mes	Bajo	Inmediata
Recuperar	32	Completar la migración de información crítica a Google Drive y configurar acceso offline.	1 mes	Bajo	Inmediata

Costo	Descripción
Bajo ($)	No requiere inversión económica directa, solo tiempo o ajustes organizacionales.
Medio ($$)	Requiere herramientas o servicios de bajo costo o inversión puntual.
Alto ($$$)	Requiere reemplazo de hardware, consultoría externa o licencias pagas.

Prioridad	Descripción
Inmediata (0–1 mes)	Acciones críticas, bajo costo y alto impacto.
Corto Plazo (1–3 meses)	Mejora significativa y factible en el trimestre.
Mediano Plazo (3–6 meses)	Requiere organización o recursos moderados.
Posterior (6–12 meses)	Depende de madurez, recursos o planificación anual.

TRABAJO FINAL DE GRADO

INTRODUCCIÓN Y OBJETIVOS

MARCO TEORICO

METODOLOGIA

CASO DE ESTUDIO

RESULTADOS

PLAN DE MEJORA

CONCLUCION Y CIERRE

Conclusiones principales

- Modelo viable y replicable para PyMEs pequeñas
- Controles aplicables sin grandes recursos
- Caso piloto evidenció brechas y oportunidades
- Encuesta validó necesidad de modelos simples

Próximos pasos: *expandir a estudios contables, jurídicos y consorcios.*

UP
Universidad de Palermo

TRABAJO FINAL DE GRADO

DIC 2025

GRACIAS!

Hagamos que la ciberseguridad este accesible para todos.