CMMI

Nivel 1

"En este nivel, los procesos de privacidad y seguridad son improvisados y reactivos. La organización tiene pocas o nulas políticas formalizadas para proteger la información, y las prácticas de seguridad y privacidad son mínimas o inexistentes. La protección de la información depende de la habilidad individual del equipo, sin un marco claro.

Indicadores de madurez en el Nivel 1:

• No existen procesos estandarizados para la gestión de datos sensibles.

• Las medidas de seguridad y privacidad se implementan de manera reactiva y solo después de incidentes o requerimientos externos.

• No hay un control adecuado sobre el acceso a los datos estadísticos y geográficos."

Nivel 2

"En este nivel, la organización comienza a gestionar de manera planeada y controlada los procesos de privacidad y seguridad de la información, aunque estos procesos aún no están completamente integrados. Las prácticas de protección de datos se establecen y documentan, lo que permite que los datos estén más protegidos y que las tareas sean más predecibles.

Indicadores de madurez en el Nivel 2:

• Se implementan procesos documentados para la protección de datos, como políticas de acceso y control de usuarios.

• Se designa un responsable de seguridad de la información para monitorear el cumplimiento de las políticas de privacidad y seguridad.

• Existen protocolos básicos para responder a incidentes de seguridad y violaciones de privacidad, pero no hay métricas avanzadas ni análisis de riesgos."

Nivel 3

"En este nivel, los procesos de privacidad y seguridad están completamente definidos y documentados. La organización cuenta con políticas claras y procedimientos estandarizados que son consistentes en toda la organización, y se busca una cultura de cumplimiento en términos de protección de datos.

Indicadores de madurez en el Nivel 3:

• Existen políticas y procedimientos bien definidos para la privacidad y seguridad de los datos estadísticos y geográficos.

• Los procesos de manejo de datos están alineados con las normativas y estándares internacionales (ej., ISO/IEC 27001, GDPR).

• Se realizan auditorías y evaluaciones periódicas de cumplimiento en temas de privacidad y seguridad."

Nivel 4

"En este nivel, los procesos son medidos y monitoreados cuantitativamente. La organización tiene métricas establecidas y realiza un análisis detallado de los riesgos de privacidad y seguridad. Esto permite identificar con precisión áreas de mejora y tomar decisiones informadas para la protección de datos.

Indicadores de madurez en el Nivel 4:

• Se utilizan métricas específicas para evaluar la efectividad de las políticas de privacidad y seguridad, como el tiempo de respuesta ante incidentes y el número de accesos no autorizados.

• Se lleva a cabo un análisis de riesgos regular que cuantifica la probabilidad y el impacto de posibles amenazas de seguridad.

• Existe una cultura de prevención proactiva en el manejo de la información."

Nivel 5

"En el nivel final, la organización se encuentra en un estado de mejora continua, optimizando constantemente sus procesos para la privacidad y seguridad de la información. Se implementan innovaciones tecnológicas y se fomenta una cultura organizacional en la que la seguridad y privacidad son fundamentales y adaptables a los cambios tecnológicos y regulatorios.

Indicadores de madurez en el Nivel 5:

• Los procesos de privacidad y seguridad se mejoran continuamente mediante técnicas avanzadas como el machine learning para detectar patrones de amenazas.

• Se realizan evaluaciones continuas de las prácticas de seguridad y se adoptan innovaciones para enfrentar nuevas amenazas.

• La organización cuenta con una infraestructura de seguridad ágil y adaptable que permite responder rápidamente a cambios en el entorno regulatorio o en el perfil de riesgos."