Es un placer presentar este documento, titulado “Cuadro de Mando de Seguridad Inicial para PYME”, como primera propuesta para abordar la medición y el control de la seguridad informática durante mi periodo de prácticas. El objetivo es proporcionar una hoja de ruta basada en indicadores objetivos y claros, que permita demostrar el valor tangible de las acciones de seguridad para proteger los activos más importantes de la empresa y apoyar la toma de decisiones informadas para el negocio.

Marco General de Métricas e Indicadores

Qué medir: Estado de accesos, incidentes de seguridad, copias de seguridad, actualizaciones, y nivel de concienciación de empleados.

Por qué es importante:

- **Protección del negocio**: Minimizar riesgos de fuga de datos y pérdida de productividad. Proteger datos críticos del CRM y la integridad del negocio.
- **Confianza de clientes y socios**: Garantizar la seguridad de la información en el CRM.
- **Eficiencia operativa**: Prevenir incidencias que afecten a procesos críticos. Reducir riesgos operativos y financieros frente a ciberataques o errores humanos.
- **Demostrar mejoras concretas** mediante la reducción de incidentes, tiempos y exposición.

Objetos de Medición: Procesos y Activos Clave

- CRM y bases de datos de clientes y ventas.
- Sistemas de gestión de usuarios, accesos y contraseñas.
- Sistemas de copia de seguridad y recuperación.
- Herramientas de protección contra phishing y sistemas de correo.
- Infraestructura TI y su actualización de parches.

Indicadores y Métricas de Seguridad Propuestos. Áreas Clave y Objetos de Monitorización.

Gestión de Accesos y Contraseñas de Usuarios

- **Indicador 1 →**Porcentaje de usuarios con contraseñas seguras (mínimo 8 caracteres/multifactor (MFA).
- **Indicador 2 →**Número de acceso fallidos por usuario/mes
- **Indicador 3 →**Frecuencia y éxito de auditorías de acceso a los datos críticos.
- **Indicador 4 →** Tiempo medio de alta/baja de usuarios en el CRM

Protección contra Phishing y Concienciación de empleados

- Indicador 5 →Número de correos de phishing detectados por el sistema.
- Indicador 6 → % de empleados que reportan correctamente un intento de phishing (simulaciones).
- Indicador 7 → % de empleados que completan formación antiphishing cada trimestre.
- Indicador 8 →Tiempo medio de respuesta ante incidentes de phishing (MTTR).

Gestión de Copias de Seguridad y Recuperación

- Indicador 9 → Frecuencia de realización de copias de seguridad (diaria, semanal).
- Indicador 10 → % de copias de seguridad completadas sin errores.
- Indicador 11 →Tiempo medio de recuperación de datos ante fallo/incidencia (RTO).
- Indicador 12 →Porcentaje de verificaciones automáticas exitosas de restauración de backups.

Actualizaciones y Parches

- Indicador 13 →Porcentaje de sistemas actualizados en plazo tras la aparición de un parche crítico respecto al total.
- Indicador 14 → Tiempo medio de aplicación de parches críticos desde su publicación
- Indicador 15 → Número de vulnerabilidades detectadas antes y después de las actualizaciones mensuales.

Recolección y Análisis de datos

- **Fuentes de datos**:
  - Logs del CRM y sistema de autenticación.
  - Informes de correo y seguridad perimetral (antiphishing).
  - Registros de backup. Resultados automáticos de backups y restauraciones.
  - Consola de gestión de actualizaciones.
  - Encuestas y pruebas de concienciación a empleados.
  - Informes de plataformas de e-learning.
  - Paneles de seguridad de endpoints y sistemas operativos.

- **Frecuencia de análisis**:
  - Semanal: Accesos, phishing y copias de seguridad.
  - Mensual: Actualizaciones y concienciación.

Ejemplo de Cuadro de Mando Inicial

Área Clave	Indicador / Métrica	Qué mide	Fuente de datos	Frecuencia de análisis	Objetivo
Gestión de Accesos y Contraseñas	% de usuarios con contraseñas seguras (MFA/8 caracteres)	Nivel de robustez de las credenciales	Logs del CRM / sistema de autenticación	Semanal	≥ 95% usuarios con contraseñas seguras
	Nº de accesos fallidos por usuario/mes	Intentos sospechosos o errores de login	Logs de acceso	Semanal	≤ 5 accesos fallidos/usuario
	Frecuencia y éxito de auditorías de acceso	Control de accesos a datos críticos	Informes de auditoría	Mensual	100% auditorías completadas

Área Clave	Indicador / Métrica	Qué mide	Fuente de datos	Frecuencia de análisis	Objetivo
	Tiempo medio de alta/baja de usuarios en el CRM	Agilidad en la gestión de identidades	CRM / Helpdesk	Mensual	≤ 24h para altas/bajas
Protección contra Phishing y Concienciación	Nº de correos de phishing detectados	Capacidad de los filtros antiphishing	Informes de correo seguro	Semanal	Detección ≥ 90% de intentos
	% de empleados que reportan correctamente phishing	Concienciación y cultura de seguridad	Simulaciones de phishing	Mensual	≥ 80% empleados lo reportan
	% de empleados que completan formación trimestral	Nivel de formación en ciberseguridad	Plataforma e-learning	Mensual	100% empleados completan formación
	Tiempo medio de respuesta a incidentes de phishing (MTTR)	Eficiencia en la contención de ataques	Equipo TI / Helpdesk	Semanal	≤ 2h respuesta
Copias de Seguridad y Recuperación	Frecuencia de copias de seguridad (diaria/semanal)	Regularidad de la protección de datos	Registros de backup	Semanal	Copias diarias completadas
	% de copias completadas sin errores	Fiabilidad de los backups	Informes automáticos de backup	Semanal	≥ 98% sin errores
	Tiempo medio de recuperación de datos (RTO)	Velocidad de restauración ante fallo	Pruebas de recuperación	Mensual	≤ 4h recuperación
	% de verificaciones automáticas exitosas	Eficiencia de restauraciones probadas	Logs de restauración	Mensual	≥ 95% verificaciones correctas

Área Clave	Indicador / Métrica	Qué mide	Fuente de datos	Frecuencia de análisis	Objetivo
Actualizaciones y Parches	% de sistemas actualizados en plazo	Cumplimiento en gestión de vulnerabilidades	Consola de actualizaciones	Mensual	≥ 95% sistemas actualizados en plazo
	Tiempo medio de aplicación de parches críticos	Rapidez en aplicar medidas de seguridad	Consola de gestión de parches	Mensual	≤ 7 días
	Nº de vulnerabilidades antes y después de actualizaciones	Impacto de las actualizaciones en la seguridad	Escáner de vulnerabilidades	Mensual	Reducción ≥ 80% vulnerabilidades

Cómo Demuestra Valor

- Incremento en los usuarios protegidos y reducción de incidentes graves.
- Disminución de tiempo de reacción y restauración ante incidentes.
- Mayor concienciación y cultura preventiva, con empleados más preparados ante amenazas.
- Disminución progresiva de vulnerabilidades técnicas y administrativas.

Este cuadro de mando convierte la seguridad en un motor que impulsa la confianza, la estabilidad y la competitividad de la PYME, con datos claros para reportar cada avance y justificar futuras inversiones en protección.

Conclusión

El uso de este cuadro de mando basado en métricas e indicadores permitirá a la empresa visualizar de forma objetiva y continua el estado de su seguridad, optimizando recursos y priorizando acciones preventivas. Durante mi periodo de prácticas, este enfoque facilitará la toma de decisiones alineadas con los objetivos estratégicos y evidenciará el valor de invertir en seguridad, transformando la protección informática de un gasto necesario a una verdadera inversión para el crecimiento y la reputación de la organización.

Fuentes Consultadas

- Visualización Estratégica: Cuadros de Mando para PYMES – AceleraPyme.
- Cuadros de Mando de Seguridad de los Sistemas de Información – CCN.
- Artículos y plantillas de KPIs y cuadros de mando: BSC Designer, Boardmix.
- Fuentes sobre gestión de seguridad en CRM, backup y antiphishing consultadas para tendencias y mejores prácticas recientes.