Implementa Políticas de Seguridad DLP a dispositivos de almacenamiento externo

Estudiante: Eric Grossermann
Fecha De Entrega: 12/08/25

Objetivo General:

- **Parte 1**: Definir y establecer políticas de DLP que ayuden a proteger la información confidencial.

Introduccion al Data Loss Prevention.

Outlook es una herramienta muy utilizada en la web Grossermann.com como centro de comunicaciones entre sus clientes y provedoores. No obstante sin la seguridad adecuada esta expuesto a una perdida de datos y robo de informacion si no se trata a tiempo.

Clasificación de datos.

A continuacion se clasificaran los datos de la siguiente manera:

Datos Públicos:

- ☐ ***Articulos de ventas deportivas en la web**
- ☐ ***Correos y Telefonos de la Empresa**
- ☐ ***Redes Sociales de la Empresa**

Datos Internos:

- ☐ ***Datos Compradores**
- ☐ ***Datos Provedoores**
- ☐ ***Datos de Trabajadores**

Datos Sensibles:

- ☐ ***Tarjetas de Creditos de Compradores.**
- ☐ ***Direcciones, Nombre y Apellido de Compradores.**
- ☐ ***Documentos Ventas y Compras de la Empresa.**

Acceso y Control

En la siguiente Clasificacion se define el flujo de revisión de permisos, indicando qué roles dentro de la organización serán responsables de estas revisiones y cómo se llevarán a cabo.

Acceso Restringido:
Los usuarios finales solo tendra acceso a puntos de ventas de la web, para evitar manipulacion y robo de informacion.

Revision de Permisos:
Los permisos de Carpeta, Archivos y accesos a los correos internos (Outlook) de la empresa solo seran permitidos por el departamento interdo de la compania.

Acceso Temporal:
En el momento en el que se requiera acceso a un archivo sensible, este sera autorizado bajo autorizacion formal y se terminara una vez completado la revision.

Monitoreo y Auditoría.

Se ejecutara una auditoria y monitoreos de manera rutinaria para una revision constante de ingreso no autorizados, falsos positivos u cualquier anomalia interna de la empresa, el cual se llevara a cabo de la siguiente manera:

- ☐ *Alertas de Seguridades (EDR, SIEM, DLP, IDS/IPS)
- ☐ *Registro de Actividades (Logs)
- ☐ *Auditorias

Prevención de Filtraciones.

Para evitar filtraciones y perdidas de informacion privilegiada se aplicara las siguientes medidas:

- ☐ *Guardar contraseñas en un Lugar seguro y Cambiar Periodicamente.
- ☐ *Validacion de contraseñas Segura (Aplicando tecnica de Contrasena Compleja)
- ☐ *Implementacion de Doble autenticacion
- ☐ *Implementacion de Alertas de Seguridad por Ingresos No Autorizados

---

Educación y concientización.

Es indispensable que los trabajadores internos de la Empresa Grossermann.com entiendan la importancia de buenas practicas y politicas de seguridad para evitar fugas de informacion privilegiada.

Para llevar a cabo la Capacitacion al personal se ejecutara un Plan periodico de:

- [ ] *Concientacion de Riesgos
- [ ] *Politicas de Seguridad del Personal

Esto se llevara de manera Bimestral para llevar Constancias y Seguimientas de politicas seguras.

Conclusion

La **I**mplementación de políticas DLP fortalece la seguridad de la información y garantiza el uso adecuado de herramientas como Outlook. Al aplicar el principio de mínimo privilegio, auditorías continuas y medidas preventivas, se reduce significativamente el riesgo de fugas de datos y se asegura la continuidad operativa de la empresa.