1.- Introducción al Data Loss Prevention

En el entorno empresarial actual, donde los datos constituyen un activo crítico y muy valioso para las empresa, la fuga de información es un acto que debe de evitar a cualquier costo, ya que pone en riesgo la reputación de la empresa, la confianza de sus clientes y socios, así como la operación correcta de la empresa. Es en este punto donde la utilización de un DLP se vuelve crítico.

Un DLP es una estrategia de protección de información sensible dentro de las empresas y evita su fuga al exterior por medio de medidas aplicadas especializadas en detección, monitoreo y protección de la información crítica. Estas medidas estan centradas en evitar el acceso no autorizado, fugas (intencional o accidental) y exposiciones al público.

2.- Clasificación de datos

Los datos deben ser clasificados de acuerdo a su sensibilidad y nivel de impacto que se fuga podría generar, por lo cual se establecen 3 categorías:

- Datos públicos:
  - Información que puede ser compartida con cualquier individuo o empresa pública sin restricciones, ya que no representa ningún riesgo y es de dominio público.
  - Ejemplos: contenido de las campañas de marketing, comunicados o entrevistas de prensa, noticias del sitio web, etc.
- Datos internos:
  - Información que circula libremente dentro de todas las áreas de la empresa pero no está autorizada a salir al exterior.
  - Ejemplos: políticas de limpieza, políticas de RH, políticas de convivencia, informes de rendimiento, informes de mantenimiento, etc.
- Datos sensibles:
  - Información de suma importancia y crítica que de ninguna manera puede ser expuesta a ninguna persona no autorizadas y que se pérdida puede causar grandes daños o repercusiones.
  - Ejemplos: datos de salud de los empleados, CURP, RFC, datos financieros de toda índole, credenciales, contratos, estados de cuenta, etc.

3.- Acceso y control

- Políticas de acceso:
  - Los accesos deben ser concedidos por rol y necesidad de acuerdo a sus actividades, para sólo otorgar la menor cantidad de permisos requerida.

- Los permisos deben ser re-evaluados cada 2 meses para hacer las modificaciones necesarias.
- Se deben otorgar accesos temporales para visitantes externos o personas que lo requieran siguiendo la política del menor privilegio y deben tener una fecha de expiración de máximo 2 días y después deben desaparecer automáticamente y requerir una renovación.

- Responsabilidad de revisión:
  - Para revisar y otorgar los accesos, es necesario que primero sean aceptados por los gerentes/encargados de cada área, una vez aceptados, serán requeridos mediante un escrito al equipo de IT donde se debe sustentar el porqué se requiere cada permiso para cada usuario.
  - Para auditorías de permisos, se deberá nombrar una persona con un puesto especial de auditor de permisos en el área de ciberseguridad para coordinar, revisar y auditar anualmente todo.
  - El equipo de TI será el encargado de otorgar, denegar y mantener los permisos de todos los usuarios.

4.- Monitoreo y auditoría

Para el monitoreo se propone lo siguiente:

- Instalación de EDR y de un DLP de endpoint en todos los equipos tanto de escritorio, como laptops, servidores y celulares de la empresa para emitir alertas al SIEM.
- SIEM: Recibir alertas y eventos en tiempo real de los EDR y otros medios para detectar amenazas y comportamiento anómalos para su investigación y mitigación.
- Logs: Activar y guardar los logs de todos los equipos por lo menos durante un año completo para posteriores revisiones.
- El encargado de las auditorias de permisos en la empresa deberá revisar constantemente los permisos y hacer una auditoría completa una vez al año.

5.- Prevención de filtraciones

Para evitar las filtraciones de información se proponen las siguiente medidas:

- Toda la información deberá ser clasificadqa de acuerdo a su nivel de importancia y sensibilidad, además de agregar metadatos y marcas de agua para identificarla fácilmente.
- La empresa otorgará a cada usuario que maneje información sensible una laptop preconfigurada, cifrada y con todas las medidas de seguridad pertinentes, así como un EDR y las siguiente políticas ya aplicadas.

- Bloqueo automático de periféricos de almacenamiento de información externos (USB, SSD, etc.).
- Cifrado de datos en reposo y en tránsito.
- Revisión y bloqueo automático de archivos enviados por correo en búsqueda de patrones o palabras clave que identifiquen a información clasificada como sensible antes de enviar cualquier correo.
- MFA para todos los usuarios.
- Cambio de contraseña cada 4 meses y debe ser de, al menos, 1 mayúscula, 1 minúscula, 1 número, 1 carácter especial y 15 caracteres en total.
- Revisión y bloqueo de información enviada a través de todas las redes wifi (especialmente la de invitados) de archivos que se consideren sensibles, así como monitero de conexiones y datos enviados a través de un firewall que detecte el tamaño de los archivos enviados y genere las alertas pertinentes para el SIEM.

6.- Educación y concientización

Se requiere una constante capacitación de los empleados para asegurar el éxito de la política DLP, por lo cual se sugiere lo siguiente:

- Capacitación anual de manejo de información sensible para todos los empleados de la empresa.
- Capacitación trimestral para el equipo de TI de la importancia de proteger la infomación sensible.
- Simulaciones periódicas de phishing al enviar correo con links maliciosos creados por el equipo de TI para poner a prueba su capacitación.
- Publicidad periódica en anuncios dentro de la empresa para recordar la política de DLP y la importancia de proteger la información sensible.
- Capacitación constante de nuevas técnicas de protección para la actualización de los equpos de ciberseguridad y TI.