**Política de Prevención de Pérdida de Datos (DLP) para EMT Madrid**

**Fecha:** 1 de abril de 2025

**Elaborado por:** Departamento de Seguridad de la Información **Versión:** 1.0

**1. Introducción al Data Loss Prevention (DLP)**

La Prevención de Pérdida de Datos (DLP) es un conjunto de estrategias, procesos y tecnologías diseñadas para asegurar que la información sensible de la Empresa Municipal de Transportes de Madrid (EMT Madrid) no se pierda, sea utilizada indebidamente o accedida por personal no autorizado. En un entorno donde se manejan datos operativos críticos, información personal de empleados y potencialmente datos de usuarios, la implementación de una política DLP robusta es fundamental. Su objetivo principal es proteger la confidencialidad, integridad y disponibilidad de los activos de información de la EMT, prevenir fugas de datos accidentales o malintencionadas, y asegurar el cumplimiento de las normativas de protección de datos aplicables (como el RGPD).

**2. Clasificación de Datos**

Para aplicar controles de seguridad adecuados, toda la información manejada en EMT Madrid se clasificará según su nivel de sensibilidad e impacto en caso de divulgación no autorizada. Se establecen las siguientes categorías:

1. **Datos Públicos:** Información diseñada para el consumo público y que no supone un riesgo para la organización si se divulga.
   * *Ejemplos:* Horarios y rutas de autobuses publicados, tarifas, notas de prensa, información general del sitio web corporativo.
2. **Datos Internos:** Información destinada al uso exclusivo del personal de EMT Madrid, cuya divulgación no autorizada podría causar un impacto operativo o reputacional moderado.
   * *Ejemplos:* Comunicaciones internas generales, procedimientos operativos no críticos, manuales de formación estándar, directorios internos básicos.
3. **Datos Sensibles (Confidenciales o Restringidos):** Información crítica o privada cuya divulgación no autorizada podría causar un daño grave a la organización, sus empleados, clientes o incumplimientos legales/regulatorios significativos. El acceso está estrictamente limitado.
   * *Ejemplos:* Datos personales de empleados (nóminas, expedientes), información financiera detallada, contratos con proveedores, planes estratégicos, detalles de infraestructuras críticas, informes de seguridad, datos de sistemas de videovigilancia, información sujeta a secreto industrial o legal.

La correcta clasificación es responsabilidad del propietario de la información y es esencial para aplicar los controles DLP adecuados.

**3. Acceso y Control (Principio del Menor Privilegio)**

El acceso a los datos de EMT Madrid se regirá estrictamente por el **Principio del Menor Privilegio** [source: 3, 9]: los empleados solo tendrán los permisos de acceso mínimos necesarios para realizar las funciones específicas de su puesto de trabajo.

* **Políticas de Acceso:** El acceso se basará en roles y responsabilidades definidos. Se denegará el acceso por defecto, requiriendo una justificación explícita para conceder permisos sobre datos Internos o Sensibles.
* **Flujo de Revisión de Permisos:**
  + **Responsables:** Los responsables de cada departamento, en colaboración con el Departamento de Seguridad de la Información y el Departamento de TI, serán los encargados de aprobar las solicitudes de acceso y revisar periódicamente los permisos asignados a su personal.
  + **Proceso:** Se realizarán revisiones de permisos de forma trimestral [source: 11] y siempre que un empleado cambie de puesto o abandone la organización. Estas revisiones verificarán que los accesos sigan siendo necesarios y apropiados según el principio del menor privilegio. Se mantendrá un registro documentado de todas las concesiones y revocaciones de acceso.

**4. Monitoreo y Auditoría**

Se implementará un sistema continuo de monitoreo y auditoría para supervisar el manejo de datos sensibles y detectar posibles violaciones de esta política.

* **Reglas de Monitoreo:** Se establecerán reglas específicas en las herramientas DLP para detectar y alertar sobre actividades sospechosas como:
  + Intentos de acceso no autorizado a datos sensibles.
  + Movimiento de grandes volúmenes de datos clasificados como Internos o Sensibles.
  + Transferencia de datos sensibles a destinos no autorizados (ej: correos personales, almacenamiento en la nube no aprobado, dispositivos USB no autorizados).
  + Impresión excesiva de documentos sensibles.
* **Herramientas:** Se utilizarán soluciones DLP específicas, que podrán integrarse con herramientas SIEM (Security Information and Event Management) para correlacionar eventos y obtener una visión completa [source: 15]. Estas herramientas monitorizarán puntos clave como el correo electrónico, el tráfico de red, el uso de dispositivos extraíbles y el acceso a aplicaciones cloud y locales.
* **Auditoría:** El Departamento de Seguridad de la Información realizará auditorías periódicas (al menos semestralmente) de los registros de acceso y las alertas generadas por las herramientas DLP para verificar el cumplimiento de la política y identificar áreas de mejora [source: 17].

**5. Prevención de Filtraciones**

Se adoptarán medidas técnicas y organizativas para minimizar el riesgo de filtración de datos sensibles:

* **Cifrado:** Los datos sensibles deberán estar cifrados tanto en reposo (en servidores, bases de datos, portátiles) como en tránsito (durante transferencias por red, correo electrónico).
* **Tecnologías DLP:** Las herramientas DLP se configurarán para bloquear activamente o poner en cuarentena las transmisiones de datos que violen las políticas establecidas (ej: envío de un documento con datos personales a un correo externo no autorizado).
* **Control de Canales de Salida:** Se restringirá o monitorizará el uso de canales que puedan facilitar la fuga de información, como el correo electrónico personal, servicios de almacenamiento en la nube no corporativos, aplicaciones de mensajería instantánea y dispositivos de almacenamiento extraíble (como se detallará en la Parte 2 de este ejercicio).
* **Etiquetado y Clasificación:** Se promoverá el uso de herramientas que permitan etiquetar los documentos según su clasificación [source: 19], facilitando la aplicación automática de políticas de protección por parte de las herramientas DLP.

**6. Educación y Concientización**

La concienciación del personal es clave para el éxito de la estrategia DLP.

* **Capacitación:** Todo el personal de EMT Madrid recibirá formación obligatoria anual sobre esta política DLP, la importancia de la clasificación de datos, los procedimientos seguros para manejar información sensible y los riesgos asociados a las fugas de datos [source: 21]. Se realizarán formaciones específicas y más detalladas para aquellos roles que manejan regularmente datos sensibles.
* **Comunicación Continua:** Se utilizarán canales internos (intranet, correos informativos, charlas) para reforzar periódicamente los conceptos clave de la política DLP y concienciar sobre nuevas amenazas o mejores prácticas [source: 22]. Se destacará la responsabilidad individual de cada empleado en la protección de la información corporativa.