Informe de Políticas de Seguridad: Data Loss Prevention (DLP)

Fecha: 30 de Mayo de 20245
Elaborado por: Germán Alberto Parra Araque
Empresa: 4Geeks Solutions

1. Introducción

Data Loss Prevention (DLP) es una herramienta de software que permite a las empresas implementar mecanismos para prevenir la filtración de información confidencial. Su correcto uso ayuda a evitar la pérdida de datos sensibles, así como posibles consecuencias asociadas, como la pérdida de confianza, daños a la reputación y compromisos legales.

En este informe se propone una política de seguridad orientada a garantizar el uso adecuado de la herramienta de software DLP dentro de la empresa.

2. Clasificación de datos

Para controlar el uso y accesibilidad de los archivos utilizados dentro de la empresa, se propone la siguiente clasificación de datos:

2.1. **Información Pública:** Información generada dentro de la empresa, que puede ser compartida sin causar ningún daño a la organización

2.2. **Información interna:** Documentación y archivos que son de uso exclusivo dentro de un entorno laboral, no debe ser divulgada al público.

2.3. **Información Confidenciales:** Documentación y archivos que solo deben ser accesibles a ciertos trabajadores.

2.4. **Información Crítica:** Documentación y archivos críticos dentro de un entorno laboral, que deben ser protegidos con cautela. La divulgación de esta información puede generar un daño grave a la organización.

3. Acceso y control

De acuerdo con el Principio del Menor Privilegio, el uso de los archivos se gestionará de acuerdo al rol que posee de la siguiente manera:

3.1. Analista

- Permisos para **leer y ejecutar archivos de ofimática**.
- **Sin acceso a la ejecución de programas** sobre el sistema operativo.
- Puede **solicitar instalación de software** mediante tickets, los cuales deben ser aprobados por el **líder de equipo** y el **administrador tecnológico**.
- Acceso a internet **limitado** y regulado por las **políticas del negocio**.

3.2. Líder

- Posee los **mismos permisos que un analista**.
- En caso de requerir nuevo software, debe:
    - **Evaluar la necesidad** junto con los **roles de finanzas** y el **administrador tecnológico**.
    - Aprobar la instalación en su equipo personal o en los de su equipo.
- Acceso a internet **limitado** por políticas del negocio.

3.3. Administrador Tecnológico

- Tiene acceso completo como administrador de sistemas a todos los equipos informáticos.
- Puede **realizar configuraciones e instalaciones de software** en toda la infraestructura.
- Acceso a internet **restringido** según las **reglas del negocio**.

3.4. Finanzas

- Acceso a **software de ofimática**.
- **No puede instalar software ni realizar configuraciones** del sistema operativo.
- Acceso a internet **limitado** conforme a las políticas del negocio.

3.5. Recursos Humanos

- Acceso a **software de ofimática**.
- **Sin privilegios de instalación ni configuración** del sistema operativo.
- Acceso a internet **limitado** conforme a las políticas del negocio.

3.6. Directivos

- Acceso a **software de ofimática**.

- **No se permite la instalación de software ni la modificación del sistema operativo**.

- Acceso a internet **limitado** conforme a las políticas del negocio.

4. Monitoreo y Auditoría

Se implementará una política de monitoreo y auditoría sobre el movimiento de datos dentro de la empresa. Para este proceso será necesario implementar las siguientes herramientas de ciberseguridad:

- **EDR (Endpoint Detection and response):** Este software se instala en los dispositivos finales de la empresa (computadoras, tabletas, teléfonos móviles, etc.) con el objetivo de detectar amenazas en tiempo real. Mediante un gestor de EDR, se podrán administrar los dispositivos de manera centralizada y tener monitoreo y respuesta en tiempo real.
- **SIEM (Security Information and Event Management):** Se implementará una herramienta SIEM (Security Information and Event Management) para centralizar la recopilación y análisis de eventos de seguridad en la red empresarial. Esta solución permitirá identificar patrones anómalos y comportamientos sospechosos en tiempo real, facilitando una respuesta rápida ante posibles incidentes de seguridad.

  Además, se conformará un equipo de trabajo especializado que, con el apoyo del SIEM, podrá realizar investigaciones profundas, priorizar alertas y coordinar acciones de mitigación eficaces.

5. Prevención de Filtraciones

Con el objetivo de fortalecer la protección de la información sensible y prevenir filtraciones no autorizadas, se implementarán las siguientes herramientas complementarias al sistema de Prevención de Pérdida de Datos (DLP):

5.1. **Cifrado de Datos**: Aplicación de técnicas de cifrado para asegurar que la información confidencial permanezca inaccesible a usuarios no autorizados, incluso en caso de acceso físico o digital no autorizado.

5.2. **Control de Accesos y Autenticación Multifactor (MFA)**: Implementación de políticas estrictas de control de acceso y autenticación multifactor para garantizar que solo usuarios autorizados puedan acceder a los sistemas y datos sensibles.

5.3. **Políticas de Uso de Dispositivos y Aplicaciones**: Definición de políticas claras sobre el uso de dispositivos personales y aplicaciones no autorizadas, minimizando riesgos asociados al acceso no controlado a datos sensibles.

6. Educación y concientización

Es primordial que los usuarios que interactúan con los sistemas de información tengan una base sólida de conocimiento sobre seguridad informática, por lo cual:

6.1. **Capacitación y Concientización del Personal**: Se desarrollarán programas de formación continua para empleados, enfocándose en buenas prácticas de seguridad y en la identificación de posibles amenazas, como el phishing.