



4Geeks Academy

Políticas de Seguridad DLP

Por: Juan Cervantes Simón

Introducción a DLP

El data loss prevention es la planificación, así como las tecnologías que permiten monitorear y proteger datos empresariales confidenciales dentro de la organización, de la misma forma que también se previene el robo o divulgación de datos no autorizada, al igual que su pérdida o filtración.

Dentro de la organización el DLP juega un papel muy importante, siendo que en el contexto empresarial actual, la información corporativa es un activo que ha de protegerse con la mayor de las prioridades, siempre tratando de garantizar la confidencialidad, disponibilidad e integridad de los datos tanto como sea posible, protegiendo a la empresa de riesgos como la pérdida de propiedad intelectual, sanciones económicas y costos legales como consecuencia de violaciones de seguridad y/o fuga de datos.

Clasificación de los Datos

La clasificación de los datos que maneja la empresa serán clasificados según su nivel de criticidad siendo más alta cuanto mayor sea el impacto que tiene su pérdida o filtrado para la organización.

➤ **Datos Públicos**

- Esta categoría recoge los comunicados de prensa, material de campañas de marketing e información corporativa de distribución, en definitiva, cualquier dato aprobado por el equipo ejecutivo de la empresa para ser compartido con el público sin restricciones.

➤ **Datos internos**

- En esta clasificación se recogen los organigramas empresariales, manuales internos y procesos operativos de sensibilidad baja cuya filtración podría ocasionar daño considerable a nivel empresarial.

➤ **Datos sensibles**

- Se corresponde con todos los datos personales identificativos del plantel, así como credenciales, datos sanitarios, claves de acceso y datos bajo propiedad intelectual, siendo que su filtración al público podría causar serios problemas a la empresa.

Acceso y Control de los datos

Política de Acceso a Datos

Con objetivo de tener un control preciso sobre los datos y qué personal puede acceder a ellos, se va a seguir el principio de mínimo privilegio, ello conlleva que, para el acceso a la plataforma empresarial, las características a las que tiene acceso el personal serán gestionadas en función de las responsabilidades que requiere su puesto, siendo que si este no tiene acceso directo a información sensible, sólo se permitirá dicho acceso bajo expresa autorización y motivo por el cual se requiere el acceso, esto ayuda a monitorear con precisión el acceso a estos para poder rastrear el origen de filtraciones con mayor agilidad

Revisiones

En cuanto a los permisos otorgados al personal, estos serán revisados periódicamente por el equipo de seguridad de datos, idealmente de forma bimestral o trimestral para *datos sensibles*, y de manera mensual para el caso de los *datos internos*.

Grupos de Responsabilidad

Para que la monitorización sea exitosa, tanto el equipo de seguridad como el departamento de recursos humanos deben de coordinarse para asegurar la integridad de los accesos a la información y, por consiguiente, la seguridad de la misma.

El equipo de seguridad de la información realiza los controles periódicos de verificación de acceso, así como la concesión de los accesos con la correspondiente aprobación de la junta ejecutiva.

Por su parte, el equipo de recursos humanos debe de notificar las altas, bajas, ascensos o degradaciones de los empleados para autorizar, revocar o actualizar permisos según los deberes y responsabilidades de los mismos cambien.

Proceso Operativo Estándar para Accesos

Cuando se requieren modificaciones de cualquier tipo en el acceso a datos por parte del personal, recursos humanos genera un informe indicando la naturaleza del acceso (nuevo empleado, despido, etc), para que tanto el equipo de seguridad como la junta ejecutiva, aprueben o declinen la solicitud, en caso de que se apruebe, el equipo de seguridad realizará las gestiones necesarias según la naturaleza del acceso requerido.

Una vez realizado el cambio en el acceso a los datos, se añaden al registro de auditoría, tanto el cambio en los permisos, como a quién se han otorgado y la fecha de actualización.

Monitoreo y Auditoría

Reglas de Monitoreo

Para que las revisiones de acceso a datos sean completas y precisas, las transferencias de archivos internos y sensibles fuera de la compañía se someterán a monitoreo en tiempo real para evitar revelación de secretos o filtraciones, del mismo modo que también se listarán las detecciones efectuadas de accesos no autorizados a bases de datos o repositorios de archivos que contengan datos sensibles.

Ambas medidas se listarán y, en caso de resultar anómalas ([p.ej.](#) acceso a datos fuera de horario laboral).

Herramientas Recomendadas

Para poder llevar a cabo el monitoreo descrito anteriormente se recomienda el uso de herramientas de *data loss prevention* como Proofpoint o Symantec, adicionalmente también se recomienda el uso de soluciones *SIEM*, [p.ej.](#) IBM QRadar.

Una vez se recaban datos, para agilizar la tarea de generar los registros de auditoría podrían usarse soluciones como el caso de Windows Event Log o la auditoría de SharePoint.

Proceso Operativo Constante

Para la comunicación periódica con el equipo ejecutivo, se elaborarán reportes mensuales con las características e incidentes ocurridos en el mes, así como auditorías por parte de un organismo ajeno cada seis meses para obtener auditorías con las que verificar y cruzar la información con el equipo interno.

Prevención de Filtraciones

Configuración de Infraestructura

Para la prevención de filtraciones de información interna y/o sensible, se procederá al bloqueo y registro de todos los intentos de acceso a contenido no autorizado, así como de intentos de extracción de datos de dispositivos empresariales por medio de dispositivos USB.

Del mismo modo se procederá a la eliminación de cualquier intento de compartir datos sensibles o internos por canales no seguros y/o no autorizados, así como la investigación de posibles filtraciones debido a dicho intento.

En cuanto al control de comportamiento y tráfico de red, se monitorizarán por medio de firewalls y proxys, lo cual permite el filtrado y categorización del flujo de red empresarial.

Cifrado

Para poder mantener la confidencialidad en los datos, y siguiendo con la política zero-trust que se ha descrito anteriormente, se utilizarán cifrados resilientes, como el *AES-256* o *Kyber*, del mismo modo que se usarán cifrados como el *TLS-1.3* para el cifrado de datos en tránsito.

Educación y Concienciación

Capacitación del Personal

Con objetivo de reducir el error humano por desconocimiento o falta de conciencia, se otorgará una capacitación inicial a todos los nuevos empleados, así como al resto del plantel si es que no la han recibido con anterioridad a la elaboración de estas políticas, asimismo se facilitarán programas anuales de actualización en el ejercicio de la seguridad de datos al personal durante toda su estancia en la empresa.

Material de Soporte para el Personal

Para poder apoyar en el ejercicio de la seguridad de datos, se proporcionarán guías al personal en las que vengan descritas buenas prácticas, así como descripciones y clasificaciones de los datos que van a tratar, ampliando este apoyo con campañas de comunicación regular con objetivo de hacer llegar los mensajes clave a todos los departamentos.

Adicionalmente se les dejará a disposición un canal de comunicación con el equipo de seguridad para consultas y/o incidencias.

Responsabilidades del Personal