Protección de datos y cifrado

La protección de datos es fundamental en cualquier sistema de gestión de seguridad de la información (SGSI) avanzado, especialmente en las pymes con recursos técnicos limitados. Este módulo profundiza en estrategias de clasificación y prevención de fugas de información (unidad 1) y en técnicas de cifrado y respaldo (unidad 2). Se explican políticas, riesgos y controles con un lenguaje accesible, ilustrando cada tema con ejemplos prácticos aplicables en entornos de pequeña empresa. Además, se incluyen actividades, un laboratorio guiado con herramientas gratuitas y un caso de estudio integrador en una pyme.

Unidad 1. Clasificación y prevención de pérdidas de datos (DLP)

1.1. Políticas de clasificación y etiquetado

Políticas de clasificación y etiquetado

Clasificar los datos en la empresa implica asignarles niveles de confidencialidad o sensibilidad. Estos pueden identificarse con etiquetas como pública, interna, confidencial o secreta, según el impacto que tendría su divulgación. La clasificación establece quién puede acceder a cada dato y qué controles deben aplicarse, como el cifrado o el acceso restringido.

El objetivo de esta práctica es proteger la información valiosa y evitar accesos no autorizados. En el ámbito hospitalario, por ejemplo, las historias clínicas se consideran «secretas», los datos administrativos de pacientes «confidenciales» y las políticas internas «internas».

Un programa de clasificación bien diseñado debe contemplar varios aspectos: definir categorías claras; capacitar al personal para etiquetar correctamente documentos y correos electrónicos (como anteponer «confidencial» en el asunto); y aplicar controles proporcionales, como cifrar documentos con contenido sensible o bloquear su envío fuera del dominio corporativo.

En las pymes, resulta útil comenzar con un conjunto reducido de categorías (pública, interna y confidencial) y utilizar etiquetas visibles.

Políticas de clasificación y etiquetado de la información en pymes

La clasificación de la información es un proceso fundamental en la seguridad de la información. Consiste en agrupar los datos y activos de la organización según su sensibilidad, valor y los riesgos asociados a su divulgación, modificación o pérdida.

Para llevarlo a cabo, las pymes deben inventariar sus activos de información y aplicar criterios basados en la confidencialidad, la integridad y la disponibilidad requeridas para cada tipo de dato. Una política sencilla puede establecer categorías como «pública» (sin restricciones de difusión), «interna» (accesible solo al personal interno) o «confidencial» (reservada para la dirección o empleados que la necesiten). Estas etiquetas se aplican a documentos, bases de datos y sistemas de información. Al identificar qué información es crítica o sensible, la empresa puede determinar qué datos cifrar, quién puede acceder a ellos y con qué frecuencia realizar copias de seguridad.

A continuación, se presenta un modelo básico de clasificación:

- Información «confidencial». Muy sensible, con acceso restringido.
- Información «interna»: de uso exclusivo para el personal.
- Información «pública»: sin restricciones para su difusión.

Alineación con estándares (ISO, NIST) y normativa

Las buenas prácticas de clasificación deben alinearse con estándares reconocidos. La norma ISO/IEC 27001, que regula los sistemas de gestión de seguridad de la información (SGSI), exige clasificar la información según criterios de negocio y riesgo, con el fin de aplicar controles adecuados. En su anexo A (control 5.12), se recomienda evitar una clasificación excesiva o insuficiente, y considerar siempre los principios de confidencialidad, integridad y disponibilidad. Así, la información destinada al público debe marcarse explícitamente como tal, mientras que los datos altamente sensibles requieren controles más estrictos.

La norma ISO/IEC 27002 refuerza esta idea al establecer, en el control 5.13, que el etiquetado de la información es el procedimiento que vuelve operativa la clasificación mediante la aplicación de las etiquetas definidas a cada activo. Su propósito es evidenciar el nivel de clasificación tanto en las comunicaciones internas como externas, y facilitar la automatización de su gestión.

En el entorno del Instituto Nacional de Estándares y Tecnología (NIST), marcos como NIST SP 800-60 y SP 800-53 instan a categorizar la información en función del impacto que puede tener sobre la confidencialidad, integridad y disponibilidad. En la práctica, esto equivale a establecer esquemas de clasificación de datos.

Además, existen implicaciones legales. En España, la Ley de Secretos Empresariales (Ley 1/2019) exige mantener «medidas razonables de protección» sobre la información confidencial que aporte valor competitivo. Un paso clave consiste en identificar y clasificar los datos que puedan considerarse secretos o confidenciales, definiendo niveles como público, interno, confidencial o secreto, en función del impacto de su divulgación. Esta clasificación facilita el cumplimiento de los requisitos legales y refuerza acuerdos de no divulgación con terceros (non-disclosure agreements).

Por otra parte, el Reglamento general de protección de datos (RGPD) obliga a proteger los datos personales sensibles. Si bien no impone directamente esquemas de clasificación, conocer y catalogar la información permite determinar qué datos deben cifrarse o restringirse

—como los de nóminas o clientes— y así cumplir con las medidas de seguridad establecidas por el reglamento.

Ejemplos concretos en pymes

En una pyme típica, la política de clasificación puede traducirse en casos prácticos. Los registros de nóminas o de pagos suelen clasificarse como confidenciales, con acceso limitado al personal de recursos humanos y a la dirección. El acceso al gestor del sitio web puede restringirse a un pequeño equipo técnico (nivel «interna»), mientras que los folletos comerciales y anuncios se marcan como públicos para su libre difusión. También es habitual etiquetar explícitamente como confidenciales los documentos enviados a asesorías o gestorías, exigiendo cifrado en tránsito. De forma similar, un sistema de planificación de recursos empresariales (ERP) que contiene datos críticos se considera un activo de alta importancia y se protege mediante copias de seguridad frecuentes.

Estas clasificaciones permiten definir medidas prácticas: se otorgan accesos solo al personal necesario, se aplican contraseñas o cifrado a los archivos adecuados, y se gestiona correctamente el ciclo de vida de la información, eliminando o archivando datos obsoletos cuando corresponde. Según lo indicado por INCIBE (2024), resulta fundamental realizar un inventario de los activos de información y clasificarlos conforme al impacto que ocasionaría su pérdida, acceso no autorizado o difusión, aplicando criterios de confidencialidad, integridad y disponibilidad.

Recomendaciones prácticas para pymes de bajos recursos

Para las pymes con recursos limitados, lo fundamental es mantener la simplicidad y adoptar un enfoque pragmático. Se recomienda comenzar con un esquema reducido (por ejemplo, tres o cuatro categorías: pública, interna, confidencial o secreta) y establecer criterios claros para su asignación. Una posible definición sería considerar como «confidencial» los datos de clientes, financieros o estratégicos; como «interna», la documentación operativa; y como «pública», la información divulgada en el sitio web. Además, es importante elaborar un inventario básico de la información, identificando quién es responsable de cada tipo de dato y dónde se almacena.

El etiquetado puede realizarse de forma manual o semiautomática. Algunas opciones incluyen funciones de clasificación disponibles en el software de oficina —como etiquetas en correos electrónicos o plantillas de documentos—, sellos manuscritos en papel o incluso carpetas con códigos de color. Lo esencial es que todo el personal conozca las etiquetas definidas y aplique correctamente la clasificación.

Para facilitar esta tarea, se recomienda asignar la responsabilidad del esquema a una persona o equipo. Los propietarios de la información —como el jefe de contabilidad o el responsable de tecnologías de la información— deben asegurarse de que los datos se clasifiquen correctamente y asumir el entrenamiento del resto del personal.

Asimismo, las pymes pueden apoyarse en medidas de bajo costo: utilizar herramientas gratuitas de cifrado —como GNU Privacy Guard—, funciones nativas de etiquetado en la nube —por ejemplo, Google Workspace o Microsoft 365 ofrecen atributos de confidencialidad—, o soluciones open source de prevención de pérdida de datos (data loss prevention) ligeras. También resulta útil seguir una lista de verificación sencilla. En este sentido, INCIBE (2024) recomienda asegurar la existencia de un inventario actualizado de la información, definir los criterios de clasificación que se aplicarán y etiquetar cada activo de acuerdo con esos criterios.

En la práctica, esto implica que todos los documentos o sistemas críticos lleven la etiqueta correspondiente —de forma manual o digital—, y que se hayan identificado las medidas de seguridad disponibles, como copias de seguridad, cifrado o controles de acceso, para cada nivel de clasificación.

Otra recomendación es apoyarse en marcos de gestión existentes para orientar la implementación. Tomar como referencia los niveles de clasificación propuestos por la norma ISO/IEC 27001 o utilizar plantillas adaptadas a pymes —como las que proporciona INCIBE— puede reducir la carga de diseño. En cualquier caso, la formación y la concienciación del personal son fundamentales. Mediante sesiones breves de capacitación —incluso a través de materiales en línea— se puede lograr que los empleados comprendan la importancia de etiquetar adecuadamente la información y apliquen la política en sus tareas cotidianas.

Buenas prácticas para mantener actualizado el esquema

Un error frecuente es establecer un esquema de clasificación y luego dejarlo en el olvido. Sin embargo, la sensibilidad y el valor de la información pueden variar con el tiempo —por ejemplo, debido a proyectos que pierden relevancia, cambios legales o avances tecnológicos—, por lo que el esquema debe revisarse de forma periódica. Se recomienda actualizar las políticas y

etiquetas al menos una vez al año, o cada vez que se modifiquen la normativa o los procesos del negocio. Durante estas revisiones, es conveniente identificar qué datos nuevos han surgido —como un nuevo producto, base de datos o cliente— y verificar si las categorías existentes siguen siendo adecuadas.

También es recomendable realizar auditorías internas o externas con cierta regularidad para comprobar la aplicación efectiva de la política de clasificación. Una forma de hacerlo es inspeccionando muestras de documentos o registros, para asegurarse de que estén debidamente etiquetados y de que los controles definidos —como accesos, cifrado o copias de seguridad— se estén aplicando correctamente.

Dado que las pymes suelen tener estructuras ágiles, conviene integrar la clasificación de la información en el ciclo de mejora continua. Por ejemplo, al adoptar una nueva tecnología o contratar un servicio, se debe evaluar desde el inicio qué tipo de datos se manejarán y asignarles una etiqueta correspondiente.

Por último, es fundamental mantener la coherencia interna: cada departamento o unidad de negocio debe comprender y aplicar el sistema de clasificación de forma homogénea, evitando divergencias que dificulten el intercambio de información dentro de la organización.

Errores comunes y cómo mitigarlos

Entre los errores más frecuentes al implementar políticas de clasificación y etiquetado en pymes se encuentran los siguientes:

Etiquetas demasiado complejas o poco claras —

Diseñar un esquema con numerosos niveles o nombres confusos desmotiva a los usuarios y dificulta su adopción. Se recomienda simplificar —por ejemplo, con las categorías «pública», «interna» y «confidencial»— y definir cada nivel con ejemplos concretos.

Clasificación excesiva o insuficiente —

etiquetar como «secreta» información que no lo es o, por el contrario, subestimar datos sensibles puede romper el equilibrio entre seguridad y operatividad. La norma ISO/IEC 27001 advierte sobre ambos extremos. Una forma de mitigarlo es vincular cada nivel de clasificación con riesgos claros —por ejemplo, evaluar qué impacto tendría una divulgación indebida— y revisar periódicamente si las clasificaciones continúan siendo adecuadas.

No etiquetar o etiquetado inconsistente —

en ocasiones, por falta de formación o atención, los empleados no aplican etiquetas a los documentos, o lo hacen de forma incorrecta. Para evitarlo, se recomienda automatizar en la medida de lo posible —por ejemplo, configurando que ciertos archivos se guarden automáticamente en carpetas marcadas como «confidencial»— y reforzar la concienciación mediante recordatorios accesibles y frecuentes.

Exceso de trabajo manual —

en pymes con recursos limitados, clasificar manualmente grandes volúmenes de datos puede volverse inviable. En estos casos, conviene adoptar soluciones semiautomáticas, como filtros básicos —por ejemplo, para identificar números de cliente o datos personales— o herramientas gratuitas de etiquetado automático. Invertir en mecanismos que ahorren tiempo —mediante secuencias automáticas o funciones del propio software— permite evitar la sobrecarga operativa.

Falta de gobernanza clara —

si no se asigna una responsabilidad concreta, la clasificación tiende a aplicarse de forma dispersa. Es fundamental definir el rol de propietario de los datos, así como documentar las revisiones realizadas, por ejemplo, mediante registros de auditoría incluidos en una lista de verificación.

Mitigar estos errores implica, en resumen, simplificar el esquema, capacitar al personal y aplicar controles automáticos siempre que sea posible. Una medida efectiva consiste en establecer un procedimiento interno claro que indique cómo se debe etiquetar la información en distintos escenarios, acompañado de pruebas piloto antes de extender la política al conjunto de la organización.

Compartir ejemplos internos —por ejemplo, mostrar cómo debe marcarse un informe financiero— refuerza la comprensión del esquema. También resulta útil revisar las lecciones aprendidas: muchas pymes documentan incidentes en los que la falta de etiquetado fue un factor relevante, lo que permite ilustrar la importancia de este tipo de control.

1.2. Riesgos de fuga y puntos de control

La fuga de datos representa uno de los principales riesgos para cualquier organización. Se entiende por fuga de datos la exposición involuntaria o no autorizada de información sensible o

confidencial a agentes externos o a usuarios sin permisos.

Este tipo de incidentes puede producirse tanto por errores humanos —por ejemplo, enviar un mensaje de correo electrónico al destinatario equivocado— como por ataques maliciosos, como malware o phishing.

Las fugas pueden comprometer datos personales, información financiera, secretos empresariales, propiedad intelectual y otros activos críticos, generando pérdidas económicas, consecuencias legales y daños reputacionales. De hecho, en 2023 se registraron más de 3200 incidentes de violación de datos solo en Estados Unidos, con millones de registros expuestos a nivel mundial (). Por ello, resulta fundamental conocer los canales, vectores, causas y tipos de fuga, con el fin de establecer medidas preventivas eficaces.

La prevención de pérdida de datos (data loss prevention, DLP) engloba las medidas destinadas a evitar que la información sensible salga de la empresa. Las pérdidas pueden producirse a través del correo electrónico, almacenamiento en la nube personal, dispositivos USB, impresiones no autorizadas, entre otros canales.

Los sistemas DLP permiten monitorear, detectar, informar y bloquear intentos de exfiltración. Por ejemplo, un sistema de este tipo puede impedir que un empleado envíe, desde su cuenta corporativa de Gmail, un archivo que contenga datos personales de clientes.

Los puntos de control típicos se ubican en los siguientes lugares:

- el perímetro de red (con firewalls y sistemas DLP en gateways de correo web);
- los dispositivos terminales o endpoints (agentes de DLP instalados en ordenadores que supervisan archivos abiertos o unidades USB insertadas);
- los servidores críticos (como bases de datos con acceso controlado).

Implementar DLP implica definir políticas claras —especificando qué datos se consideran confidenciales— y utilizar tecnologías de monitoreo adecuadas. Como medida de protección,

cualquier intento de transferencia de datos etiquetados como «confidenciales» debería generar una alerta o bloquearse automáticamente.

Estas medidas son fundamentales, ya que en una pyme una sola fuga de datos puede provocar sanciones legales y dañar seriamente la reputación de la organización.

Canales de fuga de datos

Los canales de fuga son los medios o caminos a través de los cuales la información puede salir de la organización. Existen canales físicos, electrónicos y encubiertos:

Medios físicos —

Incluyen impresiones en papel, fotografías de pantallas, extracción de discos duros o memorias USB, mensajes de texto o imágenes de documentos;

Medios electrónicos —

abarcan el correo electrónico, aplicaciones de mensajería —como WhatsApp o Slack—, tráfico web (HTTP, FTP), mensajería instantánea, servicios en la nube, redes sociales y conexiones inalámbricas. Un ejemplo típico es el envío de datos sensibles por correo electrónico sin cifrar a cuentas personales. La prevención de pérdida de datos a nivel de red se encarga precisamente de «supervisar el tráfico de red para detectar y evitar transferencias de datos no autorizadas», con el fin de garantizar que la información sensible no abandone los límites corporativos;

Canales encubiertos —

se trata de vías menos evidentes, como emisiones electromagnéticas (ataques TEMPEST), acústicas (grabaciones), ópticas (fotografías tomadas desde el exterior) o incluso la manipulación de documentos descartados (por ejemplo, búsqueda en contenedores de basura). Aunque menos comunes, estos canales existen y pueden ser aprovechados en ataques dirigidos.

Cada canal implica controles distintos. En los canales físicos, es necesario restringir el acceso a impresoras o salas donde se maneje documentación confidencial. En los canales electrónicos, se aplican filtros de correo electrónico, cortafuegos y sistemas de prevención de pérdida de datos (*data loss prevention*) para inspeccionar el contenido del tráfico de red. Un caso frecuente es el bloqueo automático del envío de archivos críticos a cuentas externas mediante correo electrónico.

Vectores y tipos de fuga de datos

Los vectores de ataque son las formas o caminos específicos que aprovechan los atacantes —o los errores— para provocar una fuga de información. Entre los más comunes se encuentran los siguientes:

Ataques externos (ciberataques) —

Incluyen el acceso no autorizado mediante malware, phishing, vulnerabilidades de software o servidores mal configurados —por ejemplo, un contenedor de almacenamiento en la nube expuesto públicamente—. Estos atacantes suelen robar credenciales o aprovechar brechas tecnológicas para extraer datos;

Amenazas internas —

involucran a usuarios malintencionados o empleados descontentos que filtran información de manera intencional —por ejemplo, copiando datos a un dispositivo USB o fotografiando pantallas—. Este vector resulta especialmente riesgoso porque el usuario tiene acceso legítimo a los datos;

Errores y descuidos humanos —

es el vector más frecuente. Comprende acciones como enviar información al destinatario equivocado, subir archivos confidenciales por error a carpetas públicas, olvidar dispositivos sin protección en espacios comunes o compartir datos en canales no cifrados. Por ejemplo, un empleado que reenvía accidentalmente una hoja de cálculo con datos sensibles;

Canales externos de colaboración —

el uso de servicios en la nube o redes sociales sin políticas definidas puede convertirse en un vector de fuga. Compartir un enlace a un documento privado de la empresa en un grupo externo es un caso típico. Además, los

atacantes suelen valerse de redes sociales, correo electrónico y aplicaciones de mensajería para obtener datos mediante técnicas como phishing o inyección de malware.

Existen diversos tipos de fuga de datos, lo cual permite comprender mejor los vectores más frecuentes. A continuación, presentamos los principales:

Fugas accidentales —

Se producen sin intención, en la mayoría de los casos por error humano. Representan la mayor parte de los incidentes registrados. Un ejemplo habitual es el envío de un mensaje de correo electrónico confidencial a la persona equivocada;

Fugas por malestar interno —

ocurren cuando un empleado frustrado o con intenciones maliciosas filtra información de manera deliberada. Puede copiar documentos a una unidad USB, fotografiarlos o incluso recurrir al dumpster diving (revisión de residuos para recuperar documentos físicos). Este tipo de fuga suele generar daños mayores, ya que quien la comete conoce dónde y cómo se almacena la información más sensible;

Fugas inducidas desde el exterior —

comprenden ataques o manipulaciones maliciosas externas —como phishing, accesos no autorizados o programas maliciosos— que provocan la exfiltración de datos. Un caso típico es un mensaje de correo electrónico con malware que registra las pulsaciones del teclado del usuario;

Fugas por debilidades operativas —

algunos especialistas añaden esta categoría para describir filtraciones involuntarias provocadas por configuraciones incorrectas —por ejemplo, una nube pública sin restricciones de acceso— o procesos mal diseñados;

Ataques dirigidos —

tanto internos como externos, estos casos incluyen situaciones de espionaje, chantaje o extorsión, con un plan deliberado para acceder y extraer información crítica.

En todos los casos, los vectores implicados corresponden a los canales ya descritos: correo electrónico, redes, dispositivos físicos, entre otros. Identificar cuáles son los vectores más probables en cada organización es esencial para diseñar controles de prevención de pérdida de datos adecuados.

Causas de fuga de datos

Las fugas de datos pueden originarse por múltiples causas, que combinan factores humanos, técnicos y organizativos. A continuación, se enumeran algunas de las más frecuentes:

Errores de configuración —

ocurren cuando servicios en la nube están mal configurados —por ejemplo, permisos públicos en un contenedor S3—, servidores carecen de parches de seguridad o las políticas del cortafuegos son demasiado permisivas. Estas condiciones permiten a los atacantes acceder sin grandes obstáculos;

Procesos operativos deficientes —

incluyen la ausencia de procedimientos claros para el manejo de datos o la falta de documentación de procesos clave. Por ejemplo, que los empleados no distingan entre datos públicos y confidenciales, o que no se auditen los envíos masivos. Estas «brechas operativas» pueden exponer información en tránsito debido a fallos logísticos o de comunicación;

Escasa concienciación y capacitación —

se refiere a empleados que desconocen los riesgos asociados a sus acciones —por ejemplo, hacer clic en enlaces sospechosos o utilizar redes inalámbricas públicas sin una red privada virtual (VPN)—. La falta de formación hace que las políticas de seguridad no se apliquen en la práctica. De hecho, se estima que más del 90 % de los incidentes de seguridad tienen origen en el factor humano;

Errores humanos simples —

abarcan situaciones como enviar un mensaje a un dominio equivocado, olvidar un dispositivo portátil con datos sensibles o usar incorrectamente aplicaciones de mensajería. Estos errores suelen deberse a la prisa, el descuido o la falta de conocimiento. La mayoría de las fugas se producen como consecuencia de errores humanos;

Presencia de malware y ataques externos —

se trata de virus, ransomware o ataques de denegación de servicio (DDoS) que buscan extraer o extorsionar mediante datos robados. Por ejemplo, un programa malicioso que analiza automáticamente la carpeta de documentos puede capturar listas de clientes o contraseñas;

Amenazas internas (insider threat) —

involucran a empleados corruptos o exempleados con resentimiento que acceden a información para venderla a la competencia o hacerla pública. Esta causa, deliberada y muchas veces difícil de prever, requiere mecanismos de monitoreo adecuados.

La fuga de datos puede producirse por múltiples causas: un error humano, una mala configuración del sistema o vulnerabilidades del software. Estas causas, a menudo, se combinan. Por ejemplo, un empleado que no actualiza su equipo —dejándolo expuesto— y, además, cae en una campaña de phishing, puede terminar filtrando información sensible. Por este motivo, prevenir las fugas exige reforzar tanto la tecnología como los procesos y la formación del personal.

1.3. Inventario de datos sensibles

El inventario de datos sensibles es un componente fundamental de la seguridad de la información, tal como establece la norma ISO/IEC 27001, que exige la identificación y documentación de los activos de información con el fin de protegerlos adecuadamente.

Para construir este inventario, es necesario:

- identificar los datos sensibles;
- clasificarlos según su importancia y el riesgo que implican;
- asignar a cada activo un responsable interno.

Este inventario permite gestionar los riesgos de seguridad, aplicar controles adecuados —como el acceso restringido o el cifrado— y asegurar el cumplimiento de las normativas vigentes.

Llevar un inventario de datos sensibles implica registrar qué información crítica existe, dónde se almacena y quiénes la utilizan. Esto equivale a inventariar activos de información como bases de datos, archivos, documentos, correos electrónicos y dispositivos que contienen datos relevantes para la empresa.

Según la norma ISO/IEC 27001, este registro es la base para aplicar los controles de seguridad apropiados. Por ejemplo, en una empresa de servicios, el inventario incluiría desde la base de datos de clientes hasta las computadoras portátiles del equipo comercial.

Deben catalogarse los datos personales, financieros, secretos industriales y cualquier otro tipo de información sensible. Un inventario bien mantenido permite priorizar la protección —por ejemplo, cifrar bases de datos críticas— y cumplir con normativas como el Reglamento general de protección de datos (RGPD), la Ley orgánica de protección de datos (LOPD) o el estándar PCI-DSS.

Sin este inventario, una pyme no podría identificar con claridad qué necesita proteger con prioridad.

En la práctica, se puede elaborar mediante hojas de cálculo u otras herramientas sencillas. Se debe listar cada tipo de dato (activo), su ubicación —ya sea en un servidor, la nube o en soporte físico—, su responsable interno y su nivel de clasificación en términos de confidencialidad.

Este registro debe actualizarse de forma periódica, incorporando nuevos activos y eliminando los obsoletos. Así, la empresa mantiene una visión clara de qué información posee y dónde se encuentra, evitando así la existencia de activos huérfanos.

Controles relevantes del Anexo A de la norma ISO 27001:2022

La norma ISO/IEC 27001:2022 incluye, en su anexo A, varios controles directamente relacionados con la gestión de datos sensibles. Entre los más relevantes se encuentran los siguientes:

A.5.9 Inventario de información y otros activos asociados. —

Este control exige que todos los activos de información —así como los activos asociados, como el hardware y el software— sean identificados y documentados en un inventario. Es en este contexto donde se deben reconocer los datos sensibles como parte de la información gestionada;

A.5.13 Etiquetado de la información —

establece que la información debe ser etiquetada conforme a un esquema de clasificación definido por la organización. Este esquema permite distinguir entre información pública, sensible, confidencial o secreta, y facilita su manejo y protección adecuados.

Proceso para crear un inventario de datos sensibles bajo ISO/IEC 27001

El proceso para crear un inventario de datos sensibles se integra dentro de la gestión general de activos de información, conforme a los lineamientos de la norma ISO/IEC 27001. A continuación, se describen los pasos recomendados:

Paso 1

Definir la política de clasificación

Establecer criterios claros para determinar qué se considera información sensible dentro de la organización. Esta política será la base para la posterior clasificación de los activos.

Paso 2

Identificar los activos de información

Elaborar un inventario completo que incluya bases de datos, documentos físicos, sistemas, dispositivos y otros recursos relevantes.

1. Realizar un recorrido por las instalaciones y entrevistar a los responsables de cada departamento para identificar todos los activos y sus recursos asociados.
2. Revisar documentación interna —como informes contables y de recursos humanos— para complementar la lista.

Paso 3

Clasificar los datos

Asignar a cada activo una etiqueta según su nivel de sensibilidad (por ejemplo, pública, interna, confidencial o secreta). La clasificación debe revisarse periódicamente para asegurar su validez y adecuación.

Paso 4

Asignar responsables

Designar un propietario para cada activo, quien será el encargado de supervisarlo durante todo su ciclo de vida.

Paso 5

Documentar los activos

Registrar los activos identificados junto con sus componentes —como bases de datos, almacenamiento, software, entre otros— y mantener actualizada su clasificación y nivel de protección.

Paso 6

Evaluar los riesgos

Analizar los riesgos específicos que pueden afectar la confidencialidad, integridad y disponibilidad de la información sensible. Esto permite identificar amenazas y vulnerabilidades asociadas a los activos críticos.

Paso 7

Implementar controles de seguridad

Aplicar medidas de seguridad proporcionales a los riesgos identificados, tales como controles de acceso, cifrado, segmentación de redes y supervisión continua.

1. Establecer restricciones de acceso basadas en la clasificación de los datos.
2. Proteger la información conforme al riesgo, clasificación y necesidades del negocio.
3. Asegurar el manejo seguro de los activos, incluso al momento de su eliminación.

Paso 8

Cumplir con la legislación

Garantizar que el inventario y su tratamiento permitan el cumplimiento de normativas de protección de datos, como el Reglamento general de protección de datos (RGPD), que exige medidas específicas para la gestión de información sensible.

Paso 9

Mantener y revisar

Actualizar el inventario y las clasificaciones de forma periódica, adaptándolos a los cambios en los procesos, sistemas o información gestionada por la organización.

Beneficios de mantener un inventario de datos sensibles

Contar con un inventario actualizado de datos sensibles aporta ventajas clave en la gestión de la seguridad de la información. Entre los principales beneficios se destacan los siguientes:

- **Gestión de riesgos.** Permite identificar las amenazas a la seguridad de la información y aplicar medidas de mitigación eficaces;
- **Cumplimiento normativo:** facilita el cumplimiento de regulaciones como el Reglamento general de protección de datos (RGPD) y otras normas sectoriales;
- **Control y eficiencia operativa:** contribuye a una respuesta rápida ante fallos, pérdidas o incidentes de seguridad, reduciendo tiempos de reacción y mejorando la toma de decisiones;
- **Generación de confianza:** demuestra a clientes, socios y partes interesadas que la organización protege adecuadamente la información que gestiona;
- **Ventaja competitiva:** disponer de buenas prácticas alineadas con estándares como ISO/IEC 27001 puede ser un factor diferenciador en procesos de contratación, ya que muchas empresas exigen estas garantías a sus proveedores.

1.4. Telemetría mínima y reporte

Para detectar fugas o accesos no autorizados, se recomienda recolectar una telemetría mínima de seguridad. Esto implica habilitar los registros de auditoría en los sistemas clave, tales como:

- registros del servidor de correo electrónico;
- registros del cortafuegos o del proxy corporativo;
- alertas de soluciones antivirus o sistemas de detección y respuesta en endpoints (EDR);
- registros del sistema de prevención de pérdida de datos (DLP);
- controles de acceso a servidores que almacenan datos sensibles.

El objetivo no es generar grandes volúmenes de datos, sino recopilar únicamente lo necesario para identificar comportamientos anómalos. Por ejemplo, resulta útil registrar intentos fallidos de envío de archivos etiquetados como «confidenciales» o accesos a bases de datos fuera del horario laboral.

Una buena práctica consiste en configurar alertas automáticas o resúmenes diarios cuando se detectan incidentes relacionados con DLP. A partir de ello, se pueden elaborar reportes simples, que incluyan:

- gráficos de eventos bloqueados;
- listas de incidentes investigados;
- acciones correctivas aplicadas —por ejemplo, un mensaje de correo electrónico bloqueado por contener un documento clasificado—.

Este enfoque permite al equipo de seguridad centrarse en la reducción de riesgos, en lugar de revisar registros de manera manual. Incluso en pymes con recursos limitados, tareas sencillas —como revisar alertas por correo electrónico o implementar una solución ligera de gestión de eventos de seguridad (SIEM), como Wazuh— pueden ser de gran utilidad para informar a la dirección sobre eventos relevantes.

Puntos de control en una arquitectura DLP

Para enfrentar el riesgo de fuga de información, las organizaciones implementan soluciones de prevención de pérdida de datos (data loss prevention, DLP). Un sistema DLP no consiste en un único dispositivo, sino en un conjunto de controles aplicados en diversos puntos críticos donde los datos podrían abandonar el entorno seguro.

La función de DLP es detectar y evitar filtraciones mediante la inspección del contenido y el análisis contextual de los datos que se transmiten por mensajería, circulan por la red, se utilizan en dispositivos finales o permanecen en reposo (almacenados).

A continuación, se describen los puntos de control más habituales:

DLP de red (perímetro o gateway) —

protege los datos en tránsito a través de la red corporativa. En este punto se monitorea el tráfico saliente —por ejemplo, mediante proxy HTTP/FTP, SMTP de correo electrónico o mensajería instantánea—, buscando contenido sensible. Un gateway DLP analiza los mensajes y archivos salientes, bloqueando o cifrando aquellos que contienen información crítica. Por ejemplo, se puede impedir que un mensaje de correo electrónico sea enviado si incluye un número de tarjeta de crédito o datos personales. También se controlan otros puntos como los puertos de red (FTP, SMB, etc.), donde el DLP puede detener la transferencia. Según Trend Micro, el DLP de red asegura «que la información sensible no abandona los límites de la organización». Un ejemplo común de control en este punto es la configuración de reglas en el cortafuegos o en el proxy para detectar patrones de datos —como expresiones regulares asociadas a números de seguridad social o palabras clave empresariales— y activar alertas o bloquear el tráfico;

DLP en dispositivos finales (endpoint) —

supervisa los datos en uso en computadoras portátiles, de escritorio o dispositivos móviles, antes de que abandonen el equipo. Se implementa mediante un agente o software cliente instalado en los dispositivos finales, que controla las acciones locales. El agente DLP puede interceptar intentos de copiar archivos a unidades USB, enviar información mediante aplicaciones no autorizadas o imprimir documentos confidenciales. Permite definir políticas detalladas, como impedir la copia de datos sensibles a dispositivos externos o restringir la impresión a impresoras seguras. Como ilustra el caso de Acronis, es habitual bloquear de forma selectiva los puertos USB, conexiones Bluetooth o el uso del portapapeles cuando contienen información sensible. En resumen, el DLP de endpoint «controla los accesos a los datos y su uso directamente en los dispositivos finales, evitando la filtración de datos desde estos equipos». Este punto de control es clave, ya que es donde el usuario interactúa directamente con la información, y el agente puede incluso auditar o cifrar los datos al salir del equipo.

DLP de correo electrónico y mensajería —

si bien podría considerarse parte del DLP de red, en muchos casos se implementa como un módulo específico. Este control supervisa el contenido de los correos electrónicos —y sus archivos adjuntos— tanto entrantes como salientes. Se definen políticas que determinan qué tipo de información puede enviarse al exterior. Por ejemplo, se puede bloquear el envío de mensajes que contengan listados de clientes o datos financieros. Este tipo de control suele aplicarse directamente en el servidor de correo o en un gateway SMTP. Además, existen soluciones DLP para plataformas de colaboración —como Slack, Microsoft Teams o redes sociales corporativas— que permiten limitar la publicación de información confidencial. Acronis menciona específicamente la capacidad de estos sistemas para bloquear archivos adjuntos o restringir conversaciones que incluyan contenido sensible.

DLP en la nube (cloud DLP) —

dada la creciente adopción de servicios en la nube —como Microsoft 365, Google Workspace, Dropbox o Salesforce—, muchas organizaciones requieren extender la protección a estos entornos. El DLP en la nube supervisa las aplicaciones SaaS y los servicios de almacenamiento en línea, detectando posibles filtraciones de datos. Por ejemplo, puede evitar que documentos confidenciales se suban a cuentas personales de Google Drive o que aplicaciones internas transfieran datos a servicios no autorizados. Estas soluciones suelen integrarse mediante intermediarios de seguridad de acceso a la nube (CASB) o interfaces de programación de aplicaciones (API), lo que permite inspeccionar archivos y mensajes para aplicar políticas de bloqueo o cifrado. Según Trend Micro, el DLP en la nube garantiza que «los datos sensibles en aplicaciones de nube y servicios de almacenamiento permanezcan seguros».

DLP de datos en reposo (data discovery) —

supervisa la información sensible almacenada en servidores de archivos, bases de datos o repositorios locales. A diferencia de los controles que vigilan datos en tránsito o en uso, este módulo verifica el contenido ya existente en el sistema. Un DLP en reposo escanea carpetas compartidas, discos duros y copias de seguridad en busca de información confidencial no cifrada. Por ejemplo, se puede utilizar OpenDLP —una herramienta gratuita— o secuencias de comandos personalizadas para detectar documentos que contengan información personal identificable (PII), con fines de auditoría interna. Este tipo de escaneo permite descubrir riesgos potenciales,

etiquetar archivos según su sensibilidad y clasificar datos críticos. Aunque algunos sistemas empresariales de DLP ya incluyen esta función, una pyme puede replicarla con búsquedas por patrones —mediante grep, scripts o herramientas de indexación— para aplicar una clasificación básica.

Otros puntos de control específicos —

además de los anteriores, existen controles aplicables a elementos concretos, como impresoras seguras —que evitan que documentos confidenciales queden olvidados—, bloqueos de capturas de pantalla —para impedir la toma de imágenes de contenido sensible— o mecanismos de supervisión en dispositivos móviles, especialmente en entornos de tipo Bring Your Own Device (BYOD), mediante herramientas de gestión de dispositivos móviles (MDM). Asimismo, algunos sistemas avanzados de DLP incluyen funcionalidades basadas en identidad o comportamiento —como User and Entity Behavior Analytics (UEBA) o módulos de insider threat— que detectan patrones de uso anómalos, como accesos masivos a información fuera del comportamiento habitual del usuario.

En suma, una arquitectura típica de DLP distribuye sus puntos de control en distintos niveles del entorno organizacional: las fronteras externas e internas de la red —como correo electrónico o gateways web—, los dispositivos finales —ordenadores y móviles—, la nube y el almacenamiento interno.

Cada punto de control intercepta diferentes canales:

- la red supervisa el tráfico de internet y los correos electrónicos;
- el endpoint controla puertos locales y aplicaciones;
- la nube protege las aplicaciones SaaS y el almacenamiento en línea;
- el reposo cubre discos locales y servidores de archivos.

La filosofía de DLP se centra en vigilar y controlar los canales de comunicación de datos dentro y fuera de la organización. El objetivo es alcanzar una visibilidad global de dónde se encuentran los datos sensibles y evitar cualquier intento no autorizado de fuga.

Buenas prácticas para pymes con recursos limitados

Las pequeñas y medianas empresas suelen contar con menos personal técnico y presupuesto restringido, por lo que deben centrarse en prácticas sencillas pero eficaces para reducir el riesgo de fuga de información. A continuación, se presentan algunas recomendaciones que no requieren grandes inversiones:

Políticas claras y clasificación de datos —

definir qué tipos de datos se consideran sensibles —como información personal identificable (PII), datos financieros o propiedad intelectual— y establecer normas básicas para su manejo. Es recomendable contar con una tabla de clasificación de la información y ofrecer capacitación mínima para que todo el personal conozca las reglas. Esta concienciación, aunque de bajo costo, previene muchos errores derivados del desconocimiento; por ejemplo, casos en que un empleado no sabía que determinada información era confidencial.

Mínimos privilegios y gestión de accesos —

aplicar el principio de menor privilegio, asegurando que cada persona acceda solo a los datos necesarios para su función. Usar cuentas de usuario individuales, establecer políticas de contraseñas robustas y fomentar el uso de gestores de contraseñas para evitar claves débiles o repetidas. Además, activar la autenticación multifactor (2FA) en todos los servicios críticos —correo corporativo, redes privadas virtuales (VPN), aplicaciones de gestión—. Así, incluso si se compromete una contraseña, no será suficiente para acceder a los datos.

Actualizaciones y parches al día —

mantener actualizados los sistemas operativos, navegadores, antivirus y demás software de uso habitual. Las aplicaciones desactualizadas representan vulnerabilidades explotables. Se recomienda programar actualizaciones automáticas o revisarlas semanalmente. También deben actualizarse el firmware de los dispositivos de red —como el router o el cortafuegos—. Contar con un entorno actualizado reduce significativamente los riesgos de infección por malware y la posibilidad de exfiltración de datos.

Cifrado de dispositivos y comunicaciones —

aunque no implica adquirir software adicional, los sistemas operativos como Windows y macOS ofrecen funciones de cifrado integradas, como BitLocker y FileVault. Es recomendable activarlas en computadoras portátiles y dispositivos que almacenen información sensible, ya que protegen los datos en caso de pérdida o robo del equipo. Asimismo, se debe utilizar HTTPS/TLS en los servidores web y en los servicios de correo electrónico. Cuando se acceda desde ubicaciones externas, se sugiere emplear una red privada virtual (VPN). El cifrado garantiza que, incluso si alguien obtiene el contenido, no pueda leerlo sin la clave correspondiente.

Restringir medios removibles y canales riesgosos —

mantener un registro actualizado de los dispositivos extraíbles autorizados, como unidades USB o discos duros externos, y aplicar medidas de control. Una práctica sencilla es bloquear los puertos USB no esenciales o exigir el cifrado de los dispositivos que se conecten. Además, es importante controlar el acceso a servicios externos como redes sociales o plataformas de almacenamiento en la nube. Si la empresa no utiliza WhatsApp Web o una cuenta corporativa de Dropbox, conviene bloquear estos sitios desde el cortafuegos o informar claramente que deben usarse únicamente los canales oficiales.

Antivirus y monitoreo básico —

antivirus gratuito o económico y habilitar funciones de monitoreo del sistema operativo. Por ejemplo, activar los registros de eventos (event logs) de Windows para rastrear accesos inusuales a archivos o conexiones sospechosas. También existen herramientas gratuitas de detección y respuesta en el endpoint (EDR) o sistemas de detección de intrusos en host (HIDS), como OSSEC o Wazuh, que permiten registrar cambios en archivos y procesos anómalos. Aunque estos registros no previenen directamente, facilitan la detección temprana de incidentes.

Formación y cultura de seguridad —

dedicar al menos una charla breve o documento básico sobre riesgos de seguridad puede marcar la diferencia. Informar al personal sobre phishing, manejo responsable de datos sensibles y buenas prácticas —como no escribir contraseñas en papel, cerrar sesión en los dispositivos o usar VPN fuera de la oficina— refuerza la prevención. El factor humano continúa siendo el eslabón más débil, por lo que capacitar al equipo —por ejemplo, mediante simulacros de phishing con herramientas gratuitas— resulta fundamental.

Copias de seguridad periódicas —

aunque no evitan la fuga de datos, las copias de seguridad aseguran la recuperación ante incidentes como ransomware o eliminaciones accidentales. Se recomienda realizar copias de seguridad automáticas y frecuentes, almacenando versiones cifradas en ubicaciones seguras —como una segunda nube o un disco externo—. Así, incluso ante pérdidas de datos o cifrado malicioso, la empresa podrá recuperar su información crítica.

En resumen, para una pyme, las buenas prácticas son simples pero deben aplicarse con constancia: mantener cuentas seguras (contraseñas y autenticación multifactor), sistemas actualizados y cifrados, limitar el uso de dispositivos y redes externas, formar al personal y realizar copias de seguridad con regularidad. Estas medidas no requieren grandes inversiones y constituyen la base sobre la que puede construirse una futura implementación de controles DLP más avanzados.

Actividad práctica: análisis de riesgos y canales de fuga

A continuación, se propone una actividad sencilla. Imagina la estructura de una pequeña empresa, con aproximadamente diez empleados, que presenta la siguiente situación:

- cuenta con un servidor de archivos interno donde almacena documentos financieros y de clientes;
- utiliza correo corporativo;
- los equipos tienen acceso a internet;
- se emplea un servicio en la nube —como Google Drive— para compartir algunos archivos con personas externas.

Consigna

A continuación, se propone una actividad sencilla. Imagina la estructura de una pequeña empresa, con aproximadamente diez empleados, que presenta la siguiente situación:

- **Qué datos se filtran.** Por ejemplo, bases de datos de clientes, reportes financieros o propiedad intelectual.
- **Por dónde podrían salir:** correo personal, unidad USB extraviada, carga en la nube pública, mensaje en una aplicación de mensajería, etc.
- **Quién sería el agente de la fuga:** error interno, empleado malintencionado o atacante externo.
- **Qué medidas preventivas podría tomar la empresa:** por ejemplo, cifrar los documentos antes de compartirlos, restringir el uso de dispositivos USB, habilitar el envío de correos solo a ciertos dominios, entre otras.

Objetivo de la actividad

Identificar riesgos reales —fugas accidentales, internas o externas— a partir de un caso práctico, y reflexionar sobre cómo mitigar cada canal de fuga. Este ejercicio te ayudará a visualizar qué controles de prevención de pérdida de datos (DLP) serían relevantes. No es necesario usar herramientas informáticas: puedes realizar el análisis en papel, pizarra o en una hoja de cálculo.

Por ejemplo, un escenario posible sería «un gerente envía por error el informe financiero (archivo de Excel) a un cliente que no debía recibirlo».

- **Causa:** error humano
- **Prevención:** cifrar los archivos sensibles, verificar los destinatarios antes de enviar el correo y aplicar reglas que alerten cuando se intenta enviar datos financieros a direcciones externas.

Otro escenario podría ser: «un empleado frustrado copia datos de clientes en un pendrive sin cifrar».

- **Prevención:** restringir el uso de puertos USB, realizar auditorías sobre el uso de dispositivos extraíbles y revocar permisos en caso de detectar riesgos.

Realizar este ejercicio entrena la identificación de flujos de datos críticos y puntos débiles de control.

Laboratorio guiado

Como práctica de laboratorio, se puede utilizar una solución open *source* para simular el monitoreo de fugas de datos. Se propone, por ejemplo, instalar Snort (un IDS de código abierto) para detectar flujos no autorizados. A continuación, se presenta una guía breve:

Paso 1

Instalar Snort

En un ordenador o máquina virtual con Linux (por ejemplo, Ubuntu), ejecutar:

sudo apt-get update && sudo apt-get install snort

Durante la instalación, configurar en modo NIDS y definir la red local (por ejemplo, 192.168.1.0/24).

Paso 2

Configurar una regla de detección simple

Editar el archivo /etc/snort/snort.conf o crear un archivo de reglas personalizadas (por ejemplo, /etc/snort/rules/local.rules). Añadir una regla que busque contenido sensible. Por ejemplo, para detectar un número de tarjeta de crédito ficticio:

alert tcp any any -> any any (msg:"Datos sensibles detectados"; content:"4111111111111111"; sid:1000001; rev:1;)

Esta regla genera una alerta si en cualquier flujo TCP aparece la cadena «4111111111111111» (número de tarjeta de prueba).

Paso 3

Iniciar Snort

Ejecutar sudo systemctl restart snort. Verificar que el servicio se haya iniciado correctamente con snort -V.

Paso 4

Generar tráfico de prueba

En otro equipo de la misma red, simular el envío de datos. Por ejemplo, usar netcat (nc) para transmitir un archivo de texto que contenga ese número de tarjeta al equipo con Snort:

- En el servidor con Snort, nc -l -p 12345 > /dev/null (esto abre el puerto 12345 y descarta lo recibido).
- En el cliente, echo "4111111111111111" | nc [IP-del-servidor] 12345. Snort debería detectar la cadena y generar una alerta en sus registros.

Paso 5

Observar alertas

Revisar el archivo /var/log/snort/alert y confirmar que aparece una línea como la siguiente:

[**] [1:1000001:1] Datos sensibles detectados [**]

Esto indicaría que Snort captó correctamente la fuga simulada.

Interpretar la práctica

Aunque se trata de un ejemplo muy simplificado, permite observar cómo un sistema DLP de red —implementado aquí con Snort— puede identificar contenido sensible en el tráfico. La empresa podría ampliar esta funcionalidad mediante reglas más complejas (por ejemplo, expresiones regulares para números de identificación, direcciones de correo electrónico, etc.) o ejecutar Snort en modo inline para bloquear el tráfico en tiempo real.

De forma alternativa, si se desea enfocar en datos en reposo, es posible utilizar un script sencillo en Python o bash que busque patrones en archivos locales. Por ejemplo, un script que recorra carpetas compartidas y aplique expresiones regulares para detectar números de identificación o palabras clave confidenciales. Aunque no se trata de un «laboratorio» con interfaz gráfica, este ejercicio permite aprender cómo automatizar la inspección de datos estáticos, emulando la funcionalidad de un DLP en reposo.

El objetivo del laboratorio es demostrar, mediante herramientas gratuitas —como Snort o scripts—, el principio de monitoreo de datos sensibles. Snort y otras herramientas IDS/IPS de código abierto (como Security Onion o Suricata) pueden configurarse fácilmente para realizar simulaciones de fuga. No requieren licencias, solo algo de configuración, y permiten comprender cómo funcionan los puntos de control en la red y la detección de filtraciones.

CONTINUAR

Unidad 2. Cifrado y resguardo

El cifrado de datos es un proceso que transforma la información legible (texto plano) en un código ilegible (texto cifrado), con el fin de protegerla contra accesos no autorizados. Para ello, se emplea una clave que permite cifrar y descifrar los datos; sin esta clave, la información resulta inservible para cualquier persona no autorizada.

Su objetivo principal es garantizar la confidencialidad, la integridad y la privacidad de la información, tanto durante su almacenamiento como en su transmisión.

Características

A continuación, se presentan las principales características del cifrado:

- **Proceso.** Convierte datos en formato legible en un formato que parece aleatorio, utilizando algoritmos matemáticos.
- **Función:** protege la confidencialidad, integridad y autenticidad de los datos.
- **Mecanismo:** requiere una clave secreta o contraseña para revertir el proceso y recuperar la información original.
- **Uso:** se aplica tanto a los datos en tránsito (transmisión) como a los almacenados (en reposo).
- **Ejemplos históricos:** incluso antes de Internet, ya se utilizaban métodos como el cifrado César para proteger las comunicaciones.

- **Ciencia detrás:** el arte y la ciencia del cifrado y descifrado se conocen como criptografía.

Conceptos clave

A continuación, se definen los principales conceptos relacionados con el proceso de cifrado:

- **Texto plano (o no cifrado).** Datos en su formato original y legible.
- **Texto cifrado:** datos transformados e incomprensibles sin la clave adecuada.
- **Algoritmo de cifrado:** fórmula matemática o conjunto de reglas utilizadas para realizar el proceso de codificación.
- **Clave de cifrado:** valor secreto (similar a una contraseña) necesario para cifrar y descifrar los datos. Sin la clave correcta, descifrar la información es extremadamente difícil.
- **Descifrado**: proceso inverso al cifrado, que convierte el texto cifrado nuevamente en texto plano mediante la clave correspondiente.

Tipos principales de cifrado

Existen dos tipos principales de cifrado, clasificados según el uso de las claves:

- **Cifrado simétrico.** Utiliza una única clave secreta tanto para cifrar como para descifrar la información. Es más rápido y eficiente para cifrar grandes volúmenes de datos. Requiere que ambas partes (emisor y receptor) compartan de forma segura la misma clave, lo cual puede representar un desafío logístico. Un ejemplo común es el algoritmo AES (Advanced Encryption Standard), que es el estándar actual.

- **Cifrado asimétrico (o de clave pública):** emplea un par de claves relacionadas matemáticamente: una clave pública (que se puede compartir libremente) y una clave privada (que debe mantenerse en secreto). Lo que se cifra con una clave solo puede descifrarse con la otra, y viceversa. Se usa habitualmente para la transferencia segura de claves simétricas, la autenticación y las firmas digitales, como en los certificados SSL/TLS de los sitios web seguros. Un ejemplo de este tipo es el algoritmo RSA.

Beneficios y uso

El cifrado de datos cumple un papel fundamental en la seguridad de la información. Entre sus principales beneficios se destacan los siguientes:

- Proteger la información confidencial (datos financieros, registros médicos, propiedad intelectual) del acceso no autorizado.
- Garantizar la privacidad en las comunicaciones en línea (correo electrónico, mensajería, navegación web).
- Proteger los datos almacenados en dispositivos (discos duros, teléfonos móviles, bases de datos) frente a robos o pérdidas.
- Asegurar el cumplimiento de regulaciones sobre protección de datos.

2.1. Casos de uso y herramientas *open source*

El cifrado es fundamental para proteger datos sensibles. Se aplica en múltiples situaciones: proteger correos electrónicos, archivos en disco, comunicaciones web, respaldos y más. Afortunadamente, existen diversas herramientas gratuitas y de código abierto útiles para pymes.

Un caso común es el uso de GnuPG (GPG), una implementación libre de cifrado de clave pública (PGP) que permite cifrar correos y archivos. Con GPG, cada empleado puede generar un par de claves pública y privada: la pública se comparte para recibir información cifrada; la privada, protegida por contraseña, permite descifrar los datos. Por ejemplo, una pyme puede utilizar GPG para cifrar correos de contabilidad con datos bancarios o para proteger un archivo de cliente antes de subirlo a la nube.

Otra herramienta es VeraCrypt, que permite crear contenedores cifrados o cifrar discos completos. De este modo, un disco externo o una laptop robada no revelarán su contenido sin la contraseña. Para sitios web y aplicaciones, Let's Encrypt proporciona certificados TLS gratuitos, y OpenSSL (herramienta de línea de comandos) permite generar y gestionar certificados propios.

En resumen, GPG, VeraCrypt, OpenSSL y otras herramientas similares ofrecen soluciones robustas sin coste: GPG para archivos y correo, VeraCrypt para discos y dispositivos extraíbles, OpenSSL y Let's Encrypt para comunicaciones seguras, OpenSSH para cifrado de túneles, y soluciones de respaldo como Duplicati o Restic, que integran cifrado. Las pymes pueden adoptarlas fácilmente sin licencias comerciales, accediendo a estándares ampliamente utilizados.

2.2. Cifrado en tránsito (TLS) y en reposo

El cifrado en tránsito protege los datos cuando se transmiten a través de redes, como Internet, redes internas, correos electrónicos o conexiones VPN. Por su parte, el cifrado en reposo protege los datos almacenados en discos, bases de datos o dispositivos físicos.

Un caso de uso cotidiano en pymes es habilitar HTTPS en su página web o portal de clientes, para que la información —como formularios o inicios de sesión— viaje cifrada. Esto se logra mediante TLS (Transport Layer Security), que cifra la comunicación entre el navegador del usuario y el servidor, garantizando la confidencialidad e integridad de los datos. Además del uso en sitios web, TLS se aplica también en el envío de correos electrónicos (SMTP con STARTTLS), conexiones VPN corporativas y transferencias de archivos.

En cuanto al cifrado en reposo, se utiliza para proteger archivos y bases de datos que se encuentran almacenados. Por ejemplo, una pyme puede activar el cifrado de disco en laptops corporativas usando herramientas como BitLocker o VeraCrypt, o habilitar el cifrado a nivel de base de datos, ya que muchas soluciones modernas permiten cifrar tablas o columnas al momento de escribir los datos. El objetivo es claro: si un atacante accede físicamente al medio de almacenamiento —como un disco robado o una nube mal configurada—, los datos no deben ser legibles sin la clave correspondiente.

El cifrado en reposo es una recomendación explícita en estándares como ISO 27001 e ISO 27002, y resulta especialmente relevante para proteger datos personales o financieros. En la práctica, una pyme debería cifrar sus servidores de archivos sensibles, aplicar cifrado a sus respaldos y utilizar TLS o SSL para todo acceso remoto.

2.3. Gestión de claves y rotación

La gestión de claves criptográficas es un componente fundamental para garantizar la seguridad del cifrado. Esto incluye todo el ciclo de vida de las claves: su generación, uso, distribución, renovación o rotación y destrucción.

Por ejemplo, en una infraestructura de clave pública (PKI) —como en los certificados TLS— se define quién emite los certificados, cómo se protegen las claves privadas y con qué frecuencia deben renovarse. En una pyme, se pueden aplicar prácticas sencillas pero eficaces: generar claves con algoritmos robustos (por ejemplo, RSA de 2048 bits o superior), almacenar las claves privadas en hardware seguro o al menos en sistemas con acceso restringido, y rotarlas periódicamente (por ejemplo, cambiar los certificados TLS o las claves de cifrado de disco cada uno o dos años).

La renovación de claves reduce el riesgo de que una clave comprometida siga siendo válida indefinidamente. Las políticas de gestión de claves deben establecer quiénes son los responsables, dónde se almacenan de forma segura (por ejemplo, en un módulo de seguridad de hardware o en un gestor de credenciales) y cómo se respaldan esas claves.

Si la organización cuenta con un sistema de gestión, existen herramientas gratuitas como HashiCorp Vault (de código abierto) u OpenSSL para generar, almacenar y revocar claves. Lo importante es tener un plan documentado: cada vez que se apruebe un nuevo proyecto —como la implementación de una VPN— debe contemplarse la emisión de nuevas claves y su futura renovación.

Según la norma ISO 27002, es recomendable definir fechas de activación y desactivación de claves para reducir los riesgos. En resumen, no basta con cifrar: es imprescindible asegurar que las claves utilizadas estén bien protegidas y se cambien con regularidad para mantener la confidencialidad.

2.4. Pruebas de restauración (backups)

Un plan de respaldo solo es eficaz si se realizan pruebas periódicas de restauración. Se recomienda aplicar la regla 3-2-1: al menos tres copias de los datos (incluyendo el original), almacenadas en dos medios distintos, y una copia ubicada fuera del sitio principal. Por ejemplo: los datos principales en el servidor local, una copia en un NAS interno y otra en un servicio de almacenamiento en la nube.

Además, ante amenazas actuales como el ransomware, se aconseja mantener al menos una copia inmutable y comprobar que las copias no presenten errores.

No obstante, lo más importante es verificar que esas copias se puedan recuperar. Cada cierto tiempo (mensual o trimestral), se debe simular un fallo y realizar una restauración en un entorno de prueba. Esto permite confirmar que los archivos no están corruptos y que el proceso de recuperación funciona correctamente.

Tal como recomiendan las buenas prácticas definidas en normas como ISO/IEC 27002, es fundamental probar periódicamente la restauración de los respaldos, para garantizar que los datos estén íntegros y que el procedimiento de recuperación funcione correctamente.

En el caso de las pymes, existen herramientas gratuitas como Duplicati, Restic o BorgBackup que permiten realizar respaldos cifrados y almacenarlos en la nube o en discos externos. El laboratorio de este módulo incluye ejemplos prácticos para configurar estas herramientas de forma sencilla. Ante un incidente real —como un ataque de ransomware—, la diferencia entre una interrupción temporal y una pérdida crítica de datos radica en tener respaldos funcionales. Las pruebas regulares aseguran que la empresa pueda recuperarse y seguir operando con normalidad.

Actividades prácticas

- **Ejercicio de clasificación**

  Define categorías de datos (por ejemplo: Pública / Interna / Confidencial) y clasifica ejemplos de información en tu empresa ficticia (como contratos, correos de clientes, manuales internos, datos financieros, etc.). Luego, anota qué controles aplicarías en cada nivel (por ejemplo: cifrado, acceso restringido).

- **Simulación DLP**

  Haz una lista de posibles vías de fuga de información en tu organización (correo, USB, nube, redes sociales). Para cada canal, propone al menos dos controles mitigantes (por ejemplo: bloquear Gmail externo, monitorear el uso de USB, usar DLP en correo) y explica

- **Inventario de datos**

  Elige tres tipos de datos críticos para una pyme (por ejemplo: datos de clientes, nóminas de empleados, diseños de productos). Realiza un inventario indicando dónde se almacena cada tipo de dato, cuál es su nivel de clasificación y quién es responsable. Luego imagina un cambio hipotético (nuevo empleado, datos antiguos legados, etc.) y actualiza la lista según ese cambio.

- **Cifrado de documentos**

  Usa GnuPG (o Kleopatra / GPG4Win) para generar un par de claves pública/privada. Cifra un archivo de texto, envíatelo cifrado a ti mismo o a un compañero, y luego descífralo. Verifica cómo crear, importar y utilizar claves

públicas y privadas para asegurar un correo o documento.

- **Respaldo cifrado**

  En el laboratorio, configura un respaldo usando Duplicati o Restic hacia un disco externo o un servicio de nube (Google Drive, Dropbox, etc.). Practica la restauración de archivos específicos desde esa copia de seguridad y verifica la integridad de los datos restaurados.

Caso de estudio integrador: Clínica SaludTotal

Clínica SaludTotal es una pequeña clínica médica con 10 empleados. Maneja historiales clínicos (datos muy sensibles), información administrativa de pacientes y facturación. Para proteger sus datos, clasifica la información en cuatro categorías:

- **Secreta:** historias clínicas
- **Confidencial:** datos de facturación
- **Interna:** procedimientos internos
- **Pública:** información de difusión general

La pyme implementa controles básicos de prevención de pérdida de datos (DLP): impide el envío de correos fuera del dominio con adjuntos clasificados como «Secreta» y monitorea el uso de dispositivos USB en los equipos. Además, cifra los discos de las computadoras que almacenan historiales mediante VeraCrypt, y utiliza GPG para cifrar los correos que contienen resultados de laboratorio. La transferencia web, que permite el acceso remoto del personal médico, está protegida con TLS usando certificados gratuitos de Let’s Encrypt.

Cada madrugada se ejecuta un respaldo automático cifrado con Restic, siguiendo la regla 3-2-1: se crean copias en un servidor NAS local y en Google Drive, una de las cuales es inmutable.

Mensualmente, el equipo técnico prueba la restauración de varios historiales desde los respaldos para asegurarse de que el proceso funciona correctamente.

Gracias a este enfoque combinado —clasificación de la información, controles DLP en canales críticos, cifrado en tránsito y en reposo, y verificación continua—, SaludTotal logra prevenir fugas de datos personales y cumplir con las normativas sanitarias vigentes.

En una ocasión, por ejemplo, un empleado casi envía por error un historial clínico a una dirección de correo equivocada. El sistema DLP lo bloqueó automáticamente y alertó al administrador, quien pudo intervenir a tiempo. Asimismo, al simular un ataque de ransomware, se comprobó que los datos podían recuperarse correctamente gracias a las copias cifradas de seguridad.

Este caso muestra cómo una pyme, incluso con recursos limitados, puede implementar políticas claras, aprovechar herramientas gratuitas y mantener procesos de verificación regulares para proteger información crítica de forma eficaz.

Laboratorio guiado: herramientas gratuitas para DLP y cifrado

En el laboratorio final se guiará al estudiante en configurar un entorno práctico, usando solo software libre o servicios gratuitos.

Entre otras actividades: instalar y configurar un DLP ligero (por ejemplo, reglas de auditoría de Windows o un proxy con inspección SSL), generar certificados TLS con OpenSSL y Let's Encrypt en un servidor local, usar VeraCrypt para crear un volumen cifrado en un USB, y montar un respaldo cifrado con Duplicati. Se demostrará cómo automatizar respaldos seguros hacia la nube y cómo simular fallos para probar restauraciones. También se explorará un ejemplo básico de gestión de claves con OpenSSL o Vault (generar un CA interna y firmar certificados). El laboratorio no requiere inversión; todas las herramientas son gratuitas y de código abierto, facilitando su adopción en pymes pequeñas.

CONTINUAR

Referencias

Comisión Europea. (2016). Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 20 respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protecci uri=CELEX%3A32016R0679

Ley 1 de 2019. Secretos empresariales. 20 de febrero de 2019.

Instituto Nacional de Estándares y Tecnología. (2008). Guía para mapear tipos de información y sistemas de inform Publication 800-60, Volumen 1, Revisión 1). https://csrc.nist.gov/publications/detail/sp/800-60/vol-1-rev-1/final

Instituto Nacional de Estándares y Tecnología. (2013). Controles de seguridad y privacidad para sistemas de inform 800-53, Revisión 4). https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final

Organización Internacional de Normalización & Comisión Electrotécnica Internacional. (2022). ISO/IEC 27001:202 protección de la privacidad – Sistemas de gestión de seguridad de la información – Requisitos. https://www.iso.org/st

Organización Internacional de Normalización & Comisión Electrotécnica Internacional. (2022). ISO/IEC 27002:202 protección de la privacidad – Código de prácticas para controles de seguridad de la información. https://www.iso.org/

Instituto Nacional de Ciberseguridad de España [INCIBE]. (2024). Clasificación de la información – Política de segu https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/2024/Clasificaci%C3%B3n%20de%20inform

Secureframe. (2024). 65 shocking data breach statistics for 2024. https://secureframe.com/es-es/blog/data-breach-st

CONTINUAR