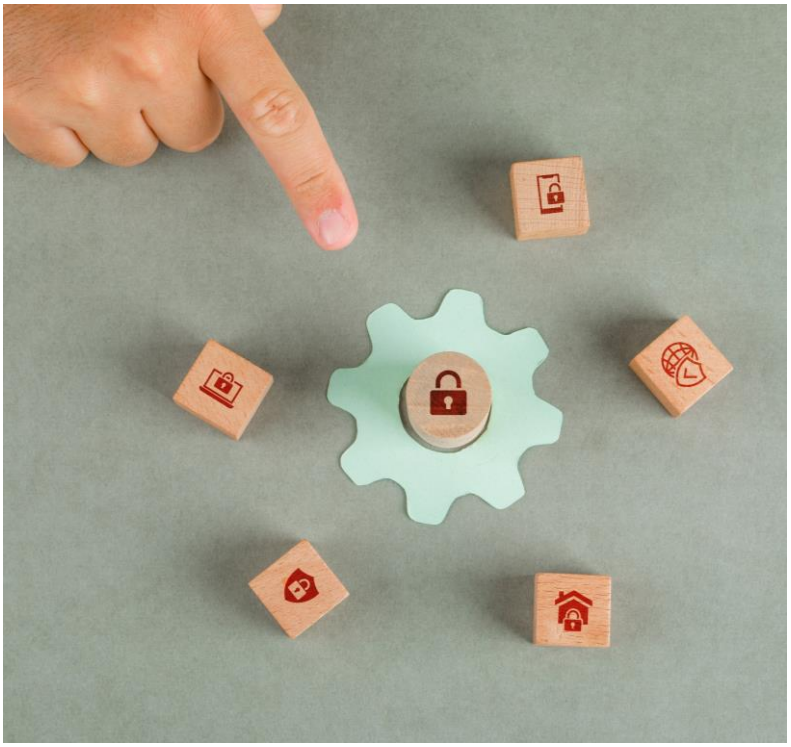

CLASIFICACION DE LA INFORMACION, DLP E IRM

Seguridad de la información

ABSTRACT

El Grupo de Seguridad de la asociación AUTELSI viene generando informes y guías de seguridad de la información. En esta ocasión, se analiza y propone lo que supone clasificar la información en los entornos empresariales y seguir controlando su acceso una vez que un documento ha "abandonado" la Organización (ya no está almacenado en sus sistemas).

Grupo de Calidad y Seguridad (AUTELSI)

Octubre 2024

Datos e información el núcleo de la empresa, en el núcleo de la ciber protección. La información en el centro de la toma de decisiones empresariales y por tanto en el foco de la ciber protección

Introducción.

En la Seguridad de la Información o, como ahora nos gusta llamarla dada la elevada superficie de exposición de los sistemas de información a internet, en la ciberseguridad, nos ocurre como con tantas otras cosas en la vida que a veces, por la inercia, perdemos el foco de lo que es verdaderamente importante. Habitualmente, pensamos más en proteger los sistemas que tratan la información que a la propia información; identificamos de forma univoca la protección de los sistemas con la protección de la información y por tanto dejamos una laguna cuando los documentos, por ejemplo, abandonan nuestros sistemas y consecuentemente cuando ya no podemos ejercer el control a través de los mismos.

La información es la base sobre la que debe cimentarse la toma de decisiones empresariales y el normal desenvolvimiento de las operaciones de negocio. La información puede tratarse sobre diferentes soportes; por ejemplo, en papel o en formato digital.

La información digital, puede ser almacenada en modo estructurado (Bases de Datos) o no estructurada (ficheros individuales que responden a documentos de textos, hojas de cálculo, presentaciones o imágenes, entre otros formatos).

Cada información o conjunto de esta, ya esté almacenada en Bases de Datos o en ficheros, debe estar clasificada para que sepamos como tratarla (recogerla, compartirla, almacenarla, copiarla o borrarla, por citar algunas de las acciones que podemos realizar con esta). Aunque la clasificación de la información no protege de por sí la documentación sensible, sí es un paso importante que facilita posteriormente adecuar su protección, trazabilidad y control.

La información puede clasificarse atendiendo a sus propiedades de seguridad; es decir, respecto a la confidencialidad, la disponibilidad e integridad. Al objeto del presente documento nos centraremos en la información albergada en documentos no estructurados, la protección de su confidencialidad, la clasificación atendiendo a la misma y los controles o medidas de seguridad para garantizar su correcta protección.

Es obvio que no toda la información que maneja una Organización es confidencial, así como que tampoco toda es pública. En este punto también debería ser obvio que no clasificarla, nos aboca a que, de forma práctica, aunque no consciente, determinada información confidencial sea tratada como pública y por tanto no confidencial, poniendo así en riesgo las operaciones y decisiones estratégicas.

Aunque en el siguiente apartado, “Conceptos”, del presente documento específicamente discriminaremos entre datos e información, a lo largo del resto del documento y salvo que se indique de forma expresa nos referiremos con el término información tanto al concepto propiamente dicho de información como al de datos. Debemos también indicar que en este apartado introduciremos el concepto de control de seguridad de la información y sus mecanismos (Clasificación, DLP e IRM) asociados a la entrega/compartición de la información.

El objeto del presente documento.

Partiendo de que todas las organizaciones generan y manejan en mayor o menor medida información sensible que se debe proteger y que está almacenada en diferentes ubicaciones y que pueden ser accedidas por diferentes personas (usuarios) y con capacidades de acceso diferentes (editar, leer, imprimir, entre otras), el presente documento busca describir los conceptos asociados a la protección de la información digital, albergada en documentos digitales no estructurados, a través de su clasificación de su confidencialidad y del control de seguridad.

Esta protección deberá ser desarrollada por cada Organización mediante una serie de controles de tipo personas, procesos y productos; o lo que es lo mismo:

- Organizativos -estrategia, estructura y recursos humanos-,
- Normativos y procedimentales --Políticas, normas internas, procesos, procedimientos y metodología. -
- Técnicos -herramientas, software y productos-

Los proyectos de clasificación de la información son complejos y requieren de disciplina, rigurosidad, implicación y complicidad del personal, pues la tecnología ayuda (y mucho) pero en esta disciplina primero es la voluntad de la Organización de ver la necesidad y querer proteger y su capacidad para llevar a cabo esta empresa.

Conceptos

Información vs dato

Un dato es un hecho, una observación o una medida que se recopila o se registra. Es una entidad que se utiliza para describir algo y es una colección de valores. Por ejemplo, el número de empleados en una empresa, la edad de una persona o el precio de un producto son todos datos.

Por otro lado, la información se refiere a la interpretación y el significado que se extrae de los datos. La información se produce a partir de la organización, el análisis y la interpretación de los datos. Por ejemplo, la información obtenida a partir de los empleados en una Organización puede ser el promedio de edad de los empleados, la tasa de absentismo o la distribución de género.

En resumen, los datos son entidades discretas y objetivas, mientras que la información es subjetiva y se deriva de la interpretación y el análisis de los datos. Los datos por sí solos no tienen significado, pero cuando se procesan y se interpretan, pueden proporcionar información valiosa y significativa.

Los datos y la información pueden existir de diversas formas:

- Cualquier combinación de palabras, números o imágenes que constituyen un registro.
- Registros físicos o electrónicos, incluyendo correos electrónicos, mensajes instantáneos, notas grabaciones de voz o de vídeo, diapositivas y notas escritas.
- Almacenados en reposo o estando en tránsito sobre una red, verbal en una conversación e incluso por teléfono, o enviada por correo postal o entregada en mano.

Ciclo de vida de la información

El ciclo de vida de la información se refiere a las diferentes etapas que atraviesa la información a lo largo de su vida útil, desde su creación hasta su eliminación.

El ciclo de vida de la información puede incluir las siguientes etapas:

- Creación: La información es creada en un formato específico (si bien posteriormente puede ser transformado a otro formato).
- Almacenamiento: La información es almacenada en un lugar seguro y accesible.
- Uso o procesamiento o tratamiento o transformación: La información es utilizada para cumplir con un propósito específico.
- Mantenimiento: La información es actualizada o modificada para asegurar su precisión y relevancia.
- Distribución o transmisión: La información es compartida con aquellos que la necesitan.
- Retención: La información es retenida para cumplir con las leyes y regulaciones aplicables, así como con las necesidades de la Organización.
- Eliminación: La información es eliminada cuando ya no es necesaria o cuando se cumplen los plazos de retención.

Cada etapa del ciclo de vida de la información puede requerir diferentes prácticas de gestión de la información, como la protección, la clasificación, la gestión de versiones y la eliminación segura. La gestión efectiva del ciclo de vida de la información puede ayudar a asegurar la

precisión, la integridad y la disponibilidad de la información, así como cumplir con las leyes y regulaciones aplicables.

A lo largo del ciclo de vida de la información, ésta puede tener que ser clasificada de distintas formas. Por ejemplo, los resultados del ejercicio fiscal de una empresa antes de su difusión pueden tener una clasificación más alta, en lo que respecta a confidencialidad, que cuando se hacen públicos esos resultados.

Dueño de la información

El dueño o responsable de la información es la persona, cargo o autoridad responsable de determinar el valor de la información (evaluándola) para la Organización, conforme a la metodología y normas que sean de aplicación para tal actividad y en última instancia es el responsable de establecer o aprobar los controles de seguridad de la información en su generación, clasificación, recopilación, procesamiento, divulgación, eliminación o borrado. Como es obvio, se ayuda en estas tareas de protección en la gobernanza y la gestión de la seguridad.

Evaluación (valoración) de la información.

La valoración de la información se realiza respecto a la perdida de sus propiedades de seguridad; la confidencialidad, la disponibilidad y la integridad. Esta valoración puede verse influenciada por las obligaciones legales o por las necesidades de la propia Organización.

Clasificar (marcar) vs asignar la clasificación

Clasificar la información es el hecho de marcarla con su clasificación correspondiente, conforme a la valoración que se haya realizado. Esta acción la suele realizar normalmente el usuario que crea o genera el activo, si bien a veces se puede realizar de manera automática, por ejemplo, cuando un sistema o aplicación produce siempre un tipo (clasificado) de información. Mientras que asignar la clasificación viene determinado por el dueño o responsable de la información, quien de manera predeterminada establece que la información, en base a los criterios establecidos, debe ser clasificada con un cierto nivel.

Por tanto, podríamos definir que la clasificación de la información es el proceso de organizar la información en categorías que faciliten su utilización de un modo racional y seguro en términos de requisitos de la organización y de tecnología.

Si nos enfocamos en seguridad TIC, la información se etiqueta según su nivel de sensibilidad, lo que facilita la búsqueda, el seguimiento y la protección de la información confidencial. De esta manera, se contribuye significativamente a la gestión de los riesgos, el cumplimiento normativo y una adecuada seguridad de la información.

Para que la clasificación de la información se efectiva y eficaz, las categorías deberán ser simples de modo que su aplicación y uso sea asumible por la organización y sus empleados. Sin embargo, para su posterior protección, es importante tener en cuenta también el contexto y necesidad de difusión. Bloquear la salida de la Organización de toda documentación marcada confidencial, puede provocar fricciones cuando es necesario compartir documentación confidencial con terceros.

Identificación

Para una buena clasificación de la información, ésta deba ser identificada correctamente, e inventariada por el dueño o responsable de la información.

La identificación puede ser manual o automática; por ejemplo, atendiendo a patrones o palabras clave, o a través de algoritmos de aprendizaje automático e inteligencia artificial. Generalmente, la clasificación automática de la información viene a ayudar (que no a resolver por sí misma) la problemática inicial que toda Organización que adopta la decisión de clasificar la información se encuentra: ¿Qué hacer con toda la información ya generada y almacenada que no está clasificada? Casi todas las organizaciones que emprenden este camino, llegan a la misma conclusión: deben buscar aquella información que cumple unos patrones y clasificarla; por ejemplo, podemos establecer una regla en una herramienta de descubrimiento, conforme a la coincidencia con determinados patrones, como puede ser que contenga datos de carácter personal, marcando los ficheros (clasificación) que contengan coincidencias. ~~e incluso.~~ Incluso se podría llegar a establecer a partir de cuantas coincidencias se clasificaría de un modo determinado.

Obligación o requisito legal

Existen ciertas regulaciones o leyes que obligan a tener la información clasificada, con el objeto de que ésta quede restringida a las personas o grupos correspondientes.

Citaremos por ejemplo la información de carácter personal en el Reglamento General de Protección de Datos y en la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales, el Esquema Nacional de Seguridad, la directiva NIS2 para los operadores (entidades esenciales o importantes) o la Ley de secretos oficiales.

El descubrimiento e identificación de información puede relacionarse no sólo con el tipo de datos que contiene el documento, sino por ejemplo al tipo de regulación a la que afectan estos datos; por ejemplo, si se descubren datos de tarjetas de crédito en un documento, éste puede inventariarse como “datos financieros y medios de pago” pero también como “PCI” ya que su pérdida podría tener repercusiones en esta regulación tan estricta para organizaciones que trabajan en la industria del pagos con tarjetas. Esta identificación puede ayudar además a determinar el nivel de clasificación y sus posteriores medidas de protección.

Necesidad estratégica y táctica de la Organización

Las Organizaciones deben determinar con criterios estratégicos y tácticos las “zonas” de confidencialidad en las que quiere dividir el acceso a su información (por ejemplo, en muy confidencial, confidencial, uso interno y uso público), siempre que la referida Organización no esté sujeta a determinada legislación que determine la clasificación a emplear.

Un ejemplo de legislación en la que se concrete la clasificación es la Ley de Secretos Oficiales y normativa derivada, que clasifica la información en cuatro grados: secreta, reservada, confidencial y difusión limitada. Asimismo, el Esquema Nacional de Seguridad la califica como ‘uso oficial’ cuando la información tiene algún tipo de restricción en su manejo debido a su sensibilidad y confidencialidad; esta calificación tan simple se complementa con el nivel de valoración asociado a la misma en las cinco dimensiones de la seguridad que contempla en ENS (confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad), asignándoles el valor BAJO, MEDIO o ALTO según corresponda

Adicionalmente hay que tener en cuenta que no es viable mantener la confidencialidad exclusivamente mediante una clasificación y unas restricciones basadas en las mismas pues un determinado documento confidencial "A" podríamos establecer que lo podría consultar el USU1 y el usuario USU2, mientras que un documento "B" también confidencial, por su naturaleza e interés, sólo lo podría consultar USU2. Es en este punto dónde toma entidad el concepto Control de Seguridad de un documento, dotándonos de una mayor granularidad. Podemos, por ejemplo, asignar para cada uno de esos documentos diferentes derechos a los diferentes usuarios mediante herramientas de Gestión de Derechos de la Información [en inglés Information Rights Management (IRM)].

En este punto, otros datos de contexto como el tipo de regulación, los grupos de usuarios o dominios a los que va dirigida la información, pueden ayudar a establecer los Controles de Seguridad más adecuados para mantener la confidencialidad evitando fricciones en su gestión por parte de la Organización.

Control de seguridad

Con una visión amplia de la protección del dato, los controles de seguridad que pueden aplicarse a los soportes y a la información son muy diversos y si bien pueden tener diferentes denominaciones según el marco de seguridad que tomemos como referencia en esencia cubren lis mismos aspectos. Si nos fijamos en el RD 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS) y lo tomamos como referencia, vemos que en los controles mp.si, soportes de información y mp.info, protección de la información da como relación los siguientes:

- Mp.si: Marcado de soportes, Criptografía, Custodia, Transporte y Borrado y destrucción.
- Mp.info: Datos personales, Calificación de la información, Firma electrónica, Sellos de tiempo, limpieza de documentos y copias de seguridad.

En este trabajo, reducimos esa visión amplia de la protección y nos centramos en el control que se debe ejercer atendiendo a la taxonomía de la información y consecuentemente a la clasificación a través del marcado de la información y en especial a la compartición/manejo de información. En este contexto el dueño o responsable de la información debe establecer el grado de control para los distintos tipos de clasificaciones de la información. Este control puede ejercerse en relación con la distribución, el nivel de acceso, la posibilidad o no de imprimir o incluso las medidas que se deben adoptar para imprimir, entre otros.

Aquí aparecen dos términos de seguridad habitualmente utilizados en este contexto; DLP e IRM.

DLP (Data Loss Prevention)

DLP por sus siglas en inglés correspondientes a Data Lost Prevention (Prevención de perdida de datos) es un conjunto de herramientas y procesos que se utilizan para garantizar que los datos sensibles no se pierdan, se usen indebidamente o los usuarios no autorizados accedan a ellos. A pesar de esta definición abierta, el DLP suele enfocarse en la protección de la información para que no "salga" en forma de brecha o revelación no autorizada información de la Organización al exterior. El descuido en el manejo y publicación de la información, así como el trabajo con terceros son fuentes de pérdidas de datos. Con la clasificación y la implementación de reglas de seguridad asociadas a la misma (DLP) la información debería ser entregada, aunque haya terceros implicados, sólo a las personas con autorización; principalmente cuando el trabajo colaborativo con otros entes y colaboradores externos está mu delimitado. EL concepto de DLP está firmemente asociado al de clasificación de la Información.

Para establecer medidas de seguridad efectivas en el ámbito del DLP es crítico tener el contexto en el que se mueven los datos. Por ejemplo, generar reglas en el perímetro de la organización que bloqueen la salida de cualquier documentación clasificada como sensible puede suponer fricciones en el uso para los usuarios, que realmente necesitan compartir información sensible con un tercero (ej. Bufete de abogados).

IRM (Information Rights Management)

Es una solución. La tecnología IRM hace referencia a la Gestión de Derechos de la Información, y fue pensada para facilitar que no se acceda, sin la debida autorización, a información sensible.

La protección acompaña al documento tanto si está en la propia red como si se encuentra en la red de un tercero (cliente proveedor, etc.), incluso si se encuentra en la nube (Ej. Azure, AWS, Google Workspace, Box, Dropbox, etc.) o en un dispositivo móvil. Puede controlar quién accede al documento y con qué permisos (ver, editar, imprimir, copiar y pegar, etc.). Puede ver el detalle de accesos al documento, y si alguien ha intentado acceder sin permisos. Si alguien que tenía acceso deja de colaborar, pueden bloquearse los documentos para que estos sean inaccesibles por ese usuario o por cualquiera.

Para ello, utiliza controles de seguridad que con independencia de si la información sigue en activos de la empresa o se encuentra fuera de la empresa, permite un "control remoto" que facilita seguir gestionando quién, cómo y con qué capacidades accede a la información en todo momento.

Gracias a su tecnología pueden establecer un periodo de tiempo concreto al acceso de los documentos, o bien revocarlo en cualquier momento; es decir, cuando lo decidan, podrán eliminarlo y todo el que lo haya recibido ya no podrá visualizarlo, aunque el usuario antes autorizado se lo haya descargado a un equipo externo a la Organización.

Se puede asignar un control de seguridad a un documento "A" por el que el USU1 podrá leerlo, editarlo, copiarlo e imprimirlo, mientras que el USU2 sólo tendrá derechos para leerlo y no podrá imprimirlo, editarlo ni copiarlo.

Para resumir las ventajas de la **protección centrada en los datos** podemos considerar:

- La protección viaja con los datos, con independencia de donde se almacene o desplace.
- Se dispone de completa trazabilidad de los datos, dejando traza de quién accede, cuándo, con qué permisos, así como si alguien intenta acceder sin permisos o desde una subred no permitida por la organización.
- Control de acciones sobre un documento, al permitir establecer permisos granulares sobre la información (visualización, modificación, impresión o copia, etc.).
- Permite responder en tiempo real frete a una posible fuga, permitiendo establecer limitaciones de tiempo de acceso a documentos, o revocar el acceso a los datos cuando se haya decidido que alguien no debe volver a acceder a los mismos. En caso de que se tengan dudas de si una determinada información está en riesgo, podrán revocarse accesos en tiempo real, ya sea a un documento concreto o a todos los documentos protegidos por una determinada política de protección.
- Sencillez de uso, ya que los documentos protegidos pueden viajar por cualquier medio. Se utilizan las aplicaciones habituales para abrirlos y pueden seguir almacenándose tal y como se hace con los ficheros no protegidos. Las soluciones IRM (como CARLA del CCN) no persiguen bloquear las posibles vías de salida de información de la red interna, sino que la información salga debidamente protegida y bajo control, lo que permite

seguir utilizando el email corporativo, la nube u otros medios para compartir la información.

Se muestra a continuación como las soluciones IRM ayudan a cumplir con las disposiciones de los marcos normativos de ciberseguridad. A modo de ejemplo lo concretaremos con algunas medidas de seguridad el Anexo II del ENS:

- [op.acc.2] Requisitos de acceso. Se protegen los recursos del sistema y la documentación crítica, con mecanismos que impiden su utilización, salvo a las entidades que disfruten de derechos de acceso suficientes. Los privilegios de acceso pueden diferenciarse por usuario o grupo de usuarios y con un control granular de permisos (ver, editar, copiar y pegar, etc.), independientemente de la ubicación de la información, incluso en dispositivos móviles.
- [op.exp.8] Registro de la Actividad. Se dispone de un registro de auditoría que identifica al usuario que ha accedido a un documento crítico, permisos, fecha y hora, tipo de evento (acceso realizado, desprotección, acceso bloqueado, etc.), etc.
- [op.exp.3] Protección de la Cadena de Suministro. Es complejo controlar el nivel de seguridad de información que se cede a la cadena de suministro. Con soluciones IRM, es posible mitigar el riesgo de pérdida o fuga de información, ya que la documentación viaja protegida a través de una política de protección marcada por la organización y que se aplica incluso aunque la documentación estuviere en un proveedor perteneciente a la cadena de suministro de la organización. Si finaliza la relación contractual, la información cedida queda inaccesible con independencia de donde se encuentre.
- [op.nub.1] Protección de Servicios en la Nube. Independientemente del servicio de nube contratado, si éste se utiliza para almacenar información sensible, IRM hace que la documentación lleve una capa de seguridad adicional independiente de la seguridad de la nube. De esta forma, tener acceso a la nube no significa necesariamente tener acceso a un contenido sensible regido por una política que viaja con la información. Esto permite que una brecha de seguridad en la nube no tenga porqué suponer una pérdida o exfiltración de datos de la Organización.

- [mp.eq.3] Protección de los dispositivos portátiles. La documentación viaja protegida independientemente de que el puesto de trabajo sea local, dispositivo móvil o se utilice almacenamiento extraíble como puede ser un ‘pendrive’. Si el dispositivo se pierde o ha sido robado, la documentación sensible habrá quedado cifrada, teniendo incluso la posibilidad de revocar accesos. No se está hablando necesariamente de cifrar el disco, sino de proteger mediante mecanismos transparentes de cifrado solo aquella documentación considerada como sensible.

- [mp.com.2] Protección de la confidencialidad. Aunque se esté trabajando de forma remota vía VPN (lo que implica un canal de comunicaciones cifrado) con IRM es adicionalmente el propio documento el que asimismo está protegido mediante mecanismos de cifrado transparente, garantizando doblemente la protección de la confidencialidad en las comunicaciones ante el supuesto caso de interceptación de las mismas.
- [mp.com.3] Protección de la integridad y de la autenticidad. Las soluciones IRM incluyen en los documentos protegidos datos firmados electrónicamente que, caso de que se intentaran alterar para comprometer la integridad, el documento quedará inutilizado. Además, se garantiza que quien ha protegido la documentación es un usuario autenticado/verificable y que quien puede acceder al contenido está también autenticado.
- [mp.si.1] Marcado de soportes. IRM permite proteger la información, etiquetándola mediante mecanismos de cifrado, aplicando controles de uso (sólo ver, editar, etc.), e incluyendo, entre otros elementos, metadatos que indiquen que se trata de información

protegida. Además, tales controles permiten incluir “Marcas de agua digitales” indicando al usuario que está trabajando con información protegida.

- [mp.si.2] Criptografía, [mp.si.3] Custodia, [mp.si.4] Transporte. Más allá de cifrar el dispositivo extraíble, USB, etc., IRM protege los ficheros independientemente de dónde se encuentren. Esto permite que si la documentación se traslada a un soporte tipo pendrive o memoria USB viaje y se almacene etiquetada y protegida.
- [mp.si.5] Borrado y destrucción. Las soluciones IRM permiten una “destrucción lógica” de la documentación contenida en cualquier dispositivo. Es posible inhabilitar el acceso a la misma garantizando que, aunque el dispositivo se conecte o instale en otro equipo, el acceso a esta documentación quede inhabilitado.
- [mp.info.1] Dato personales. Con IRM todos los datos personales incluidos en ficheros no estructurados pueden ser protegidos controlando quién accede, cuándo, con qué permisos, y dejando una auditoría completa de accesos o intentos de accesos bloqueados a la información.
- [mp.info.2] Calificación de la Información. Con soluciones IRM es posible proteger de forma automática documentación con un nivel determinado de calificación (USO OFICIAL o USO NO OFICIAL). Asimismo, puede protegerse en base al máximo nivel de la información que contiene (nivel BAJO, MEDIO o ALTO). Por ejemplo, ante un documento calificado como USO OFICIAL, el administrador puede establecer políticas de seguridad de forma que cuando el fichero se abra, guarde, o almacene en un equipo en red, nube, etc., éste se proteja de forma automática con el nivel de protección adecuado a la calificación del mismo.
- [mp.s.1] Protección del correo electrónico. IRM permite la protección de la información distribuida por medio de correo electrónico en lo que respecta a los documentos adjuntos. Es posible monitorizar accesos al contenido, limitarlo a determinados permisos (sólo ver, etc.) y permite revocar el acceso a emails y adjuntos, aunque hayan sido reenviados y estén en manos de un tercero.

Diferencias entre DLP e IRM

- IRM: permite que el documento esté protegido, aunque salga de la organización, e incluso pueden cambiarse las acciones permitidas. Las que pueden llevarse a cabo por parte de cada usuario son controladas en la gestión.
- DLP: permite reforzar las políticas de acceso y tratamiento de la información, automatizando y reduciendo la responsabilidad del usuario final. El control se apoya en el contenido de la documentación, el control de los repositorios, o lugares de almacenamiento, y medios de transmisión de la información dentro de un sistema o de los sistemas de la Organización.

Clasificación.

Si nos enfocamos en seguridad TIC, la información se etiquetan según su nivel de sensibilidad, lo que facilita la búsqueda, el seguimiento y la protección de la información confidencial. De esta manera, se contribuye significativamente a la gestión de los riesgos, el cumplimiento normativo y una adecuada seguridad de la información.

Para que la clasificación de la información se efectiva y eficaz, las categorías deberán ser simples de modo que su aplicación y uso sea asumible por la Organización y sus empleados.

A título de ejemplo y a fin de ir visualizando conceptos, podríamos decir que la empresa ACME decide establecer cuatro categorías principales. Las cuales podrían ser:

- USO CONFIDENCIAL: información que, de hacerse pública, supone para la Organización riesgo legal, incumplimiento normativo, perjuicios a clientes, pérdidas económicas y desventajas competitivas frente a la competencia.
- USO RESTRINGIDO: información que, si se hace pública, supone un riesgo potencial para el funcionamiento de la organización.
- USO INTERNO: información no confidencial, pero no es de acceso público.
- PUBLICA: información a la que todas las personas dentro y fuera de la organización tienen acceso.

Esta categorización básica es un ejemplo y en la práctica nos podemos encontrar que incluso manteniendo estas etiquetas y siendo cuatro los niveles, otra Organización considere confidencial no como el nivel más alto sino por detrás de restringido. Es decir, existen infinidad de variantes y especificidades en función del tipo de Organización, siendo esta quién en su normativa interna y/o procedimientos correspondientes deberá fijar los criterios, niveles, etiquetas y descripción (además de otros ítems que iremos desarrollando).

Categorías y Criterios de un Esquema de Clasificación de la Información. Metodología de implantación

Necesidad de una clasificación para su correcta protección

La información es uno de los activos principales de cualquier Organización y como tal, tenemos que protegerla adecuadamente. Pero no todas las informaciones son iguales ni tienen el mismo valor, ni están sometidas a los mismos riesgos ni a las mismas obligaciones contractuales o legales

Contar con esta clasificación conlleva los siguientes beneficios a la Organización:

- Mejora la eficacia y la eficiencia de la protección de la información, al establecer criterios objetivos conforme a su sensibilidad, valor, criticidad.
- Mejora la accesibilidad y la eficiencia organizativa de la información.

Tanto la norma ISO 27001:2022 como la NIST* y el RD 311/2022 (ENS), recomiendan disponer de una clasificación (o calificación) de la información para asegurarla en base a su criticidad y riesgo determinado. Estas normas adicionalmente desaconsejan tratar todos los datos de la misma manera. Puede consultarse en el Anexo 1 información complementaria al respecto.

La taxonomía como fuente de categorías y criterios de clasificación

Un esquema de clasificación de la información es una "**taxonomía**" de la información que gestiona una organización: es decir, un proceso para la identificación de la información que está accesible o en poder de esta organización, que identifica las distintas tipologías y/o categorías de información existentes, los distintos atributos que tiene cada pieza de información, y como cada pieza de información requiere de una distinción y de un tratamiento específico en función de las categorías y atributos aplicables a la misma.

Una definición menos formal y más directa se estructura en el reconocimiento de lo que hace un momento hemos expresado: que no todas las informaciones son iguales ni tienen el mismo valor, ni están sometidas a los mismos riesgos ni a las mismas obligaciones legales. Es decir, que se pueden identificar "**atributos"** asociados a la información que puede tomar distintos "**valores**" en cada pieza de información en función de "**criterios de identificación**" para asegurar que cada pieza de información se protege adecuadamente en función del valor de esos atributos. Por lo tanto, habrá que determinar cuáles son los posibles valores que puede tener una información para determinar **la forma de tratamiento adecuado** de los datos que comparten los mismos atributos.

Los esquemas de clasificación de información pueden pues ser diversos y específicos de cada organización, en función de los atributos de la información que la organización determine como más relevantes, el número de posibles valores que la organización determine para estos atributos y los criterios que se establezcan para asignar dicho valor, y las medidas de protección que aplique en cada caso.

Así, no hay una clasificación de la información estándar o una tipología única. Hay esquemas de clasificación en dos, tres, cuatro o más categorías. Se pueden apoyar en atributos como la confidencialidad de esta información, el daño por pérdida, el daño por revelación, la relevancia para ciertas funciones, etc. Todos ellos son viables. Incluso hay casos de esquemas de clasificación de la información no obvios como las leyes de protección de datos y más en concreto la antigua LOPD (Ley Orgánica 15/1999).

A modo de referencia en este capítulo se describen algunos de los esquemas de clasificación más utilizados. Para cada uno de ellos se indican los atributos que analiza, los valores que pueden tener y los criterios que se aplican. En base a ellos, se compararán los esquemas analizados y se identificarán los escenarios en que puede ser más adecuado aplicarlos.

Los esquemas que se van a describir son:

a) Clasificación de la información en las entidades públicas

b) Esquema de clasificación aplicado en entidades de defensa europeas

c) Modelo TLP (Traffic Light Protocol)

Por último, se describe un esquema general de metodología de implantación de un esquema de clasificación de la información.

Clasificación, en las entidades públicas, de la información conocida legalmente como información clasificada.

En este apartado nos referiremos únicamente a las diferentes categorías de información de uso oficial que se manejan en el ámbito de las administraciones públicas, así como de los requisitos o criterios de clasificación de la información. No se entrará en el detalle de la desclasificación ni en la organización que debe acompañar a un proyecto de clasificación en aspectos tan importantes como la identificación o designación del órgano responsable de la clasificación/desclasificación o las figuras responsables de la seguridad que deben asegurarse de que se cumplen las medidas de seguridad correspondientes, ni en los procedimientos de control que deben establecerse en el manejo de la información de acuerdo con su categoría y según el principio básico de necesidad de conocer. Este principio básico de "necesidad de conocer" debe regir cualquier política de manejo de información clasificada.

Las administraciones públicas, y especialmente aquellas cuyas competencias están relacionadas con la defensa y la seguridad tanto del estado como de los ciudadanos y empresas, acostumbran a manejar información con cierto nivel de clasificación. En estos casos, este manejo se realiza de acuerdo a lo establecido en una norma de rango legal: la **Ley 9/1968, de 5 de abril, sobre secretos oficiales (LSO) .**

El **atributo** que se utiliza para valora en la información es "daño causado por revelación no deseada", es decir, la categorización se basa en la valoración del impacto de esa posible divulgación indeseada.

La LSO establece una limitación sobre la "publicidad" que puede hacerse de la información atendiendo al perjuicio que esa publicidad podría derivar *"para la causa pública, la seguridad del estado o los intereses de la colectividad de la colectividad"* de los ciudadanos. Se entiende que este alcance incluye también a empresas, especialmente cuando estas forman parte de la estructura de los servicios esenciales o críticos del estado.

Por su parte, el requisito o limitación de uso de la información se explicita con la posibilidad de publicitar o no dicha información. Y debe entenderse de forma estricta de manera que se puede considerar que la seguridad de la información clasificada queda comprometida por el simple hecho de que esa información sea conocida por **una** única persona no autorizada.

Atendiendo a este criterio básico de impacto y, por tanto, de grado de protección necesario, la LSO introduce dos categorías de clasificación: Secreto y Reservado. Sin embargo, es habitual manejar dos categorías adicionales para el manejo de información clasificada de uso interno. Son las categorías identificadas como "Confidencial" y de "Difusión Limitada". Estas dos últimas categorías se introducen en normas adicionales aprobadas por la correspondiente autoridad: la Autoridad Nacional para la protección de la información clasificada.

Este esquema, por tanto, establece 5 posibles valores para la información clasificada que, ordenados de mayor a menor nivel de restricción, son:

- Secreta.
- Reservada.
- Confidencial.
- Difusión Limitada.
- Pública.

La clasificación de «**secreto**» se aplica las materias que precisan del más alto grado de protección por su excepcional importancia y cuya revelación no autorizada **pudiera dar lugar a riesgos o perjuicios de la seguridad del Estado, o pudiera comprometer los intereses fundamentales de la Nación** en materia de defensa nacional, la paz exterior o el orden constitucional.

La clasificación de «**reservado**» se aplica a los asuntos, actos, documentos, informaciones, datos y objetos no comprendidos en el apartado anterior por su menor importancia, pero cuyo conocimiento o divulgación pudiera **afectar a los intereses fundamentales de la Nación**, la seguridad del Estado, la defensa nacional, la paz exterior o el orden constitucional.

La clasificación de «**confidencial**» se aplica a la información cuya revelación no autorizada o utilización indebida pudiera **causar una amenaza o perjuicio** para los intereses de España en los diferentes ámbitos.

La clasificación de «**difusión limitada**» se aplica a la información cuya revelación no autorizada o utilización indebida pudiera **ser contraria a los intereses** de España en cualquiera de los ámbitos relacionados en los apartados anteriores.

La categoría de información «**pública**», si bien no está recogida como tal en la LSO, por no ser objeto de clasificación alguna, aplica al resto de la información, que será de acceso público y libre.

Dado que este esquema o grados de clasificación no coincide actualmente con los esquemas o grados de clasificación que se usan internacionalmente, se dispone de una guía o tabla de equivalencia para poder identificar internacionalmente la información clasificada con las categorías españolas. Estos cuadros se utilizan para identificar las equivalencias entre las categorías nacionales y las categorías usadas en la Unión Europea, OTAN y Agencia Espacial Europea.

Puede encontrarse información más completa y detallada sobre la seguridad de la información manejada por las administraciones públicas en la Norma “NS-04 Seguridad de la Información”, de la Autoridad Delegada para la Seguridad de la Información Clasificada y en el Anexo II de la Guía CCN-STIC-822: Procedimiento de clasificación y tratamiento de la información clasificada.

Esquema de clasificación aplicado en entidades de defensa europeas

El ámbito de mayor extensión geográfica y temporal donde se aplican esquemas de clasificación de la información similares o con mínimas diferencias probablemente sea en entidades de defensa europeas. Estos esquemas de clasificación de la información se aplican desde hace décadas con un éxito apreciable. Por su eficacia y extensión, se han utilizado referencia para otros esquemas de clasificación, en organizaciones similares de otras geografías o en otras organizaciones europeas como, por ejemplo, la Comisión Europea, el Consejo de Europa, países miembros u otras organizaciones supranacionales.

El esquema de clasificación se apoya en la confidencialidad de la información clasificada y utiliza como criterio de clasificación la valoración del daño que podría suponer una difusión no deseada

de esta información, sea para el propietario de la información, sea para las entidades que la gestionan, custodian, utilizan y/o acceden a ella.

Así, el esquema de clasificación establece 5 niveles de clasificación, denominados en orden de menor a mayor restricción de acceso a la información como “Unclassified”, “Restricted”, “Confidential”, “Secret” y “TopSecret”.

Este modelo permite la coexistencia en paralelo de múltiples organizaciones con capacidad de clasificación su propia información en base a un esquema de clasificación cuasi-compartido. Por ello, es habitual que el nivel de clasificación explicite la organización bajo la que se clasifica esta información y así pueden identificarse informaciones clasificadas como “NATO-Restricted”, “UE-Confidential” u otras similares. Cada organización establece mediante instrumentos legales de rango suficiente su autoridad sobre la información que clasifica y su capacidad de definir las instrucciones precisas que regirán el esquema de clasificación. Así, puede modular los elementos fundamentales de sus esquemas de clasificación: los criterios aplicables a cada nivel, la coexistencia de informaciones en distintos niveles de clasificación, las reglas de protección de la información en cada nivel, o los mecanismos que permiten el acceso a terceros a información clasificada o su compartición con otras entidades que también clasifican información. El esquema también permitir segmentar la información de una organización en dominios separables que pueden operar con aislamiento suficiente y permita controlar el tránsito de información dentro de la propia organización. También permite el uso de categorías específicas para determinadas informaciones de tipologías especiales, y de etiquetas y categorías de tratamiento también específicos.

El esquema requiere que cada organización con acceso a información clasificada constituya un órgano encargado de la protección en la organización de esta información clasificada, garantizando en todo momento la protección y uso de la información de acuerdo a su nivel de clasificación. Este órgano se suele encargar de la asignación formal del nivel de clasificación que debe aplicarse a cada pieza de información. Asimismo, suele actuar como punto de entrada y salida de la información clasificada en la organización.

Como nota adicional, este esquema de clasificación establece la necesidad de acreditación de la idoneidad de los medios que se emplearán para el manejo de información clasificada antes de que se produzca efectivamente este manejo. Esto incluye la necesidad de acreditación tanto de la propia organización, como de las instalaciones concretas donde se manejará la información clasificada, como de los recursos empleados en el mismo (medios informáticos, copiadoras, redes, archivadores, etc.), y, por último, la acreditación de las personas que efectivamente manejarán la información clasificada.

No se sorprenda si esta descripción le suena conocida, o le recuerda a película de James Bond, series de espías o libros de Tom Clancy. Su intuición es correcta. Todos estos productos culturales están influenciados por estos esquemas de clasificación y se apoya en ellos para el desarrollo de sus historias. Y frases como que “este documento está clasificado al máximo nivel”, están basadas en hechos reales. En estos esquemas de clasificación.

Traffic Light Protocol (TLP)

El esquema “*Traffic Light Protocol*” (TLP) se enfoca en el intercambio de información sensible tanto en el ámbito de la seguridad de la información como en otros ámbitos como operaciones comerciales, foros de opinión, encuentros, etc. Es un esquema simple e intuitivo para indicar cuán sensible es la información sobre ciberseguridad que va a ser compartida, el nivel de difusión autorizado para la misma, lo que facilita la colaboración entre entidades y organizaciones a nivel nacional e internacional. El autor puede indicar, de una forma ágil y

sencilla, hasta dónde puede circular la información más allá del receptor inmediato, y éste debe consultar al autor original cuando la información necesite ser distribuida a terceros.

Se utiliza de forma operativa simplemente por organizaciones públicas y privadas en el sector de la ciberseguridad, tanto en España, como en otros países como Estados Unidos, Australia, Canadá, Finlandia, Francia, Alemania, Hungría, Italia, Japón, Países Bajos, Nueva Zelanda, Noruega, Suecia, Suiza, y Reino Unido.

La definición formal más actualizada (v2) del esquema ha sido realizada en agosto de 2022 por el Forum of Incident Response and Security Teams (FIRST)[1]. INCIBE ha realizado una traducción al español del mismo[2].

Se utiliza de distintas maneras, según el contexto en el que se necesite. Por ejemplo, en **mensajería** – como correo electrónico y chat – se debe incluir la etiqueta TLP en la línea del asunto de aquellos mensajes que requieren ser marcados con este protocolo. Cuando sea necesario, también se añadirá la etiqueta al final del texto al que se aplica la etiqueta TLP. Por otro lado, los **documentos** afectados deben contener la etiqueta TLP correspondiente (tamaño de letra: 12 puntos; ubicación: a la derecha), tanto en el encabezado y como en el pie de página de todas las páginas del documento.

TLP no está diseñado para el intercambio de información automatizados, dejando su uso a elección de los informadores siempre que esté en concordancia con el estándar.

Existe un código de cuatro colores -rojo (RED), amarillo (AMBER), verde (GREEN) y transparente (CLEAR)-, con diferentes significados, marcado por el FIRST.

Código	Cuándo utilizarlo	Cómo compartirlo	Color	Fondo
TLP:RED	Se debe utilizar TLP:RED cuando la información está limitada a personas concretas, y podría tener impacto en la privacidad, reputación u operaciones si es mal utilizada.	Los receptores no deben compartir información designada como TLP:RED con ningún tercero fuera del ámbito donde fue expuesta originalmente.	#ff2b2b	#000000
TLP:AMBER	Se debe utilizar TLP:AMBER cuando la información requiere ser distribuida de forma limitada, pero supone un riesgo para la privacidad, reputación u operaciones si es compartida fuera de la organización.	Los receptores pueden compartir información indicada como TLP:AMBER únicamente con miembros de su propia organización que necesitan conocerla, y con clientes, proveedores o asociados que deban estar al tanto para protegerse a sí mismos o evitar daños. El emisor puede especificar restricciones adicionales para compartir esta información. Nota: se debe especificar TLP:AMBER+STRICT, si la fuente desea restringir la compartición sólo a la propia organización.	#ffc000	#000000
TLP:GREEN	Se debe utilizar TLP:GREEN cuando la información es útil para todas las organizaciones que participan, así como con terceros de la comunidad o el sector.	Los receptores pueden compartir la información indicada como TLP:GREEN con organizaciones afiliadas o miembros del mismo sector, pero nunca a través de canales públicos.	#33ff00	#000000
TLP:CLEAR	Se debe utilizar TLP:CLEAR cuando la información no supone ningún riesgo de mal uso, dentro de las reglas y procedimientos establecidos para su difusión pública.	La información TLP:CLEAR puede ser distribuida sin restricciones, sujeta a controles de Copyright.	#ffffff	#000000

Se entiende por organización a un grupo que comparte una afiliación común por medio de una membresía formal y que se rige por políticas comunes establecidas por la Organización. Una organización puede ser tan amplia como todos los miembros de una Organización de intercambio de información, pero raramente más amplia.

Se entiende por clientes a aquellas personas o entidades que reciben servicios de ciberseguridad de una organización. Los clientes se incluyen por defecto en TLP: AMBER para que los receptores puedan compartir la información más adelante con el fin de que los clientes tomen medidas para protegerse. En el caso de los equipos con responsabilidad nacional, esta definición incluye a las partes interesadas y a los mandantes.

Si el receptor necesita difundir dicha información con terceros, más allá del alcance de la designación TLP indicada, debe remitirse a la fuente original.

- [1] FIRST, https://www.first.org/tlp/
- [2] INCIBE, https://www.incibe-cert.es/tlp

Comparativa entre los esquemas de clasificación descritos

Los tres esquemas de clasificación expuestos son algunos ejemplos de esquemas de clasificación utilizados por las organizaciones. Todos ellos comparten los elementos comunes descritos para todos los esquemas de clasificación. Cuando no se basan en un imperativo legal, cada Organización los particulariza para crear tanto esquemas más exigentes, detallados y que requieren una mayor inversión de recursos como otros más livianos y simplificados.

Así, una empresa de menor tamaño (y por ello, con menos recursos y probablemente con menor cantidad de información sensible) se beneficiará más usando un esquema de clasificación más simple como TLP, mientras que una gran empresa encontrará ventajoso utilizar esquemas de clasificación similares a los de la administración pública.

No son los únicos esquemas de clasificación existentes. Hay más, y no son pocas las organizaciones que han desarrollado su propio esquema. Cada Organización debe identificar el esquema que mejor responde a sus necesidades de protección de información y capacidades de inversión. Esperamos que estos ejemplos sean de utilidad.

Metodología de clasificación

La metodología que permite a las organizaciones implantar un esquema de clasificación de la información, es muy sencilla; conceptualmente. ISO 27002:2022 propone en su control 5.12 una aproximación en los siguientes pasos:

1. Identificar la información existente en la organización, sus propietarios y ubicación, e inventariarla.
2. Seleccionar o definir un esquema de clasificación de la información, que contemple las necesidades y prioridades legales, contractuales y de negocio que sean aplicables, y los criterios de clasificación adecuados.
3. Clasificar la información existente de acuerdo con el esquema definido.
4. Aplicación de las medidas de seguridad establecidas para cada nivel, incluyendo el etiquetado de la información identificada.
5. Identificar inconsistencias, imperfecciones, incompletitudes y/o posibles mejoras en el esquema, tras su aplicación sobre los datos existentes. Iterar en su caso el paso 2.
6. Manejar y tratar la información que ha sido clasificada de acuerdo con el esquema.

Centrándonos el punto 3 de la clasificación propiamente dicha, este proceso va a consistir en la clasificación de la información asignando distintos niveles a la misma. Los niveles y número de ellos dependerán de cada entidad, de la complejidad y magnitud de la información, de las obligaciones legales y contractuales y de la metodología elegida en el punto 2.

La aplicación del esquema de clasificación puede seguir un método iterativo, que se aplique sobre cada información. Se trataría de medir el nivel del impacto de cada uno de los criterios establecidos en la metodología seleccionada, para luego asignar el nivel global de impacto de acuerdo con el nivel más restrictivo. Este nivel global se volvería a analizar para comprobar su idoneidad en función de los objetivos de seguridad de la información de la entidad o incluso del tiempo que ha pasado desde su clasificación inicial (una información confidencial en el 2019 puede que ya no lo sea en su revisión del 2024). Por otro lado, es habitual que los esquemas inicialmente seleccionados no sean directamente aplicables en un primer intento, requiriendo iteraciones adicionales para perfeccionar su aplicación.

En todo caso, y al igual que cada Organización debe seleccionar y/o definir un esquema de clasificación de la información que se adapte a sus necesidades, así ha de seleccionar y adaptar la metodología de trabajo general que aquí se ha descrito para su efectiva implantación en la Organización.

Se puede ver un ejemplo de cómo llevar a cabo la clasificación de la información por el responsable de la información en el ANEXO “Instrucción técnica”.

Organización, procesos y recursos necesarios en un esquema de clasificación de la Información

La mera definición de un esquema de clasificación de la información no resulta efectiva si no se acompaña del despliegue de medios, procesos y recursos adecuados para que la organización se asegure de que se aplica en el día a día.

En este sentido, todas las organizaciones están experimentando una progresión alcista en cuanto a volumen y variedad de información digital que tratan en sus procesos de negocio y en sus actividades, por lo que el acto de identificar una información como clasificada (o calificada) y tratarla de acuerdo con sus necesidades constituye una actividad cada vez más frecuente en las organizaciones. Consecuentemente con la anterior y a pesar de ser una tarea no trivial y que requiere de recursos y esfuerzos, se está convirtiendo en una actividad cotidiana en aquellas organizaciones que clasifican volúmenes o porcentajes apreciables de información en su día a día. Para ello, estas organizaciones deben pues embeber las actividades de clasificación de la información en sus procesos de operación cotidianos para que esta sea efectiva.

La clasificación de la información en estas organizaciones que clasifican información recurrentemente requiere de disciplina y orden, así como de la aplicación intensiva de tecnologías TI específicas para automatizar las operaciones de Identificación y/o clasificación y/o etiquetado y/o difusión y/o tratamiento de la información clasificada.

El uso de soluciones TI para este fin no resulta suficiente para la completa implantación del esquema de clasificación de la información: se precisa además del despliegue de medidas organizativas, de la adaptación de los procesos de la organización y, sobre todo, de la colaboración, complicidad y rigurosidad de las personas de la organización. Estos aspectos se tratan a continuación y debería reflejarse en el marco normativo de la Organización (ya pertenezca ésta al sector público o al sector privado).

Identificar. Tipos de Información para ser clasificada y medios organizativos (roles y responsabilidades) para su protección.

Como ya hemos dicho en repetidas ocasiones, la definición de un esquema de clasificación de la información implica el reconocimiento del valor de la información; es decir, del diferente valor que tienen diferentes informaciones y esa consciencia debe generar la responsabilidad de la organización sobre la adecuada custodia de esa información.

Reconocida esta responsabilidad, la organización determina cómo va a ejercerla y a qué entidad interna (o entidades) se asignará el ejercicio de la misma y las responsabilidades que se deriven de ella. Dado que el establecimiento y aplicación de un esquema de clasificación de la información suele ser parte los marcos de control de ciberseguridad habituales (ENS, ISO 27001, NIST, …), esta responsabilidad en determinas organizaciones suele asignarse al CISO de la organización. De esta forma, el esquema de clasificación se integra como parte de las medidas de ciberseguridad generales de la organización y se incluye en el ciclo de vida global de gestión de controles de seguridad. Pero como es obvio, cada Organización atendiendo a diferentes cuestiones debe establecer si esa responsabilidad se le asigna a una persona en concreto o aun conjunto o incluso a un comité.

Incluso recayendo esa responsabilidad en la organización global de la ciberseguridad nos podemos encontrar con organizaciones que, de forma coherente con una separación de funciones en la organización de la seguridad, el CISO establezca los principios y supervise la práctica con esos principios, pero no ejecute, recayendo esa actividad en el área de operaciones de seguridad. Este modelo simple sufrirá de una mayor variedad de roles y delegación de funciones en aquellas empresas que sean complejas y tengan capacidad para acercar la clasificación a quién genera la información.

En el ENS se define el Responsable de la Información, rol que establece y aprueba la valoración de la información en tres niveles (bajo, medio y alto) en cada una de las cinco dimensiones de la

seguridad que considera el ENS. En base a dichas valoraciones el Responsable de la Seguridad (equivalente al CISO) supervisará las medidas de seguridad, las cuales implantará y operará el Responsable del Sistema junto a su posible equipo interno o externo.
Todas estas variantes suelen coincidir en la necesidad de que, una vez se ha identificado una información y la clasificación que le corresponde, se apliquen etiquetas, modificadores o metadatos a este dato que permitan la identificación del nivel de clasificación de esta información y su adecuado tratamiento. El formato y tipo de etiquetas deberá ser definido por la Organización como parte del esquema de clasificación.
No existen patrones estandarizados para este procedimiento, por su variabilidad en las organizaciones: la clasificación puede ser determinada por el creador de la información, por el CISO, o por la entidad que controla el envío y recepción de la información; se puede establecer a priori, antes de la creación de la información, o tras su creación; puede estar condicionada por haberse apoyado para su creación en información previamente clasificada o no; la clasificación puede necesitar uno o varios pasos; puede ser una clasificación directa o requerir de validación posterior; etc. El número de variantes posibles en el procedimiento es muy elevado y la organización debe analizarlas y decidir sobre ellas.
A partir de este punto se abren infinitas posibilidades, la organización puede o no permitir reclasificaciones por determinadas personas, en determinados procesos o por la aplicación de este subproceso de forma iterativa por cada departamento que deba distribuir la información. Por eso los tipos de información y por tanto los criterios deben ser claros y estos, junto con los roles deben estar formalmente documentados.
Los roles pueden ser:

- Creador de información
- Receptor de información externa (a la Organización).
- Propietario
- Usuario
- Clasificador / Reclasificador / Desclasificador
- Supervisor

Estos roles pueden recaer sobre una misma persona, sobre un conjunto de personas o sobre un comité y a su vez para el conjunto de la información, puede recaer en una, más de una o en un comité. La función puede ser delegada no ya por tipo de información, sino por departamento que genera la información, pudiendo marcarla cada uno de los autores o una persona delegada. La Entidad o empresa es quién debe decidir su modelo de responsabilidad.

Definición del esquema de Clasificación.

Cabe la posibilidad de que la información se procese de forma inadecuada por ausencia de clasificación o por tener una clasificación inadecuada. Por ello, es necesario disponer de un procedimiento de clasificación de la información.
La **definición del esquema de clasificación** que se aplicará en la organización debe ser válido para satisfacer tanto las necesidades de clasificación propias de la organización, como las necesidades de la información de terceros que maneje la organización que esté sujeta a medidas de seguridad propias.
Debemos, por tanto:

- Identificar los tipos de información que la Organización maneja (lo que hemos definido anteriormente como “taxonomía”), bien por su naturaleza o por el impacto que puede provocar por su acceso no autorizado; por ejemplo, una taxonomía principal que responda al tipo de impacto podría ser:
    - Financiera
    - Reputacional
    - Legal y regulatoria

    - Oportunidades de Negocio
    - Salud
    - Seguridad

  O bien por su naturaleza:

    - De carácter personal (Nombres, apellidos, DNI, etc.)
    - Empresarial (Financiera, Recursos Humanos...)
    - Regulada por seguridad (Infraestructura crítica, servicio esencial, sensible EEUU...).
    - Otras…

- Establecer criterios de identificación. Por ejemplo, palabras claves o repositorios específicos, que aplicada al tipo de información y al grado de difusión nos permita identificar la etiqueta (o etiquetas en algunas organizaciones) con las que debe ser clasificado (manual o automáticamente, como recomendación de marcado o como valor de marcado). En el caso de apoyarnos en marcado automático debemos disponer de herramientas o productos que o bien generan una clasificación por defecto o bien lo hacen por comparación de plantillas o palabras clave y es el autor del documento el que confirma o modifica la clasificación. Este apoyo de herramientas, funciones y servicios TI debería ejercerse tanto sobre la nueva información que se genera como sobre la que no fue etiquetada en su génesis, pero que una vez aflorada por el descubrimiento realizado con herramientas específicas, la comparan con los modelos y clasifican (o pre-clasifican).
- Cabe comentar, los criterios de identificación no son fijos. Un documento no tiene por qué tener un único tipo de información. Podría incluir datos personales, regulatorios, y financieros simultáneamente. También podría tener impacto en diferentes ámbitos como reputacional, legal, etc. Un criterio correcto de identificación basado en herramientas automáticas debería considerar los porcentajes de este tipo de datos en un documento y no sólo una categoría concreta cara a determinar la etiqueta o nivel de confidencialidad. La generación de etiquetas automáticas no es un proceso trivial y es por eso que la confirmación del autor permite afinar más su precisión.

En un caso ideal, todas las necesidades serán satisfechas por un esquema de clasificación único, pero la organización debe considerar la opción de establecer entornos y recursos dedicados y separados para la gestión de la información de terceros, adaptándola a los requisitos concretos que se piden en los esquemas de clasificación de estos terceros. En ese caso, la Organización deberá dotarse de recursos adicionales para la definición, despliegue y gestión en paralelo de los diversos entornos de clasificación de la información que existan. Y como parte de esta decisión, puede designar una figura, conjunto de personas o departamentos en quien delegue las funciones de clasificación de información en estos entornos separados.

Procedimiento de almacenamiento e intercambio de información clasificada.

El almacenamiento de la información se basa en la utilización de diversos recursos de almacenamiento preconfigurados (idealmente no solamente con la capacidad) para cumplir los controles de seguridad establecidos para cada nivel.

De una forma global para los diferentes tipos de soporte, los medios de almacenamiento combinan elementos como cajoneras, armarios archivadores, salas dedicadas, almacenamiento en diversos servidores y/o redes, cifrado de información, cajas fuertes, etc., según se determine.

Centrándonos en la información digital y en los activos de información que los almacenan, estaríamos hablando de: unidades de almacenamiento externas, discos locales, servidores de red o almacenamiento en la nube y cuanto elemento relacionados con ellos, permitieran establecer controles de seguridad respecto al acceso y a las operaciones que se pueden realizar

sobre los documentos digitales tales como lectura, escritura, copia o borrado. Incluso se establecen controles como criptografía, inventario de soportes y destrucción segura de la información.
Por su parte el intercambio de información suele requerir del control de los canales autorizados, incluyendo el uso o no de correo electrónico, servidores de almacenamiento, aplicaciones de mensajería, servicios de transferencia de ficheros (ftp), valijas internas y acceso compartimentado a la propia información, así como los ya citados de comunicaciones cifradas y control de soportes. En muchos casos, estas medidas se combinan con las medidas de control de acceso a la información, instrumentalizando la autorización de acceso a los usuarios para permitir o no a la misma. También se suelen combinar estas medidas con otras como el uso de IRM y/o de DLP.
Merece una mención específica la cuestión relativa al establecimiento de canales de información para el intercambio de información clasificada por terceros, ya sea para el envío como para la recepción de esta información clasificada. En este caso, las organizaciones habitualmente designan un procedimiento que centraliza estos intercambios, asegurándose que se aplican correctamente las medidas de protección establecidos para cada nivel de clasificación. Entre estas medidas se incluye el control de que la Organización no comparta esta información recibida con entidades que no tiene la acreditación/acuerdos necesarios para manejar información de ese nivel de clasificación. También incluye la verificación de que los canales de comunicación usados para el intercambio son adecuados y seguros para cada nivel de la información. Aunque es habitual la centralización de las comunicaciones de información clasificada en un punto único, existen organizaciones y esquemas de clasificación que permiten el envío y recepción de información clasificada por varios canales e interfaces de la organización, o incluso por cualquier persona. En ocasiones, esta opción resulta viable para niveles de clasificación menos restrictivos, mientras que la información de mayor clasificación usa un modelo centralizado. Esta solución resulta también viable cuando la dotación de recursos es insuficiente o escasa, puesto que el establecimiento y operación de un departamento/grupo u oficina que centralice esas comunicaciones implica mayores costes operativos y un mayor tiempo de envío o recepción de información. Todos estos riesgos deben ser valorados por la organización cuando diseñe el esquema de clasificación de la información aplicable.

Formación del personal para el manejo de información clasificada

La clasificación (o calificación) de la información es una medida de seguridad con una relación muy cercana a las personas, en tanto que modula la forma en la que manejan la información en su día a día y busca controlar posibles riesgos de acceso no previstos. Por ello, deben implantarse controles y acciones específicas para asegurar que las personas que manejan información clasificada entienden su rol en el manejo de las distintas informaciones clasificadas, qué expectativas tiene la organización y cómo deben actuar para satisfacer estas expectativas.
Por ello, la organización debe emprender acciones tanto de concienciación, como de formación.

Los empleados deben recibir formación y concienciación sobre la importancia de la clasificación de la información y los procedimientos, políticas y medidas de seguridad que deben seguirse para proteger la información durante todo su ciclo de vida. El personal debe ser capacitado para llevar a cabo esas obligaciones, lo que incluye el manejo de aplicaciones, funciones y servicios TI que le presten apoyo en tales obligaciones.

Estas acciones de concienciación, formación y capacitación deben incluir a todo el personal de la organización, porque todos ellos pueden tener que manejar información clasificada (o calificada) propia o de terceros. Esto incluye tanto a las personas que se desempeñan en la organización como las que se irán incorporando. Y debe concretarse en un compromiso de todo el personal en la aplicación del esquema de clasificación definido.

Las acciones de concienciación deben enfocarse a conseguir que las personas de la organización asuman la relevancia de sus actuaciones en la efectiva implantación del esquema. Así, deben entender la importancia de que identifiquen los niveles de clasificación definidos por la Organización. También deben asumir la necesidad de identificar en qué nivel está clasificada o valorada una determinada pieza de información y porqué debe tratarse esta información según se define en el esquema. Deben entender también que estas actividades deben ser realizadas en todo momento y con toda la información, dadas las consecuencias negativas que tendría no aplicar o hacer excepciones en la aplicación del esquema de clasificación.
Por otra parte, las acciones de formación se enfocarán a capacitar al empleado para aplicar correctamente las herramientas, procedimientos y recursos que la organización ha dispuesto durante la implantación del esquema. Deben pues describir cómo han de identificar la información clasificada y el nivel de clasificación que les aplica, que restricciones y medidas de seguridad han de aplicarse, qué procedimientos y acciones son permitidos para cada acción y cuáles no, etc.
Tanto las acciones de formación como las de concienciación deben ser adaptadas a las distintas funciones de la organización. Todas las personas deberían conocer el esquema general y los casos de uso específicos de su puesto. En particular, cuando la organización haya designado una unidad especializada en actividades de clasificación de la información. La organización puede también esperar de las personas de manejan información de mayor nivel o en mayor volumen que acrediten su ética profesional en alguna manera, o incluso establecer criterios de selección de personal específicos para estos puestos.

La formación debe ser acompañada de la aplicación de medidas de control de acceso a la información ajustadas a los niveles de clasificación, a la formación de las personas y a la necesidad de conocer de estas personas. Este acceso deberá estar integrado en las medidas de control de acceso globales de la Organización.
La condición de usuario de información clasificada o sensible no debe implicar ningún derecho o prerrogativa especial sobre la propiedad de dicha Información.
Entre las responsabilidades que debe tener asignada el usuario, caben destacar algunas que se citan a continuación:

1. Responsabilidad de proteger adecuadamente la información clasificada a su cargo.
2. Conocer el esquema de clasificación aplicable a la información, cumplirlo y seguir las normas específicas de seguridad referentes a la protección según el tipo de información que utilice.
3. Mantener la confidencialidad de la información clasificada a la que accedió en el desempeño de un puesto cuando cese en el desempeño de ese puesto, sea porque cesa la relación laboral que la motivó, sea porque pase a desempeñar una posición distinta.
4. No manejar la información clasificada al margen de los canales y procedimientos formalmente establecidos y aplicables para ese nivel de clasificación.
5. Cooperar con el responsable de la información clasificada de la Organización, en lo que le sea requerido.

Adicionalmente, la Organización debería adoptar medidas de monitorización y seguimiento de la efectiva implantación del esquema de clasificación de la información implantada, que identifique las no aplicaciones de este y cómo actuar ante ellas. Incluyendo cuando la no aplicación se produce por personas concretas individuales. Y estar capacitada para reaccionar ante estos eventos.

Por último, se debe facilitar en la medida de lo posible a los usuarios los procedimientos y/o herramientas que faciliten las decisiones a la hora de clasificar la información y medidas de protección que no supongan una fricción elevada en su uso diario. De lo contrario, puede existir el problema de que muchos usuarios catalogarán como “uso público” la información para que no les entorpezca su trabajo diario.

REQUISITOS Y CONDICIONES DE TRATAMIENTO DERIVADOS DE LA CLASIFICACION A LO LARGO DEL CICLO DE VIDA DE LA INFORMACION

Ciclo de vida de la información clasificada.

El ciclo de vida ya se trató en la sección de introducción de esta guía. Consideraremos las siguientes etapas de dicho ciclo:

- Creación: La información es creada en un formato específico (si bien posteriormente puede ser transformado a otro formato).
- Almacenamiento o archivado: La información es almacenada en un lugar seguro y accesible.
- Uso o procesamiento o tratamiento o transformación: La información es utilizada para cumplir con un propósito específico.
- Mantenimiento: La información es actualizada o modificada para asegurar su precisión y relevancia.
- Compartición, distribución o transmisión: La información es compartida con aquellos que la necesitan.
- Retención: La información es retenida para cumplir con las leyes y regulaciones aplicables, así como con las necesidades del negocio.
- Eliminación: La información es eliminada cuando ya no es necesaria o cuando se cumplen los plazos de retención.

Responsabilidad del tratamiento de la información clasificada a lo largo de su ciclo de vida.

Es necesario nombrar una persona responsable de la seguridad en el tratamiento de la información clasificada, con responsabilidad y autoridad para identificar los riesgos en los procesos de tratamiento de la información clasificada en cada fase de su ciclo de vida y establecer y supervisar los mecanismos y métodos que protejan los mismos frente a dichos riesgos, las políticas de concienciación y formación y los roles de las personas que van a formar parte del equipo encargado de la seguridad durante el tratamiento y ciclo de vida de la información clasificada.

Riesgos de la información clasificada a lo largo de su ciclo de vida.

Estos incluyen el riesgo de divulgación o fuga de la información clasificada fuera del círculo de usuarios con permiso, riesgo de manipulación o alteración indebida o no autorizada de la misma, y riesgo de su destrucción o desaparición. Estos riesgos existen en cada fase del ciclo de vida, aunque dependiendo de la fase del ciclo de vida en que se encuentre la información clasificada, el riesgo se manifestará de forma distinta, los vectores de ataque serán diferentes y los mecanismos y métodos de protección serán distintos en función de los factores anteriores. Será necesario establecer los más adecuados para cada fase.

Requisitos de tratamiento a lo largo del ciclo de vida.

Abordamos en esta sección un análisis de los aspectos a tener en cuenta para el tratamiento de la información clasificada en cada una de las etapas de su ciclo de vida:

1. Almacenamiento.

1.1 Seguridad física. Se contemplan los siguientes aspectos:

a. Localización: Es importante asegurarse de que la ubicación del almacenamiento físico de la información clasificada sea segura y autorizada, preferiblemente en un lugar protegido y vigilado.
b. Acceso: Para el acceso físico es importante establecer controles de acceso, cerraduras de alta seguridad, sistemas de alarma, sistemas de vigilancia, entre otros.
c. Protección: El almacenamiento físico de la información clasificada debe estar protegido contra riesgos físicos, como incendios, inundaciones, terremotos, entre otros. Para ello, se pueden utilizar medidas de protección como sistemas de detección y extinción de incendios, sistemas de respaldo de energía, entre otros.
d. Etiquetado: Todos los documentos y dispositivos de almacenamiento físico que contengan información clasificada deben estar etiquetados claramente con su nivel de confidencialidad y con información de contacto para reportar cualquier problema o incidente relacionado con su seguridad.
e. Organización: Los documentos y dispositivos de almacenamiento físico deben ser almacenados de forma ordenada y organizada para facilitar su acceso y control. Además, es recomendable utilizar cajas de seguridad o armarios resistentes para protegerlos.

1.2 Almacenamiento y archivado lógico de la información clasificada en formato digital:

Un aspecto clave de la protección de la información clasificada en la fase de almacenamiento es la definición de los tipos de información clasificada y tipos de datos dentro de la misma que deben almacenarse cifrados. Deben además definirse las técnicas de cifrado y descifrado a utilizar que sean adecuadas para la Organización y que mantengan la seguridad de la información no solamente mientras está almacenada cifrada, sino cuando se accede a ella.

Otro aspecto clave es la resistencia del dato en el archivado con la realización de copias de seguridad (mutables e inmutables) y la recuperación de la información clasificada, siendo procesos críticos para garantizar la confiabilidad, disponibilidad y la integridad de la información A continuación, se describen algunos aspectos importantes a considerar:

1.3 Archivado: La información clasificada debe almacenarse de manera segura y protegida en un lugar adecuado, donde pueda mantenerse en buen estado y protegerse de daños físicos y digitales. Es importante establecer políticas y procedimientos claros para la gestión del archivo, incluyendo la identificación y etiquetado de los archivos, la documentación y la trazabilidad.

1.4 Copias de Seguridad: Es importante realizar copias de seguridad regulares de la información clasificada y almacenarlas de manera segura. Se deben establecer políticas y procedimientos claros para la realización de copias de seguridad,

incluyendo la frecuencia de las copias, los medios de almacenamiento y la rotación de las copias.

1.5 Recuperación: Es importante establecer un plan de recuperación para la información clasificada, en caso de pérdida o daño de los datos. Este plan debe incluir los procedimientos necesarios para restaurar los datos de las copias de seguridad, las medidas de seguridad para garantizar la integridad de los datos y la documentación de las actividades de recuperación.

1.6 Verificación y Validación: Es importante verificar y validar regularmente la integridad y la autenticidad de los archivos y las copias de seguridad, para garantizar que los datos estén disponibles y sean precisos en todo momento.

1.7 Organización: La organización del almacenamiento puede facilitar la clasificación y la asignación de derechos IRM, por ejemplo, bajo el directorio del departamento X puede establecerse un directorio por cada nivel de clasificación y por debajo del nivel superior de clasificación un directorio por cada proyecto, asignándole a cada uno de los directorios de proyectos los derechos IRM; así al depositar un fichero , si se han creado las reglas, se le asignarían la etiqueta de clasificación y la etiqueta de IRM con sus permisos de derechos.

2 Acceso restringido. Gestión de Acceso y Permisos: La información clasificada como confidencial o crítica debe ser restringida sólo al personal autorizado, utilizando mecanismos de autenticación y autorización seguros. Quién tiene acceso a qué dato y en qué circunstancia o condiciones.

a. Crear y mantener actualizado los repositorios de información, datos y permisos de acceso
b. Establecer el procedimiento para comprobar nivel de autorización
c. Política zero trust. Eliminar cualquier tipo de permiso implícito. Solo dar permisos a la información necesaria para cada individuo
d. Definir e implementar política de autenticación multifactor.
e. Apoyarse en soluciones de IRM
f. Crear y recopilar los registros de acceso.

3 Uso y procesamiento o tratamiento de la información clasificada: Los sistemas de tratamiento y computación de la información deben incorporar en sus procesos y en su arquitectura las medidas de seguridad lógica necesarias para garantizar la confidencialidad, integridad y disponibilidad de la información durante su uso.

Se deben considerar técnicas modernas de cifrado que permiten tratar y procesar la información cifrada sin necesidad de descifrarla, y adoptar aquellas que sean adecuadas para el tipo de organización y sus objetivos.

En cuanto a políticas y medidas de seguridad para los sistemas de almacenamiento y tratamiento digital de la información tanto ‘on-premise’ como en la Nube, se deben considerar como mínimo los siguientes:

1. Antivirus
2. Firewalls
3. Correo electrónico seguro

4. Navegación segura
5. Acceso seguro a la Nube
6. Almacenamiento de datos seguro tanto ‘on-premise’ como en la Nube
7. Políticas zero-trust
8. Sistemas de DLP o control de movimiento de información clasificada.
9. Sistemas de transmisión de la información seguros con cifrado extremo a extremo.
10. Soluciones IRM cara a mantener el control de los datos una vez fuera del perímetro o la nube de almacenamiento.

4 Compartición de información clasificada. Es necesario considerar los siguientes aspectos:

4.1 Autorización: Antes de compartir cualquier información clasificada, es importante verificar que las personas o entidades destinatarias estén debidamente autorizadas para acceder a la información.

4.2 Control (remoto) en todo momento: Asignación de IRM

4.3 Canal de comunicación seguro: La información clasificada debe compartirse solo a través de canales seguros y confiables, como correo electrónico cifrado, redes privadas virtuales (VPN) o servicios de intercambio de archivos seguros.

4.4 Acuerdo de no divulgación: Es importante establecer un acuerdo de no divulgación con las personas o entidades destinatarias de la información clasificada, para garantizar que comprendan sus responsabilidades y obligaciones en relación con la información compartida.

4.5 Rastreo y registro: Es importante realizar un seguimiento y registro de todas las actividades relacionadas con la compartición de información clasificada, para poder identificar cualquier problema o violación de seguridad.

5 Eliminación: la eliminación segura de la información clasificada es crucial para garantizar la confidencialidad y la privacidad de los datos. Aquí se describen algunos aspectos importantes a considerar para una eliminación segura de la información clasificada:

5.1 Política de eliminación: Es importante tener una política clara y bien definida sobre cómo eliminar los datos clasificados. La política debe especificar los requisitos de eliminación, incluyendo el momento de la eliminación, los procedimientos de eliminación y los requisitos de verificación.

5.2 Procedimientos de eliminación: Es importante tener procedimientos claros y documentados para la eliminación segura de la información clasificada. Los procedimientos deben incluir instrucciones detalladas sobre cómo eliminar los datos, incluyendo el borrado seguro de los dispositivos de almacenamiento y la destrucción segura de los documentos físicos.

5.3 Herramientas de eliminación: Es importante utilizar herramientas de eliminación de datos certificadas que puedan garantizar la eliminación segura de los datos. Estas herramientas pueden incluir software de borrado de disco, trituradoras de papel y otros equipos de destrucción segura.

5.4 Verificación de eliminación: Es importante verificar que la eliminación se haya realizado correctamente y de manera efectiva. Esto puede incluir la revisión de los registros de eliminación, la realización de pruebas de recuperación de datos y la verificación de la destrucción física de los documentos

Monitorización, trazabilidad, detección y prevención de violaciones a las políticas de seguridad de la información clasificada.

Es importante mantener una monitorización permanente de los datos sensibles, con detección y prevención de violaciones a las políticas de seguridad de la información que permitan actuar de manera reactiva y correctiva. Algunas medidas a tomar en este sentido son:

a. Implementar sistemas de monitorización de la vida de un dato.
b. Recoger logs de trazabilidad: quien accede, cuando accede, que uso hace.
c. Establecer alertas y mecanismos de detección temprana de posibles riesgos o violaciones de seguridad de los datos, como por ejemplo copia a un repositorio personal o duplicación del dato en un dominio distinto al definido en la política para su almacenamiento.
d. Implementar un sistema de respuesta, que permita bloquear en tiempo real las violaciones detectadas.

Auditoría

Todos los mecanismos y procesos anteriores deben ser auditados periódicamente con el fin de comprobar su correcto funcionamiento y detectar posibles desviaciones o vulnerabilidades en los mismos. Se debe:

1. Establecer la periodicidad y alcance de las auditorías,
2. Incluir revisión de todos los controles establecidos
3. Actualizar, mediante la incorporación de todos los nuevos requisitos legales que puedan haber surgido
4. Elaborar un plan de acción y seguimiento
5. Actuar en modo de revisión continua

CONSEJOS PARA EL DESPLIEGUE

Hemos hablado de clasificación, metodologías, responsabilidades, entre otras cuestiones, por eso llega el momento de poner algún ejemplo como los que se pueden encontrar en el ANEXO 1 y en ANEXO2, son reales y han sido generosamente cedidos por una de las principales empresas españolas, aunque para preservarla mínimamente hemos cambiado su denominación real por ACME. En este apartado se dan algunos consejos, por si alguno puede resultar útil.

- Se ambicioso pero pragmático.
- Sigue esta guía para identificar y establecer la clasificación
- Busca para cada fase del ciclo de vida las herramientas y funcionalidades en los productos que respondan a la necesidad.
- Prueba durante un periodo amplio en tu departamento lo que quieras implantar en toda la Organización. Haz un plan de pruebas que contemple, entre otras cosas:
    - Clasificación manual
    - Clasificación automática
    - Configuración de DLP en Office 365 (o en la suite colaborativa que tengas)
    - Configuración de DLP en equipos finales
    - Configuración de IRM
    - Buscar como relacionar DLP e IRM
    - Prueba con documentos fuera de la Organización
    - Pérdida de dispositivo
- Identifica áreas de tu organización que sean proclives a usar la clasificación. Empatiza
- Piensa para esas áreas (de una en una) en su información, en cómo aplicar la clasificación y en su ciclo de vida especifico y en los medios que van a intervenir.
- Explica e implica
- Despliega de forma gradual en base a los departamentos más proclives.

Tras cada despliegue, revalúa si es necesario revisar y modificar (clasificación, herramientas, formación, identificación de responsabilidades, etc.)ANEXO 1

ACME

NS-04
NORMA DE CLASIFICACIÓN DE LA INFORMACIÓN

Elaborado:	Revisado:	Aprobado:

CONTROL DE VERSIONES

Revisión	Fecha de Aprobación	Motivo de la Revisión

TLP: RED	La información está limitada a personas específicas y podría afectar la privacidad, la reputación o las operaciones si no se maneja correctamente.	Esta información no debe compartirse con terceros fuera del alcance en el que se presentó originalmente.
TLP: AMBER	La distribución de información debe ser limitada, pero representa un riesgo para la privacidad, la reputación o las operaciones si se comparte fuera de la organización.	La información solo se puede compartir con miembros de la propia organización del destinatario que la requieran, y con clientes, proveedores o asociados que la necesiten para protegerse o evitar daños. El remitente puede especificar restricciones adicionales para compartir esta información.
TLP: GREEN	La información es de utilidad para todas las organizaciones participantes y terceros de la comunidad o sector	Los destinatarios pueden compartir la información con terceros afiliados o miembros del mismo sector, pero esto nunca debe hacerse a través de canales públicos.
TLP: WHITE	La información no presenta ningún riesgo de mal uso, dentro de las normas y procedimientos establecidos para su difusión pública.	La información se puede distribuir sin restricciones, dentro de los límites impuestos por los derechos de autor.

1. INTRODUCCIÓN

La información que utiliza el Grupo ACME debe permitir alcanzar los objetivos empresariales, así como otras responsabilidades y obligaciones. Para ello es imprescindible realizar la identificación y marcado de la misma, para posteriormente proceder a su clasificación.

Esta clasificación de la información debe permitir establecer diferencias entre las medidas de seguridad a aplicar. La clasificación y en consecuencia las medidas de seguridad atenderán a criterios de confidencialidad, integridad, disponibilidad y trazabilidad.

La clasificación se realizará tanto de la información, como de los sistemas que tratan dicha información.

Las medidas de seguridad deben implantarse y gestionarse a lo largo del ciclo de vida de la información (generación, almacenamiento, tratamiento, difusión, copia, destrucción, etc.). Los niveles de protección siempre estarán basados en un principio de proporcionalidad.

2. OBJETIVO

El principal objetivo de la "*Norma de Clasificación de la Información*" es definir las categorías de información del Grupo ACME, así como establecer un procedimiento de clasificación de esta y de las medidas de protección aplicables a su manejo, almacenamiento y, en su caso, destrucción. La presente norma viene a desarrollar los principios generales de la seguridad, identificados en la vigente Política de Seguridad de la Información (PSI), en el Apartado VI.5.2 "*Clasificación, marcado y tratamiento de la información*".

3. ÁMBITO

Esta norma resulta de aplicación para todo el Grupo ACME.
El ámbito de aplicación de la presente Norma son los soportes de información (cualquier papel impreso, documento electrónico, contenido multimedia –vídeos, cursos, presentaciones, etc.- documentos, o publicaciones), que contengan información del Grupo ACME que deba protegerse con medidas de seguridad específicas.
Las responsabilidades que en esta norma son las exclusivamente relacionadas para el ámbito de seguridad de la Información.
A lo largo de la presente Norma el concepto <<Seguridad de la Información>> puede ser escrito simplemente como <<Seguridad>>.

4. DOCUMENTACIÓN RELACIONADA

- Política de Seguridad de la Información (PSI)
- IT.09 NS.04.PE.GRS.TIC. Instrucción técnica de borrado seguro y borrado metadatos
- PG-01.PE.GMC.DOC Gestión de la Información Documentada del Sistema de Gestión
- CCN-STIC-835 Esquema Nacional de Seguridad. Borrado de Metadatos
- Incibe-CERT Manual de Clasificación de la información
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

5. ROLES Y RESPONSABILIDADES

5.1. Propietario o responsable de la Información

- Es el responsable de área o cargo directivo del Grupo ACME que tiene la decisión sobre la finalidad, contenido y uso de la información que genera.
- Tiene la capacidad de poder clasificar, desclasificar o reclasificar una información, así como la responsabilidad de establecer y velar por el cumplimiento de los controles de seguridad requeridos.
- El Propietario de la información debe decidir cómo marcar la información según el tipo de soporte, en base a lo indicado en el punto 7 apartado 1.

- El Propietario de la Información, con el apoyo de la Gerencia de Ciberseguridad y Privacidad (si fuera preciso), establecerán los controles necesarios para los distintos soportes, garantizando los niveles de protección adecuados para cada información.
- Debe autorizar la distribución y acceso a la información, y se realizará según su clasificación.
- Dispondrá que se mantengan actualizados los grupos de usuarios o miembros que deben acceder a la información Restringida y Reservada.
- Si lo considera necesario, dispone de la potestad de actualizar el nivel de clasificación de la información.
- En caso de que el Responsable de Seguridad de los Sistemas de Información le informe de que es necesario modificar una clasificación cuando ésta se considere errónea, o bien cuando la misma ponga en peligro la confidencialidad, deberá valorar y en su caso atender a la solicitud.

5.2. Receptor de la información

- Sujeto a lo establecido en la presente Norma.
- En el caso de información restringida **TLP: AMBER**, pueden compartir esta información únicamente con miembros de su propia organización que necesitan conocerla, y con clientes, proveedores o asociados que necesitan conocerla para protegerse a sí mismos o evitar daños.
- En el caso de información reservada **TLP: RED**, no deben compartir esta información con ningún tercero fuera del ámbito donde fue expuesta originalmente.
- Si el receptor de la información generada (con origen) en el interior de la empresa, recibe documentación no clasificada, deberá proceder conforme al punto 7 apartado 4. de esta Norma. Si no obtuviera respuesta, o no pudiera localizar al Propietario de la información, deberá entender que como mínimo debe ser tratada como Información de Uso Interno (UIN) **TLP: GREEN**.
- El receptor de la información con origen en el exterior del Grupo ACME pasa a ser el Propietario de la misma, y debe identificar su clasificación de forma visible.

5.3. Superior jerárquico del Propietario de la Información

- Tiene la capacidad de poder clasificar, desclasificar o reclasificar una información, así como la responsabilidad de establecer y velar por el cumplimiento de los controles de seguridad requeridos.
- En caso de que el Responsable de Seguridad de los Sistemas de Información le informe de que es necesario modificar una clasificación cuando ésta se considere errónea, o bien cuando la misma ponga en peligro la confidencialidad, deberá valorar y en su caso atender a la solicitud.

5.4. Responsable de Seguridad de los Sistemas de Información

- Podrá recomendar al Propietario de la Información que modifique una clasificación cuando ésta se considere errónea, o bien cuando la misma ponga en peligro la confidencialidad.
- Elevará la recomendación, en caso de no ser atendida por el Propietario de la Información, al superior jerárquico del mismo, advirtiéndole del peligro de la clasificación errónea de la información en cuestión.
- Elaborará las instrucciones técnicas de inspección y borrado tanto de metadatos, como de otros datos ocultos asociados a los documentos electrónicos, así como de borrado seguro.

6. CLASIFICACIÓN DE LA INFORMACIÓN POR SU CONFIDENCIALIDAD

La clasificación de la Información ha de realizarse sobre la propia información, independientemente del Sistema de Información que la trate o de la fase del ciclo de vida en la que se encuentre la información. Mediante la clasificación, la organización limita el acceso y uso a la información.

6.1. Niveles de Clasificación de la Información

La información clasificada puede estar en formato electrónico (MS Word, Excel, PowerPoint, Adobe Acrobat, correo electrónico, etc.), o almacenada en soporte físico (papel, DVD, CD, pendrive, disco, etc.).
Para la generación, almacenamiento, acceso, distribución, y control de la información en general, se tendrán en cuenta los siguientes niveles de confidencialidad y el Traffic Light Protocol (TLP) de Incibe[3]:

TLP	Niveles de Clasificación de la Información (Confidencialidad)	Descripción
TLP:WHITE	INFORMACIÓN PÚBLICA (**IPU**)	Información cuya divulgación no afecte a la empresa en términos de pérdida de imagen y/o económica. Se debe utilizar cuando la información no supone ningún riesgo de mal uso, dentro de las reglas y procedimientos establecidos para su difusión pública.
TLP:GREEN	USO INTERNO (**UIN**)	Información que, sin ser reservada ni restringida, debe mantenerse en el ámbito interno de la empresa y no debe estar disponible externamente a través de canales públicos, excepto a terceras partes involucradas previo compromiso de

[3] Traffic Light Protocol (TLP) es un esquema creado para fomentar un mejor intercambio de información sensible en el ámbito de la seguridad de la información. A través de este esquema, de una forma ágil y sencilla, el propietario de la información puede indicar hasta dónde puede circular la información más allá del receptor inmediato, y éste debe consultar al propietario de la información cuando la información necesite ser distribuida a terceros.

TLP	Niveles de Clasificación de la Información (Confidencialidad)	Descripción
		confidencialidad y con el conocimiento y consentimiento del Propietario de la misma.
TLP:AMBER	RESTRINGIDA (**RST**)	Información sensible, interna a áreas o proyectos a los que debe tener acceso controlado un departamento, miembros del proyecto, de un comité, etc., pero no toda la empresa, y que deber ser protegida por su impacto en los intereses de la empresa, de sus clientes o asociados y empleados. También se incluye en esta categoría aquella información que contenga datos de carácter personal. Es decir, se debe utilizar cuando la información requiere ser distribuida de forma limitada, pero supone un riesgo para la privacidad, reputación u operaciones si es compartida fuera de la organización. Los receptores pueden compartir esta información únicamente con miembros de su propia organización que necesitan conocerla, y con clientes, proveedores o asociados que necesitan conocerla para protegerse a sí mismos o evitar daños. El emisor puede especificar restricciones adicionales para compartir esta información.
TLP:RED	RESERVADA (**RSV**)	Información de alta sensibilidad que debe ser protegida por su relevancia sobre decisiones estratégicas, impacto financiero, oportunidades de negocio, potencial de fraude o requisitos legales. Su manejo es nominal y en grupo reducido de personas, es decir, listas de distribución de acceso y gestión cerradas y con autorización previa del Propietario de la información. También se ha incluir en esta categoría aquella información que contenga datos personales considerados como especiales (datos de origen étnico o racial, salud, orientación sexual, afiliación sindical, opiniones políticas o religiosas y datos biométricos o genéticos). Se debe utilizar cuando la información está limitada a personas concretas, y podría tener impacto en la privacidad, reputación u operaciones si es mal utilizada. Los receptores no deben compartir esta información con ningún tercero fuera del ámbito donde fue expuesta originalmente

Se utilizará el código de colores para identificar de forma ágil y sencilla el nivel de clasificación de la información.
Por defecto, cualquier información no clasificada se tratará como USO INTERNO, por lo que su divulgación debe ser autorizada por su Propietario.
Así mismo, la decisión de desclasificar o reclasificar (cambiar de nivel de clasificación) una información será potestad de la persona que desempeñe la autoridad del puesto que hubiese clasificado dicha información o por su superior jerárquico. Adicionalmente, el propietario de la información, deberá llevar a cabo de forma periódica la revisión de la clasificación de la información de la que es propietario.
El Responsable de Seguridad de los sistemas de información, como parte de sus tareas de supervisión de la Seguridad de los mismos, podrá recomendar al Propietario de la Información que modifique una clasificación cuando ésta se considere errónea, o bien cuando la misma ponga en peligro la confidencialidad.
En caso de que esta recomendación no sea atendida, elevará la misma al superior jerárquico del propietario de la información, advirtiéndole del peligro de la clasificación errónea de la información en cuestión.
Por otro lado, la decisión de clasificación puede ser implícita o expresa.
Los siguientes documentos tienen la clasificación especificada por defecto, salvo que el Propietario del documento lo modifique.

TLP	Clasificación de la Información	Documentos
TLP:WHITE	INFORMACIÓN PÚBLICA (**IPU**)	- Política, Manual de Gestión y Mapa de Procesos - Tarifas vigentes de servicios. Promociones, etc.
TLP:GREEN	USO INTERNO (**UIN**)	- Fichas de Proceso, Procedimientos Generales, Manuales (de estilo, marca…) - Informes de mercado, Organigramas y listines de teléfono - Normativas, Procedimientos Internos, Descripción de Sistemas, etc., (por ejemplo: afectado por la LOPD), etc.
TLP:AMBER	RESTRINGIDA (**RST**)	- Procedimientos Específicos, Hojas de Datos - Información que legal o contractualmente se establece como confidencial - Información que pueda suponer un riesgo reputacional para las entidades del Grupo ACME. - Análisis de Riesgos. - Informes de Auditoría Interna (salvo que, por su contenido estratégico, tengan la consideración de información reservada). - Secretos comerciales, estudios y análisis de clientes, tarifas de futuros servicios - Organigramas y reestructuraciones no publicadas, etc. - **Documentos que contengan datos de carácter personal NO considerados reservados de acuerdo con la clasificación TLP: RED**
TLP:RED	RESERVADA (**RSV**)	- Documentación técnica (know-how) - Documentos relativos a Gestión de Riesgos (Seguridad Física, Seguridad en la Circulación, Prevención de Riesgos, y Seguridad TIC´s). - Documento de Pase a Producción. - Información estratégica (Actas del Comité de Dirección, Consejo de Administración…)

TLP	Clasificación de la Información	Documentos

		- Información relativa a investigaciones internas de Compliance.
		- Resultados financieros de la empresa aprobados, pero no publicados.
		- Información de alianzas o adquisiciones estratégicas futura, información de nuevos servicios estratégicos para la empresa, estudios de entrada de nuevos mercados, etc.
		- **Documentos que contengan información de carácter personal de categorías especiales, es decir, que incluyan:**
		  - **Datos de origen étnico o racial**
		  - **Datos de salud**
		  - **Datos sobre orientación sexual**
		  - **Datos sobre afiliación sindical**
		  - **Datos sobre opiniones políticas o religiosas.**
		  - **Datos biométricos o genéticos**

7. TRATAMIENTO DE LA INFORMACIÓN RESERVADA Y RESTRINGIDA

Las fases del ciclo de vida de la información son las siguientes:

1. **Generación y clasificación e identificación de la información interna**: el Propietario de la información es el que la genera, y marca la información según el tipo de soporte:

   Formato papel: llevará en lugar visible, por ejemplo, a continuación del símbolo y leyenda de protección de derechos de copia, reproducción, distribución y utilización, cuando exista, o en el pie de página, el literal que corresponde según el nivel de confidencialidad.

   - Información pública (IPU) **TLP: WHITE**
   - Información para uso interno (UIN) **TLP: GREEN**
   - Información restringida (RST) **TLP: AMBER**
   - Información reservada (RSV) **TLP: RED**

   Formato electrónico: los archivos llevarán por ejemplo la siguiente denominación. “XXX_INFORME CUENTA DE RESULTADOS”.

2. **Recepción, clasificación e identificación de información:**
   a. Procedente del Interior. Si el receptor de la información generada (con origen) en el interior de la empresa, recibe documentación no clasificada, deberá proceder conforme al punto 4. de este mismo apartado. Si no obtuviera respuesta, o no pudiera localizar al Propietario (por ejemplo, por cambios Organizativos), deberá entender que como mínimo debe ser tratada como Información de Uso Interno (UIN).
   b. Procedente del exterior: el receptor de la información con origen en el exterior del Grupo ACME pasa a ser el Propietario de la misma, y debe identificar su clasificación de forma visible.

   En ambos casos, si la información no ha sido etiquetada en Origen:

a. Si el Formato es electrónico debe renombrarse conforme al "Formato Electrónico" del punto 1, del presente apartado.
b. Si el Formato es en Papel: Si es posible se estampará con un sello la clasificación, en el caso que no fuera posible o resultara una carga excesiva o fuera inviable, puede marcarse la clasificación en la portada, carpeta, archivador o hoja que haga las veces de portada.

3. **Almacenamiento**: el Propietario y los responsables de Almacenamiento, con el apoyo del departamento de Seguridad de la Información (si fuera preciso), establecerán los controles necesarios para los distintos soportes, garantizando los niveles de protección adecuados para cada información.
4. **Distribución y acceso**: se efectuará siempre con el marcado preceptivo de la información, en el caso contrario el receptor, responsable de su distribución, reclamará la clasificación al Propietario.

   La distribución y acceso debe ser autorizada por el Propietario, y se realizará según su clasificación:

   - Pública **TLP: WHITE**. No existen restricciones de acceso.
   - Uso Interno **TLP: GREEN**. Se restringe a miembros de la empresa.
   - Restringida **TLP: AMBER**. Acceso limitado a un grupo de usuarios definido por el Propietario. Puede ser un departamento, colectivo, miembros de un equipo de trabajo o proyecto, etc.
   - Reservada **TLP: RED**. Su acceso y distribución será nominal.

   Será responsabilidad del Propietario de la información Restringida y Reservada mantener actualizados los grupos de usuarios o miembros que deben acceder a dicha información.
5. **Copias**: el número de copias que pueden generarse atenderá al nivel de clasificación, de tal manera:

   - Pública **TLP: WHITE**. No hay límite impuesto.
   - Uso Interno **TLP: GREEN**. Solo se podrán generar copias para uso profesional.
   - Restringida **TLP: AMBER**. Solo podrán realizar copias el personal autorizado por parte del Propietario de la Información. Puede ser un departamento, colectivo, miembros de un equipo de trabajo o proyecto, etc.
   - Reservada **TLP: RED**. Únicamente el Propietario de la Información podrá realizar copias.

6. **Destrucción**: inspección y borrado tanto de metadatos, como de otros datos ocultos asociados a los documentos electrónicos.

   Para la información reservada se utilizarán programas de borrado seguro, si es en formato electrónico y mediante destructora o trituradora si es formato físico.
   Por otra parte, hay que hacer una mención especial sobre los metadatos y datos ocultos registrados en determinados documentos. Este tipo de información puede contener datos sensibles, a veces desconocidos por los usuarios de la información,

con el consiguiente riesgo que ello supone ante la posibilidad de revelar dicha información cuando el documento salga fuera de su ámbito de seguridad.

En el caso de tratarse sistemas de información con categoría Reservada **TLP: RED**, se deberá consultar con la Gerencia de Ciberseguridad y Privacidad del método apropiado para su destrucción

Para evitar este riesgo se deberán establecer, a través de las instrucciones técnicas que en cada caso apliquen de buenas prácticas que ayuden a realizar la inspección y borrado tanto de metadatos, como de otros datos ocultos asociados a los documentos electrónicos, así como de borrado seguro. Las instrucciones técnicas serán elaboradas por el Responsable de Seguridad de los Sistemas de Información y aprobadas por el CSTIC.

En concreto debe consultarse la Instrucción técnica de borrado seguro y borrado metadatos IT.09 NS.04.PE.GRS.TIC.

8. REVISIÓN DE LA NORMA

El presente documento debe ser revisado y actualizado al menos una vez al año; o cuando surjan nuevas modificaciones que requieran de actualizar el presente documento. Siempre deberá ser aprobada por el Comité de Seguridad TIC.

ANEXO 2

ACME

INSTRUCCIÓN TÉCNICA
PROCESO A SEGUIR POR PARTE DEL RESPONSABLE DE LA INFORMACIÓN PARA LA CLASIFICACIÓN DE LA MISMA

Elaborado:	Revisado:	Aprobado:

CONTROL DE VERSIONES

Revisión	Fecha de Aprobación	Motivo de la Revisión

TLP: RED	La información está limitada a personas específicas y podría afectar la privacidad, la reputación o las operaciones si no se maneja correctamente.	Esta información no debe compartirse con terceros fuera del alcance en el que se presentó originalmente.
TLP: AMBER	La distribución de información debe ser limitada, pero representa un riesgo para la privacidad, la reputación o las operaciones si se comparte fuera de la organización.	La información solo se puede compartir con miembros de la propia organización del destinatario que la requieran, y con clientes, proveedores o asociados que la necesiten para protegerse o evitar daños. El remitente puede especificar restricciones adicionales para compartir esta información.
TLP: GREEN	La información es de utilidad para todas las organizaciones participantes y terceros de la comunidad o sector	Los destinatarios pueden compartir la información con terceros afiliados o miembros del mismo sector, pero esto nunca debe hacerse a través de canales públicos.
TLP: CLEAR	La información no presenta ningún riesgo de mal uso, dentro de las normas y procedimientos establecidos para su difusión pública.	La información se puede distribuir sin restricciones, dentro de los límites impuestos por los derechos de autor.

1. INTRODUCCIÓN

La información es el activo más importante del Grupo ACME. Por tanto, es necesario proteger este activo y para ello se deben poner a disposición de los responsables o propietarios de la información del Grupo ACME los mecanismos necesarios que permitan su protección.

Uno de estos mecanismos, es la Norma "NS-04 Norma de Clasificación de la información" que define las categorías de información del Grupo ACME, y establece un procedimiento de clasificación de esta y de las medidas de protección aplicables a su manejo, almacenamiento y, en su caso, destrucción.

Adicionalmente otro de estos mecanismos, es la presente Instrucción Técnica, la cual pretende permitir al Responsable o propietario de la información clasificar la información bajo su responsabilidad ayudándose de la definición de confidencialidad de la información para así llegar a clasificar la información en uno de los niveles de clasificación citados en la anterior Norma.

Es relevante tener en cuenta la importancia de una correcta clasificación de la información, y no infravalorar ni supervalorar la información, puesto que es necesario establecer de forma correcta las medidas de seguridad pertinentes en función de la clasificación establecida.

2. ALCANCE

La información del Grupo ACME debe ser clasificada siguiendo la presente Instrucción y siguiendo la estructura indicada en la Norma "NS-04 Norma de Clasificación de la información".

El ámbito de aplicación de la presente instrucción debe ser aplicado por el Responsable de la Información para clasificar la siguiente información bajo su responsabilidad:

- Información tratada internamente por empleados del Grupo ACME y por las filiales que pertenecen a dicho Grupo.
- Información tratada por personal adscrito a un servicio adjudicado a un proveedor del Grupo ACME.

3. COMO LLEVAR A CABO LA CLASIFICACIÓN DE LA INFORMACIÓN POR EL RESPONSABLE DE LA INFORMACIÓN

Las funciones del Responsable o propietario de la Información, en relación con la clasificación de la misma, tal y como se establece en la Norma "NS-04 Norma de Clasificación de la Información" del Grupo ACME, son las siguientes:

- Es el responsable de área o cargo directivo del Grupo ACME que tiene la decisión sobre la finalidad, contenido y uso de la información que genera.

- Tiene la capacidad de poder clasificar, desclasificar o reclasificar una información, así como la responsabilidad de establecer y velar por el cumplimiento de los controles de seguridad requeridos.
- El Propietario de la información es el que genera la misma, y debe marcarla según el tipo de soporte.
- el Propietario, junto con los responsables de Almacenamiento y con el apoyo del departamento de Seguridad de la Información (si fuera preciso), establecerán los controles necesarios para los distintos soportes, garantizando los niveles de protección adecuados para cada información.
- Debe autorizar la distribución y acceso a la información, y se realizará según su clasificación.
- Tiene la responsabilidad de mantener actualizados los grupos de usuarios o miembros que deben acceder a la información Restringida y Reservada.
- En caso de que el Responsable de Seguridad de los Sistemas de Información le informe de que es necesario modificar una clasificación cuando ésta se considere errónea, o bien cuando la misma ponga en peligro la confidencialidad, deberá valorar y en su caso atender a la solicitud.

Tal y como se indica anteriormente, el Responsable de la Información debe encargarse de clasificar la información en base a los 4 niveles y su correspondiente valor del Traffic Light Protocol (TLP) de INCIBE[4], que se indican en la "NS-04 Norma de Clasificación de la información", y que son los siguientes (ver ANEXO I de la presente Instrucción):

A. RESERVADA (RSV) -> TLP: RED
B. RESTRINGIDA (RST) -> TLP: AMBER
C. USO INTERNO (UIN) -> TLP: GREEN
D. INFORMACIÓN PÚBLICA (IPU) -> TLP: CLEAR

Para clasificar la información en base a estos niveles, el Responsable de la Información debe hacer uso del criterio de valoración de la dimensión se seguridad de "confidencialidad de la información", según lo indicado en la Guía de Seguridad CCN-STIC-803 y que se expone a continuación:

A. Una determinada información será clasificada como RESERVADA (TLP: RED) cuando la valoración de la dimensión de seguridad de la "confidencialidad de la información" sea de nivel **ALTO**, lo que implica que Responsable de la información identifica, al menos, como aplicable uno de los siguientes aspectos en relación con la información a clasificar:
    - porque la información debe conocerla un número muy reducido de personas

[4] Traffic Light Protocol (TLP) es un esquema creado para fomentar un mejor intercambio de información sensible en el ámbito de la seguridad de la información. A través de este esquema, de una forma ágil y sencilla, el propietario de la información puede indicar hasta dónde puede circular la información más allá del receptor inmediato, y éste debe consultar al propietario de la información cuando la información necesite ser distribuida a terceros.

- por disposición legal o administrativa: ley, decreto, orden, reglamento,
- porque su revelación causaría un grave daño, de difícil o imposible reparación
- porque su revelación supondría el incumplimiento grave de una norma
- porque su revelación causaría pérdidas económicas elevadas o alteraciones financieras significativas
- porque su revelación causaría un daño reputacional grave con los ciudadanos o con otras organizaciones
- porque su revelación podría desembocar en protestas masivas (alteración seria del orden público)

B. Una determinada información será clasificada como RESTRINGIDA (TLP: AMBER) cuando la valoración de la dimensión de seguridad de la "confidencialidad de la información" sea de nivel **MEDIO**, lo que implica que Responsable de la información identifica, al menos, como aplicable uno de los siguientes aspectos en relación con la información a clasificar y no ha identificado como aplicable ninguno de los asociados a un valor de nivel **ALTO**:
   - porque la información deben conocerla sólo quienes lo necesiten para su trabajo, con autorización explícita
   - por disposición legal o administrativa: ley, decreto, orden, reglamento,
   - porque su revelación causaría un daño importante, aunque subsanable
   - porque su revelación supondría el incumplimiento material o formal de una norma
   - porque su revelación causaría pérdidas económicas importantes
   - porque su revelación causaría un daño reputacional importante con los ciudadanos o con otras organizaciones
   - porque su revelación podría desembocar en protestas públicas (alteración del orden público)

C. Una determinada información será clasificada como USO INTERNO (TLP: GREEN) cuando la valoración de la dimensión de seguridad de la "confidencialidad de la información" sea de nivel **BAJO**, lo que implica que Responsable de la información identifica al menos como aplicable uno de los siguientes aspectos en relación con la información a clasificar y no ha identificado como aplicable ninguno de los asociados a un valor de nivel **ALTO** ni **MEDIO**:
   - porque la información no deben conocerla personas ajenas a la organización
   - por disposición legal o administrativa: ley, decreto, orden, reglamento
   - porque su revelación causaría algún perjuicio
   - porque su revelación supondría el incumplimiento leve de una norma
   - porque su revelación supondría pérdidas económicas apreciables
   - porque su revelación causaría un daño reputacional apreciable con los ciudadanos o con otras organizaciones
   - porque su revelación podría desembocar en múltiples protestas individuales

D. Una determinada información será clasificada como INFORMACIÓN PÚBLICA (TLP: CLEAR) cuando la valoración de la dimensión de seguridad de la "confidencialidad de la información" sea "no valorable" o "no adscrita", lo que implica que Responsable de la

información identifica que la información es “información de carácter público, accesible por cualquier persona”.

4. APLICACIÓN DE LA CLASIFICACIÓN DE LA INFORMACIÓN

En el presente apartado se incluirán, por parte de la Gerencia de Ciberseguridad y Privacidad, aquellas situaciones en las que la clasificación de la información por parte de su Responsable (Responsable de la Información) determine de forma directa o indirecta una decisión sobre cómo se debe tratar la información:

4.1 TRATAMIENTO DE LA INFORMACIÓN EN CORREO ELECTRÓNICO

En el caso en el que el Responsable de la Información haya clasificado información que va ser tratada por personal interno del Grupo ACME, o por personal de las filiales del Grupo ACME, o por personal adscrito a un servicio del Grupo ACME, con un valor de confidencialidad de nivel **MEDIO** o **ALTO** lo que equivale a un clasificación RESTRINGIDA (TLP: AMBER) o RESERVADA (TLP: RED), la información debe ser tratada en cuentas de correo electrónico que pertenezcan a un dominio interno de ACME (@ACME.es o @colaboradores.ACME.es).

- De esta forma la información se ve protegida con las medidas de seguridad y de monitorización descritas en:NS-09 Norma de Uso aceptable de los medios informáticos
- NS-11 Norma de Gestión de Incidentes de Seguridad

4.2 EMPLEO DE EQUIPOS PROPIEDAD DE ACME POR PERSONAL EXTERNO ADSCRITO A UN SERVICIO

En el caso en el que el Responsable de la Información haya clasificado información que va ser tratada por personal adscrito a un servicio del Grupo ACME, con un valor de confidencialidad de nivel **MEDIO** o **ALTO** lo que equivale a una clasificación RESTRINGIDA (TLP: AMBER) o RESERVADA (TLP: RED), este personal deberá utilizar equipos propiedad de ACME.

De esta forma, la información se ve protegida con las medidas de seguridad y de monitorización de las que disponen los equipos propiedad de ACME, descritas en:

- NS-09 Norma de Uso aceptable de los medios informáticos
- NS-11 Norma de Gestión de Incidentes de Seguridad

En el caso en el que el Responsable de la Información haya clasificado información que va ser tratada por personal adscrito a un servicio del Grupo ACME, con un valor de confidencialidad de nivel **BAJO**, lo que equivale a una clasificación de USO INTERNO (TLP: GREEN), o como INFORMACIÓN PÚBLICA (TLP: CLEAR), siempre y cuando exista autorización expresa de la Gerencia de Ciberseguridad y Privacidad, y se cumplan las medidas de seguridad recogidas en los procedimientos de Seguridad “PS-19 Procedimiento de acceso activos terceros a red de ACME” y

“PS-21 Procedimiento de acceso a instalaciones, redes, sistemas o información del Grupo ACME”, este personal podrá utilizar equipos de la empresa adjudicataria del servicio.

5. REVISIÓN DE LA INSTRUCCIÓN

El presente documento debe ser revisado y actualizado al menos una vez al año; o cuando surjan nuevas necesidades de capacitación que resulten de aplicación para la figura de Responsable de Seguridad de los Sistemas de Información.

ANEXO I. NIVELES DE CLASIFICACIÓN DE LA INFORMACIÓN

TLP	Niveles de Clasificación de la Información (Confidencialidad)	Descripción
TLP:CLEAR	INFORMACIÓN PÚBLICA (**IPU**)	Información cuya divulgación no afecte a la empresa en términos de pérdida de imagen y/o económica. Se debe utilizar cuando la información no supone ningún riesgo de mal uso, dentro de las reglas y procedimientos establecidos para su difusión pública.
TLP:GREEN	USO INTERNO (**UIN**)	Información que, sin ser reservada ni restringida, debe mantenerse en el ámbito interno de la empresa y no debe estar disponible externamente a través de canales públicos, excepto a terceras partes involucradas previo compromiso de confidencialidad y con el conocimiento y consentimiento del Propietario de la misma.
TLP:AMBER	RESTRINGIDA (**RST**)	Información sensible, interna a áreas o proyectos a los que debe tener acceso controlado un departamento, miembros del proyecto, de un comité, etc., pero no toda la empresa, y que deber ser protegida por su impacto en los intereses de la empresa, de sus clientes o asociados y empleados. Es decir, se debe utilizar cuando la información requiere ser distribuida de forma limitada, pero supone un riesgo para la privacidad, reputación u operaciones si es compartida fuera de la organización. Los receptores pueden compartir esta información únicamente con miembros de su propia organización que necesitan conocerla, y con clientes, proveedores o asociados que necesitan conocerla para protegerse a sí mismos o evitar daños. El emisor puede especificar restricciones adicionales para compartir esta información. **Nota**: se debe especificar **TLP:AMBER+STRICT**, si la fuente desea restringir la compartición sólo a la propia organización.
TLP:RED	RESERVADA (**RSV**)	Información de alta sensibilidad que debe ser protegida por su relevancia sobre decisiones estratégicas, impacto financiero, oportunidades de negocio, potencial de fraude o requisitos legales. Su manejo es nominal y en grupo reducido de personas, es decir, listas de distribución de acceso y gestión cerradas y con autorización previa del Propietario de la información. Se debe utilizar cuando la información está limitada a personas concretas, y podría tener impacto en la privacidad, reputación u operaciones si es mal utilizada. Los receptores no deben compartir esta información con ningún tercero fuera del ámbito donde fue expuesta originalmente

ANEXO II. NIVELES DE CLASIFICACIÓN DE LA INFORMACIÓN EN FUNCIÓN DE LA VALORACIÓN DE LA CONFIDENCIALIDAD DE LA INFORMACIÓN

Valoración de la Confidencialidad de la Información	TLP	Niveles de Clasificación de la Información (Confidencialidad)	Descripción
NO VALORABLE	**TLP:CLEAR**	INFORMACIÓN PÚBLICA (**IPU**)	Información cuya divulgación no afecte a la empresa en términos de pérdida de imagen y/o económica. Se debe utilizar cuando la información no supone ningún riesgo de mal uso, dentro de las reglas y procedimientos establecidos para su difusión pública.
BAJA	**TLP:GREEN**	USO INTERNO (**UIN**)	Información que, sin ser reservada ni restringida, debe mantenerse en el ámbito interno de la empresa y no debe estar disponible externamente a través de canales públicos, excepto a terceras partes involucradas previo compromiso de confidencialidad y con el conocimiento y consentimiento del Propietario de la misma.
MEDIA	**TLP:AMBER**	RESTRINGIDA (**RST**)	Información sensible, interna a áreas o proyectos a los que debe tener acceso controlado un departamento, miembros del proyecto, de un comité, etc., pero no toda la empresa, y que deber ser protegida por su impacto en los intereses de la empresa, de sus clientes o asociados y empleados. Es decir, se debe utilizar cuando la información requiere ser distribuida de forma limitada, pero supone un riesgo para la privacidad, reputación u operaciones si es compartida fuera de la organización. Los receptores pueden compartir esta información únicamente con miembros de su propia organización que necesitan conocerla, y con clientes, proveedores o asociados que necesitan conocerla para protegerse a sí mismos o evitar daños. El emisor puede especificar restricciones adicionales para compartir esta información. **Nota**: se debe especificar **TLP:AMBER+STRICT**, si la fuente desea restringir la compartición sólo a la propia organización.
ALTA	**TLP:RED**	RESERVADA (**RSV**)	Información de alta sensibilidad que debe ser protegida por su relevancia sobre decisiones estratégicas, impacto financiero, oportunidades de negocio, potencial de fraude o requisitos legales. Su manejo es nominal y en grupo reducido de personas, es decir, listas de distribución de acceso y gestión cerradas y con autorización previa del Propietario de la información. Se debe utilizar cuando la información está limitada a personas concretas, y podría tener impacto en la privacidad, reputación u operaciones si es mal utilizada.

Valoración de la Confidencialidad de la Información	TLP	Niveles de Clasificación de la Información (Confidencialidad)	Descripción
			Los receptores no deben compartir esta información con ningún tercero fuera del ámbito donde fue expuesta originalmente

ANEXO III. RESTRICCIONES EN EL USO DE LA INFORMACIÓN EN FUNCIÓN DE SU CLASIFICACIÓN

1 IPU: Información Pública

Actividad	Restricciones
Etiquetado	Los documentos deben llevar la etiqueta TLP:CLEAR
Difusión	De libre acceso
Acceso lógico	Sin restricción específica
Impresión	Sin restricción específica
Traducción	Se autoriza el uso de traductores online
Intercambio	Sin restricción específica
Almacenamiento	Sin restricción específica
Archivado	Sin restricción específica
Destrucción	Sin restricción específica

2 UIN: Uso Interno

Actividad	Restricciones
Etiquetado	Los documentos deberán estar fechados y manejar un número de referencia y un asunto. Cada página deberá estar numerada y marcada claramente con la etiqueta TLP: GREEN
Difusión	De libre acceso para cualquier usuario y colaborador con acuerdo de confidencialidad de la información y acceso a las redes, sistemas de Información, o información de ACME. Sin embargo, esta información no se publicará en internet ni se divulgará la exterior.
Acceso lógico	Sin restricción específica
Impresión	Sin restricción específica
Traducción	Se evitará el empleo de traductores online. En caso de disponer el Grupo ACME de un software específico para la traducción de documentación, será éste el mecanismo corporativo para dicha actividad.
Intercambio	El uso de plataformas de intercambio de información online no está autorizado (tales como WeTransfer, TrasferNow, Dropbox, TransferXL, Google Drive, …). Para esta actividad se debe emplear siempre los mecanismos corporativos existentes (OneDrive, OwnCloud, SharePoint, …), y siempre entre usuarios internos o usuarios colaboradores, a través de sus cuentas corporativas o colaborativas.
Almacenamiento	El uso de plataformas de intercambio de información online no está autorizado (tales como WeTransfer, TrasferNow, Dropbox, TransferXL, Google Drive, …).

	Para esta actividad se debe emplear siempre los mecanismos corporativos existentes (Carpetas de Red, OneDrive, OwnCloud, SharePoint, …), a través de sus cuentas corporativas o colaborativas.
Archivado	Sin restricción específica
Destrucción	Para la versión impresa, se empleará una trituradora

3 RST: Restringida

Actividad	Restricciones
Etiquetado	Los documentos deberán estar fechados y manejar un número de referencia y un asunto. Cada página deberá estar numerada y marcada claramente con la etiqueta TLP: AMBER
Difusión	Acceso restringido en el perímetro definido para un departamento, miembros del proyecto, de un comité, etc., con acuerdo de confidencialidad de la información y acceso a las redes, sistemas de Información, o información de ACME.
Acceso lógico	**Se debe implementar un mecanismo de autenticación estándar**
Impresión	**La versión impresa debe almacenarse en un escritorio cerrado.**
Traducción	El uso de traductores en línea no está autorizado. En caso de disponer el Grupo ACME de un software específico para la traducción de documentación, será éste el mecanismo corporativo para dicha actividad.
Intercambio	Los datos deben cifrase in-transit (en tránsito). El uso de plataformas de intercambio de información online no está autorizado (tales como WeTransfer, TrasferNow, Dropbox, TransferXL, Google Drive, …). Para esta actividad se debe emplear siempre los mecanismos corporativos existentes (OneDrive, OwnCloud, SharePoint, …), y siempre entre usuarios internos o usuarios colaboradores, a través de sus cuentas corporativas o colaborativas. Adicionalmente, se debe contar con los permisos correctos y delimitados para cada uno de los usuarios involucrados. Se han de revisar los permisos periódicamente para evitar mantener esta información expuesta de manera deliberada indefinidamente en el tiempo
Almacenamiento	Los datos deben encontrarse cifrados at-rest (en reposo). El uso de plataformas de intercambio de información online no está autorizado (tales como WeTransfer, TrasferNow, Dropbox, TransferXL, Google Drive, …). Para esta actividad se debe emplear siempre los mecanismos corporativos existentes (Carpetas de Red, OneDrive, OwnCloud, SharePoint, …), a través de sus cuentas corporativas o colaborativas. Adicionalmente, se debe contar con los permisos correctos y delimitados para cada uno de los usuarios involucrados. Se han de revisar los permisos periódicamente para evitar mantener esta información expuesta de manera deliberada indefinidamente en el tiempo.
Archivado	Los datos deben encontrarse cifrados at-rest (en reposo)
Destrucción	Para la versión impresa, se utilizará una trituradora

4 RSV: Reservada

Actividad	Restricciones
Etiquetado	Los documentos deberán estar fechados y manejar un número de referencia y un asunto. Cada página deberá estar numerada y marcada claramente con la etiqueta TLP: RED
Difusión	Los destinatarios no pueden compartir información de esta categoría con ninguna parte fuera de las personas implicadas en la reunión o conversación específica en la que se reveló originalmente.
Acceso lógico	**Se debe implementar un mecanismo de autenticación estándar**
Impresión	**La versión impresa debe almacenarse en un escritorio cerrado y seguro.** **Los documentos deberán tener un número de copia en cada página, si se van a distribuir en varias copias.** **Cada propietario de una versión impresa será identificado por el originador.**
Traducción	El uso de traductores en línea no está autorizado. Los documentos no se copiarán ni traducirán sin el consentimiento previo por escrito del autor. En caso de disponer el Grupo ACME de un software específico para la traducción de documentación, será éste el mecanismo corporativo para dicha actividad.
Intercambio	Los datos deben cifrase in-transit (en tránsito). El uso de plataformas de intercambio de información online no está autorizado (tales como WeTransfer, TrasferNow, Dropbox, TransferXL, Google Drive, …). Para esta actividad se debe emplear siempre los mecanismos corporativos existentes (OneDrive, OwnCloud, SharePoint, …), y siempre entre usuarios internos o usuarios colaboradores, a través de sus cuentas corporativas. Adicionalmente, se debe contar con los permisos correctos y delimitados para cada uno de los usuarios involucrados. Se han de revisar los permisos periódicamente para evitar mantener esta información expuesta de manera deliberada indefinidamente en el tiempo.
Almacenamiento	Los datos deben encontrarse cifrados at-rest (en reposo). El uso de plataformas de intercambio de información online no está autorizado (tales como WeTransfer, TrasferNow, Dropbox, TransferXL, Google Drive, …). Para esta actividad se debe emplear siempre los mecanismos corporativos existentes (Carpetas de Red, OneDrive, OwnCloud, SharePoint, …), a través de sus cuentas corporativas. Adicionalmente, se debe contar con los permisos correctos y delimitados para cada uno de los usuarios involucrados. Se han de revisar los permisos periódicamente para evitar mantener esta información expuesta de manera deliberada indefinidamente en el tiempo.
Archivado	Los datos deben encontrarse cifrados at-rest (en reposo)
Destrucción	Para la versión impresa, se utilizará una trituradora

ANEXO 3

INFORMACIÓN COMPLEMENTARIA

Ejemplos de información en marcos de seguridad en relación con la clasificación de la información.

RD 311/2022, de 3 de mayo, por el que se regula el ENS

5.7.2 Calificación de la información [mp.info.2].

dimensiones	C		
nivel	BAJO	MEDIO	ALTO
	n.a.	aplica	aplica

Requisitos.

- [mp.info.2.1] Para calificar la información se estará a lo establecido legalmente por las leyes y tratados internacionales de los que España es miembro y su normativa de aplicación cuando se trate de materias clasificadas. El valor a emplear en el caso de información de materias no clasificadas sería USO OFICIAL para información con algún tipo de restricción en su manejo por su sensibilidad y confidencialidad.
- [mp.info.2.2] La política de seguridad establecerá quién es el responsable de cada información manejada por el sistema.
- [mp.info.2.3] La política de seguridad recogerá, directa o indirectamente, los criterios que, en cada organización, determinarán el nivel de seguridad requerido, dentro del marco establecido en el artículo 40 y los criterios generales señalados en el anexo I.
- [mp.info.2.4] El responsable de cada información seguirá los criterios determinados en el apartado anterior para asignar a cada información el nivel de seguridad requerido, y será responsable de su documentación y aprobación formal.
- [mp.info.2.5] El responsable de cada información en cada momento tendrá en exclusiva la potestad de modificar el nivel de seguridad requerido, de acuerdo a los apartados anteriores.

Aplicación de la medida (por confidencialidad).

– Nivel BAJO: no aplica.
– Nivel MEDIO: mp.info.2.
– Nivel ALTO: mp.info.2

En el Anexo I del ENS se detalla como valorar la información en cada una de las cinco dimensiones de la seguridad (confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad) obteniendo un nivel que puede ser BAJO, MEDIO o ALTO. A partir de dicha valoración, la medida de seguridad [org.3.4] señala que se dispondrá de documentación que señale como tratar la información en función del precitado nivel de seguridad:

3.3 Procedimientos de seguridad [org.3]

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

Se dispondrá de una serie de documentos que detallen de forma clara y precisa cómo operar los elementos del sistema de información:

(…)

- [org.3.4] La forma en que se ha de tratar la información en consideración al nivel de seguridad que requiere, precisando cómo efectuar:
    a) Su control de acceso.
    b) Su almacenamiento.
    c) La realización de copias.
    d) El etiquetado de soportes.
    e) Su transmisión telemática.
    f) Cualquier otra actividad relacionada con dicha información.

ISO/IEC 27001:2022

La clasificación de la información según ISO 27001 es un proceso en el que la organización evalúa los datos que posee y el nivel de protección que cada uno requiere. Se trata de uno de los aspectos más complejos, pero sin duda más interesantes, en la gestión de la seguridad de la información.

ID.AM-5: los recursos se priorizan en función de su clasificación, criticidad y valor empresarial

ID.RA-1: …la clasificación de datos puede ayudar a determinar los activos o, en algunos casos, los pasivos que se encuentran ocultos en los documentos. Tener todos los documentos clasificados y etiquetados de acuerdo con la confidencialidad mostrará el riesgo que corre la empresa.

PR.AC-4: …para controlar eficazmente el acceso a los recursos y activos de información, debe clasificar los documentos de acuerdo con su clasificación de confidencialidad. Solo así la organización puede obtener una visión general y restringir el acceso a la información confidencial.

PR.DS-1: Los datos en reposo están protegidos. La clasificación de datos ayuda a proteger los datos según su criticidad.

PR.DS-2: Los datos en tránsito están protegidos. La clasificación de datos ayuda a proteger los datos según su criticidad.

PR.DS-3: …la clasificación de datos ayuda a proteger los datos de acuerdo con su criticidad y elimina la información confidencial que ya no tiene ningún valor.

PR.DS-5: …al tener clasificados los datos no estructurados, puede aplicar la protección adecuada de la información crítica y predecir la fuga de datos.

PR.IP-6: …haber clasificado sus documentos no estructurados lo ayudará a identificar aquellos documentos que puede y debe eliminar.

DE.AE-4: …haber clasificado sus datos no estructurados lo ayudará a obtener una descripción general de los impactos de un evento. El impacto es mucho mayor si alguien obtiene acceso a una máquina con muchos documentos confidenciales que un dispositivo con solo registros públicos.

ID: Identificación / AM -Asset Management / RA - Risk Assesment

PR: Protección /AC -Autenticación y Access Control /DS Data Security/IP Information Protection Processes & Procedures /

DE: Detect /AE -Anomalies and Events