Trazabilidad del dato en el contexto del Esquema Nacional de Seguridad (ENS)

Abstract: *el incremento de las organizaciones, ya pertenezcan al sector público o al privado, que confían en los datos para dirigir sus operaciones institucionales o de negocio, está haciendo que la seguridad centrada en los datos esté creciendo más que nunca.*

Contenido:

1 OBJETO

Los controles de seguridad sobre los datos se basan en un enfoque que enfatiza la seguridad de los propios datos sobre la seguridad de los dispositivos, aplicaciones, servidores o redes.

La transformación digital, el incremento del teletrabajo propiciado no solo por el convencimiento en su flexibilidad, sino por situaciones acaecidas de contingencia generalizada, **han provocado que el perímetro físico y lógico de las organizaciones se diluya cada vez más**.

En consecuencia, el incremento de las organizaciones, ya pertenezcan al sector público o al privado, que confían en los datos para dirigir sus operaciones institucionales o de negocio, está haciendo que **la seguridad centrada en los datos esté creciendo más que nunca**. Con los datos corporativos almacenados en diferentes localizaciones, tales como la nube, sistemas locales, bases de datos distribuidas, etc., **se refuerza la necesidad de establecer requisitos mínimos y estrategias de seguridad como Zero-Trust**.[1]

Existen diferentes elementos clave para un eficaz sistema de seguridad centrado en los datos:

- **Identificación, descubrimiento y clasificación de la información sensible:** el objetivo de un atacante, sea interno o externo, suele ser la información más

[1] *Confianza Cero* consiste en que los dispositivos conectados no deben ser considerados confiables, independientemente de que estos estén vinculados y verificados desde una red corporativa. https://www.sealpath.com/blog/zero-trust-security-model-implement-strategy/

sensible y valiosa: datos a través de los cuales, de forma directa o indirecta, puede obtener beneficios.

- **Protección centrada en los datos:** los controles de seguridad centrados en los datos se basan en asegurar el contenido valioso de la organización, de forma que pueda estar protegido frente a una posible salida no autorizada del sistema, de la red, de la nube o frente a cualquier exfiltración o fuga de datos.
- **Auditoría y seguimiento de accesos a los datos:** para determinar el nivel de riesgo sobre los datos corporativos, es importante poder analizar el uso de estos y determinar si los patrones de comportamiento de los usuarios sobre los datos se corresponden o no con un modelo o estándar determinado.
- **Administración y gestión de políticas sobre los datos:** quién debe o no tener permisos de acceso a los datos no es algo que pueda establecerse de forma permanente. Es necesario aplicar políticas dinámicas sobre los datos de forma que si se deja de colaborar con alguien o si se detecta que un determinado dato puede estar en riesgo pueda, no solo intentar impedirse que salga de la red corporativa, sino especialmente revocar el acceso al mismo con independencia de dónde se encuentre.

CARLA es la solución de protección centrada en los datos del CCN-CERT, que permite tener la documentación sensible de las organizaciones etiquetada, ya se encuentre en tránsito, en uso local, en uso remoto o preservada en reposo, minimizando así la posibilidad de fugas de datos y aumentando el control de la organización sobre la misma.

En este sentido, CARLA ayuda a las organizaciones a cubrir las limitaciones o retos de los equipos de seguridad a través de las siguientes características:

- **Protección que viaja con los datos:** CARLA aplica un etiquetado sobre la información que le acompaña allí donde se almacene o desplace. Esta protección se mantiene también fuera del perímetro de seguridad de la red, cuando se ha compartido la documentación con un tercero.
- **Trazabilidad y visibilidad sobre los datos:** CARLA permite monitorizar el fichero desde que se protege, dejando traza de quién accede, cuándo, con qué permisos, y si alguien intenta acceder sin permisos o desde una subred no permitida por la organización, con independencia de si la información está ubicada en dependencias ajenas a la organización (en casa de un empleado en teletrabajo, por ejemplo), en otro país o en equipos no controlados directamente por la organización o dentro de su perímetro de seguridad, (como puede ser un proveedor).
- **Control de acciones sobre el documento:** con CARLA se puede permitir que un usuario vea un documento, pero que no lo modifique, lo imprima o explore su contenido; pudiendo establecer permisos granulares sobre la información y

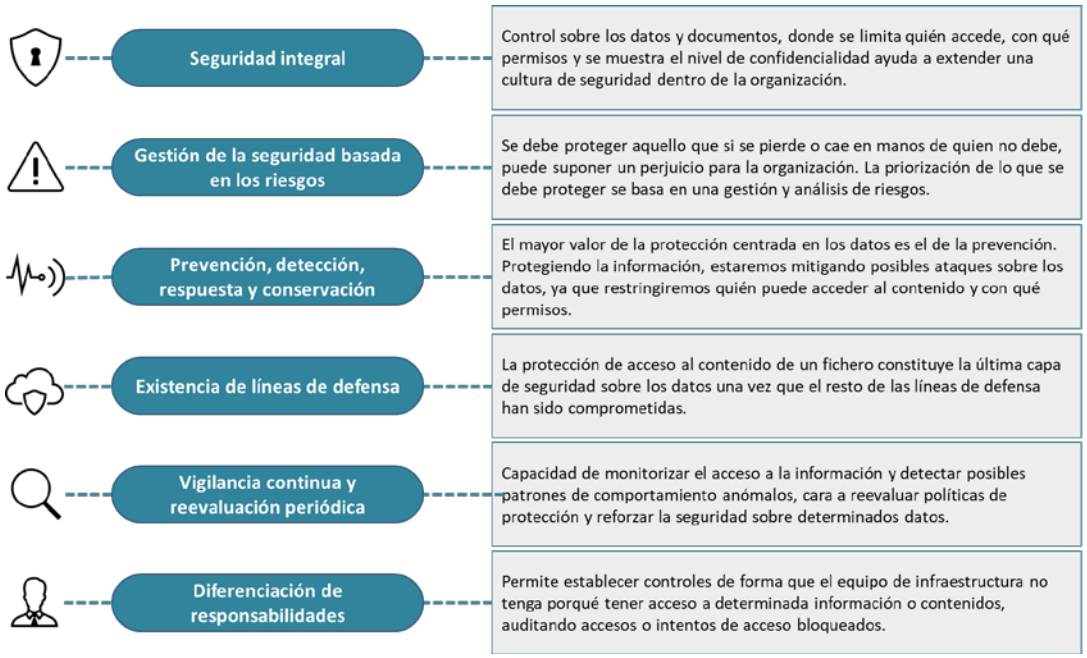
decidir el nivel de control que un tercero tiene sobre la información tratada por la organización. La protección es también en uso, pudiendo en todo momento mantenerse la propiedad sobre los datos corporativos.

- **Responder en tiempo real frente una posible fuga:** CARLA permite poner 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:** 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. CARLA no persigue bloquear las posibles vías de salida de información de la red, 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.

2 PRINCIPIOS BÁSICOS DEL ESQUEMA NACIONAL DE SEGURIDAD CENTRADOS EN EL DATO

El objeto último de la seguridad de la información es garantizar que una organización podrá cumplir sus objetivos, desarrollar sus funciones y ejercer sus competencias utilizando sistemas de información.

En este sentido, se destaca la relación de la seguridad centrada en los datos ofrecida por CARLA según los principios básicos señalados en el Esquema Nacional de Seguridad (ENS).



3 POLÍTICA DE SEGURIDAD, REQUISITOS MÍNIMOS Y SU RELACIÓN CON LA SEGURIDAD DEL DATO

Cada entidad del ámbito de aplicación del ENS debe contar con una política de seguridad formalmente aprobada por el órgano competente. La política de seguridad se establece de acuerdo con los principios básicos señalados anteriormente y se debe desarrollar aplicando los siguientes requisitos mínimos:

En el ámbito de los requisitos mínimos, y en relación a CARLA, cabe destacar:

- La seguridad centrada en los datos aplicada con CARLA exige una **priorización de qué información se debe proteger primero** y dónde tenemos el mayor riesgo sobre los datos.
- En el propio ADN de CARLA está la **configuración de accesos por mínimo privilegio**, dando sólo acceso a la información a quien lo necesita y a nadie más.
- CARLA permite la **protección tanto en tránsito, como en reposo y en uso**. La protección acompaña a la información allí donde viaja.
- CARLA **registra la actividad en el acceso al contenido** sobre la información, permitiendo relacionar los posibles incidentes con otros ocurridos en el perímetro o dispositivo.

3.1 TRAZABILIDAD DEL DATO Y CUMPLIMIENTO DEL ESQUEMA NACIONAL DE SEGURIDAD

A continuación, se muestran, dentro del modelo de medidas de seguridad del ENS, aquellas donde la seguridad centrada en los datos puede ayudar al **cumplimiento en base a dos (2) niveles de contribución: BÁSICO y MEDIO-ALTO**.

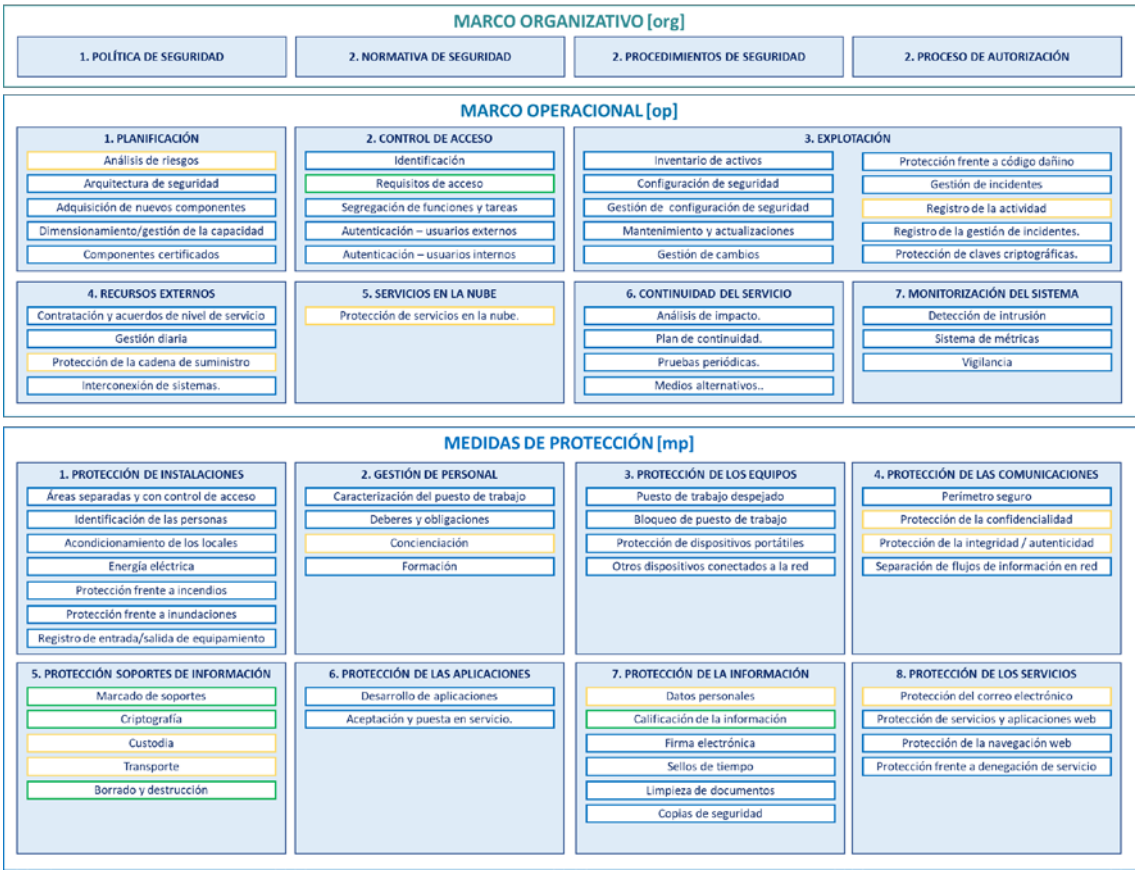
■ **Contribución BÁSICA:**

Aunque los requisitos del ENS abarcan significativamente más, CARLA contribuye o ayuda de forma básica al cumplimiento de la medida.

■ **Contribución MEDIA-ALTA:**

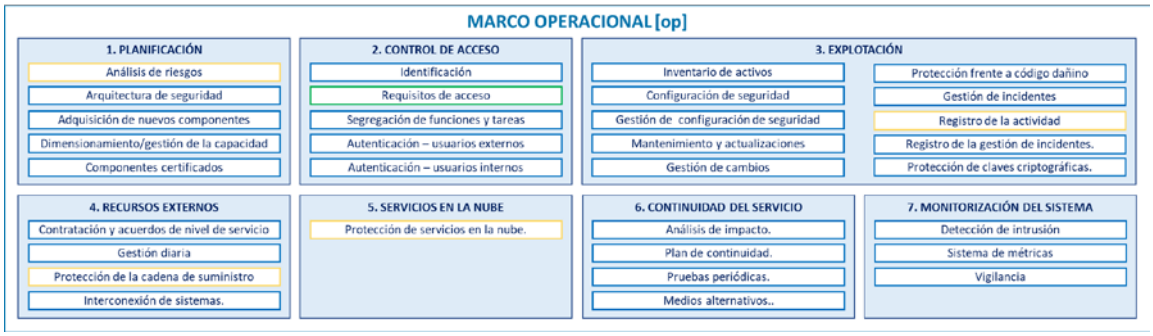
CARLA contribuye de forma media-alta al cumplimiento de la medida del ENS.

En los apartados posteriores se explica en qué grado CARLA contribuye a cada una de las medidas, que se muestran esquemáticamente en la siguiente tabla.



3.1.1 CARLA EN EL MARCO OPERACIONAL

En el ámbito del marco operacional cabe destacar las siguientes consideraciones de un enfoque de seguridad centrado en los datos a través de CARLA:

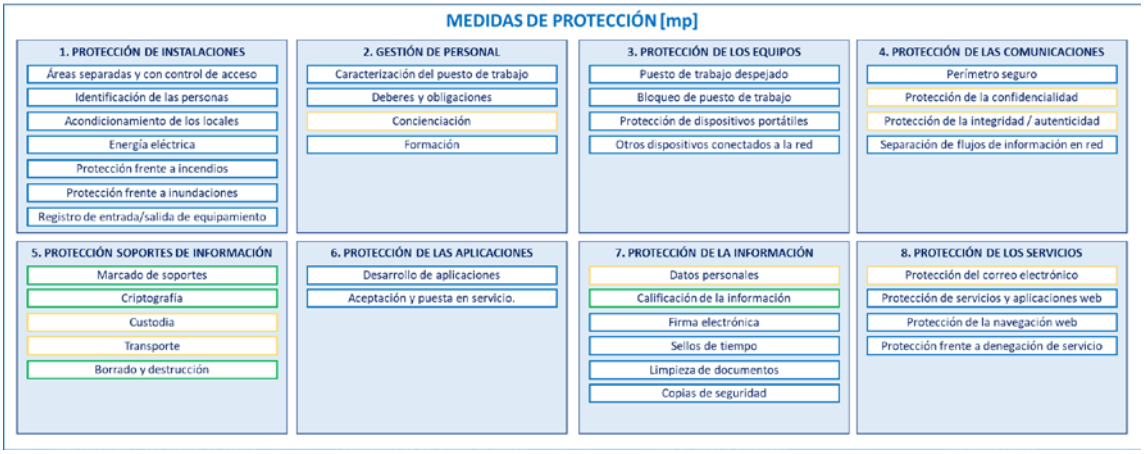


- **PLANIFICACIÓN [op.pl]**
  - **Análisis de Riesgos [op.pl.1]**
    - *A través de un enfoque de protección centrado en los datos, es necesario realizar previamente un análisis de riesgos para identificar los activos más valiosos, posibles amenazas y priorizar aquellos que se deben proteger. En función de los resultados del análisis de riesgos, no es necesario proteger todo, sino únicamente aquella documentación cuya pérdida puede causar daños importantes a la organización.*
    - ***Contribución: BÁSICA ■.***
- **CONTROL DE ACCESO [op.acc]**
  - **Requisitos de Acceso [op.acc.2]**
    - *Protegiendo los recursos del sistema y la documentación crítica, con mecanismos que impidan su utilización, salvo a las entidades que disfruten de derechos de acceso suficientes. Los privilegios de acceso sobre la documentación 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.*
    - ***Contribución: MEDIA-ALTA ■.***
- **EXPLOTACIÓN [op.exp]**
  - **Registro de Actividad [op.exp.8]**
    - *A través de CARLA 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.*
    - ***Contribución: BÁSICA ■.***
- **RECURSOS EXTERNOS [op.ext]**
  - **Protección de la Cadena de Suministro [op.ext.3]**
    - *Es complejo controlar el nivel de seguridad de información que se cede a la cadena de suministro. Con CARLA, 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.*
    - ***Contribución: BÁSICA ■.***

- **SERVICIOS EN LA NUBE [op.nub]**
  - **Protección de servicios en la nube [op.nub.1]**
    - *Independientemente del servicio de nube contratado, si éste se utiliza para almacenar información sensible, CARLA 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 el propio contenido. Esto permite que una brecha en la nube no tenga porqué suponer una pérdida o brecha de seguridad en la organización.*
    - ***Contribución: BÁSICA ■.***

3.1.2 CUMPLIMIENTO DE MEDIDAS DE PROTECCIÓN CON CARLA

Un enfoque de seguridad centrada en los datos a través de CARLA puede ayudar en las siguientes medidas de protección.



- **GESTIÓN DE PERSONAL [mp.per]**
  - **Concienciación [mp.per.3]**
    - *CARLA permite a los usuarios ver qué documentos han sido protegidos y con qué nivel de protección (permisos restringidos, marcas de agua, etc.). Esto permite incrementar el nivel de concienciación sobre la seguridad necesaria para la información sensible que gestionan (ej. Categorías especiales de datos personales).*
    - ***Contribución: BÁSICA ■.***
- **PROTECCIÓN DE LOS EQUIPOS [mp.eq]**
  - **Protección de dispositivos portátiles [mp.eq.3]**
    - *Con CARLA la documentación viaja protegida independientemente de que el puesto de trabajo sea local, dispositivo móvil o se utilice almacenamiento extraíble. 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 etiquetar mediante mecanismos de cifrado solo aquella documentación considerada como sensible.

- ***Contribución: BÁSICA ■.***

- **PROTECCIÓN DE LAS COMUNICACIONES [mp.com]**
  - **Protección de la confidencialidad [mp.com.2]**
    - *Aunque se esté trabajando de forma remota vía VPN (lo que implica un canal de comunicaciones cifrado) con CARLA adicionalmente es el propio documento el que asimismo está etiquetado mediante mecanismos de cifrado, garantizando doblemente la protección de la confidencialidad en las comunicaciones en el supuesto caso de interceptación de las mismas. CARLA permite que, más allá de un canal cifrado de comunicación como HTTPS, etc., el contenido de la documentación que se intercambia viaje protegido y se almacene y use protegido en destino.*
    - ***Contribución: BÁSICA ■.***
  - **Protección de la integridad y de la autenticidad [mp.com.3]**
    - *CARLA incluye en los documentos protegidos datos firmados electrónicamente que, caso de que se intentará 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.*
    - ***Contribución: BÁSICA ■.***
- **PROTECCIÓN DE LOS SOPORTES DE INFORMACIÓN [mp.si]**
  - **Marcado de soportes [mp.si.1]**
    - *CARLA permite proteger la información, etiquetando la información 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.*
    - ***Contribución: MEDIA-ALTA ■.***
  - **Criptografía [mp.si.2]**
    - *Más allá de cifrar el dispositivo extraíble, USB, etc., CARLA protege los ficheros independientemente de dónde se encuentren. Esto permite que si la*

documentación viaja en un pendrive o memoria USB esté etiquetada y protegida.

- *Contribución: MEDIA-ALTA* ■.

- **Custodia [mp.si.3]**
  - *CARLA garantiza el control de acceso con medidas lógicas a la documentación bajo responsabilidad de la organización, independientemente de dónde se encuentre. No aplica a equipos o dispositivos, aunque sí a activos de información de la organización, protegiéndolos con medidas lógicas de seguridad.*
  - ***Contribución: BÁSICA*** ■.
- **Transporte [mp.si.4]**
  - *En el caso de transporte de información en soportes es posible etiquetar mediante mecanismos de cifrado el contenido de la documentación con CARLA, de forma que se garantice la confidencialidad en el transporte, independientemente del método de envío empleado y de la naturaleza del soporte*
  - ***Contribución: BÁSICA*** ■.
- **Borrado y destrucción [mp.si.5]**
  - *CARLA permite 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.*
  - ***Contribución: MEDIA-ALTA*** ■.

- **PROTECCIÓN DE LA INFORMACIÓN [mp.info]**
  - **Datos personales [mp.info.1]**
    - *Con CARLA 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.*
    - ***Contribución: BÁSICA*** ■.
  - **Calificación de la información [mp.info.2]**
    - *Con CARLA 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.

- ***Contribución: MEDIA-ALTA ■.***

- **PROTECCIÓN DE LOS SERVICIOS [mp.s]**
  - **Protección del correo electrónico [mp.s.1]**
    - *CARLA 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.*
    - ***Contribución: BÁSICA ■.***

4 CONCLUSIONES

El ENS persigue incrementar el nivel de seguridad para que las organizaciones del sector público, y del sector privado pertenecientes a su cadena de suministro en el ámbito del ENS, presten sus servicios de forma adecuada, custodiando y asegurando la información tratada y su transmisión, impidiendo que llegue a personas no autorizadas.

En la actualización de 2022 del ENS se ha puesto el foco en alinearlo con el marco normativo y contexto estratégico actual, ajustando los requisitos para adaptarlos a la realidad de diferentes colectivos y sectores de actividad a través de un "*perfil de cumplimiento específico*", dando así una mejor adaptación y respuesta a las tendencias de ciberseguridad actuales.

Las medidas de protección incluidas en el ENS son suficientemente extensas como para pretender que una o unas pocas herramientas ayuden a abordarlas en su totalidad. Sin embargo, sí pueden ayudar a cubrir medidas importantes facilitando a las organizaciones llegar a la plena adecuación al ENS, ya sea de forma estándar, o mediante un perfil de cumplimiento específico al que por sus circunstancias se puedan adscribir.

El enfoque de una herramienta de seguridad centrada en los datos como CARLA permite que la información corporativa viaje protegida y bajo control en todo momento y pueda tenerse una trazabilidad completa de acciones sobre la misma. La protección se extiende más allá del perímetro de la red y permite aplicar controles efectivos sobre información calificada, siguiendo el principio de "mínimo privilegio".

Como se ha visto en los apartados anteriores, CARLA ayuda a facilitar la implantación y consecuente cumplimiento de determinadas medidas de seguridad del Anexo II del RD 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.