Casos de acceso a tratamiento de información sensible

Abstract: el presente documento recoge diferentes casuísticas de partida donde las organizaciones presentan necesidades en el acceso, transmisión y tratamiento para el manejo de información sensible, dado un Sistema sobre el que pretende obtener una declaración de conformidad del Centro Criptológico Nacional (CCN).

Contenido:

1. INTRODUCCIÓN

El presente documento recoge diferentes casuísticas de partida donde las organizaciones presentan necesidades en el acceso, transmisión y tratamiento para el manejo de información sensible, dado un Sistema sobre el que pretende obtener una declaración de conformidad del Centro Criptológico Nacional (CCN).

Los casos surgen de los diferentes planteamientos que se han identificado en diversas entidades con relación a la necesidad de garantizar la seguridad de la información y poder obtener una conformidad de dichos sistemas.

Las diferentes casuísticas a evaluar se basan en múltiples circunstancias en relación con los usuarios (internos y/o externos), la madurez de los procedimientos operativos de seguridad o la necesidad de que la información (sensible o no) deba salir o no del Sistema:

- La confiabilidad en los usuarios internos.
- La confiabilidad en los proveedores.
- La necesidad de tener un control de la información según una escala: control máximo (confinamiento), control normal o control bajo.
- La madurez en el manejo de información sensible e implantación de procedimientos operativos de seguridad por parte de usuarios internos y/o proveedores.
- Necesidad de conectividad con Internet de forma concurrente y acceso a un Sistema con información sensible.
- Existencia de sistemas acreditados para el manejo de un determinado grado de información, donde se establecen interconexiones entre sistemas para el almacenamiento o tratamiento de información sensible.

Una vez las organizaciones hayan analizado su situación particular y quieran solicitar la declaración de conformidad respectiva, deberán de presentar un modelo de validación al Centro Criptológico Nacional donde se recojan las medidas técnicas, la medidas compensatorias y complementarias de vigilancia y los compromisos a implementar en base a las particularidades en el acceso, flujos, tratamiento y trazabilidad para el manejo y protección de información sensible.

2. CASUÍSTICAS

Con lo anteriormente expuesto, se plantean diferentes casuísticas en las entidades que manejan información sensible, así como las recomendaciones que garanticen la seguridad de la protección de la información, atendiendo a diferentes necesidades.

2.1 CASO 1. Necesidad de confinamiento de la información

2.1.1 Condiciones

En esta casuística se establecen las siguientes consideraciones:

- Existe una necesidad manifiesta de control exhaustiva de la información sensible (orientación al confinamiento de la información) en un Sistema.
- Se manifiesta una baja confianza en la puesta en marcha de operaciones seguras por parte de los usuarios internos.
- Se manifiesta una baja confianza en la puesta en marcha de operaciones seguras por parte de los usuarios externos.
- No existe, no hay madurez o no hay confianza en el uso de procedimientos operativos de seguridad por parte de usuarios internos o proveedores.
- La información (sensible o no), no tiene necesidad de salir del Sistema.

- Los usuarios, en el acceso al Sistema no deberían tener conexión con Internet concurrente o no hay necesidad del empleo de servicios públicos por parte de los usuarios o proveedores.

2.1.2 Opciones recomendables

- OPCIÓN A.
  - Uso de tecnología VPN (Virtual Private Network) y vigilancia mas sistema IRM (Information Rights Management) con procedimientos de seguridad mejorados (POS y trazabilidad). También en lugar de IRM se podría emplear/complementar tecnología DLP (Data Loss Prevention).
  - Máximas a lograr: información cifrada en tránsito, vigilancia del cliente y limitación o control de flujo de la información.
- OPCIÓN B.
  - Uso de tecnología VDI (Virtual Desktop Infrastructure) y vigilancia.
  - Máximas a lograr: acceso basado en el envío de pantallas por canales seguros, la información es tratada en un entorno controlado sin posibilidad de sacar la información fuera del sistema. Los clientes que acceden deben cumplir una serie de medidas de seguridad.

2.2 CASO 2: Necesidad de controlar la información

2.2.1 Condiciones

En esta casuística se establecen las siguientes necesidades:

- Existe una necesidad manifiesta de control exhaustivo de la información sensible (con una orientación al confinamiento de la información en un sistema).
- Se manifiesta una baja confianza en la puesta en marcha de operaciones seguras por parte de los usuarios internos.
- Se manifiesta una baja confianza en la puesta en marcha de operaciones seguras por parte de los usuarios externos.
- Puede existir la necesidad de concurrencia de conectividad a redes públicas.
- Se necesita evitar que la información circule de forma no controlada, pero existe la necesidad de tránsito de la información (sensible o no) fuera del Sistema.

2.2.2 Opciones recomendables

- *OPCIÓN A.*
  - Uso de tecnología VPN y vigilancia más sistema DLP/IRM
  - Máximas a lograr: información cifrada en tránsito, vigilancia del cliente y limitación o control de flujo de la información.

- *OPCIÓN B.* Los usuarios tienen necesidad de realizar conexión con Internet y al Sistema para el manejo de información sensible de forma concurrente.
    - Uso de tecnología VPN y vigilancia más máquina virtual (MV) para el acceso a Internet y tecnología IRM.
    - Máximas a lograr: información cifrada en tránsito, vigilancia del cliente y limitación o control de flujo de la información, elemento diferenciado para el acceso a internet.
- *OPCIÓN C.*
    - Uso de tecnología VDI y vigilancia con procedimientos de seguridad mejorados (POS y trazabilidad).
    - Máximas a lograr: acceso basado en el envío de pantallas por canales seguros, la información tratada se realiza en un entorno controlado con información controlada fuera del Sistema, los clientes que acceden deben cumplir una serie de medidas de seguridad.

2.3 CASO 3. No hay una necesidad de confinar la información o hay confiabilidad en los usuarios

2.3.1 Condiciones

En esta casuística se establecen las siguientes necesidades:

- Hay confianza en los usuarios internos y/o los proveedores.
- Sistemas asegurados con altas medidas de seguridad y vigilancia.
- Hay desplegados Procedimientos Operativos de Seguridad (POS) con un alto nivel de madurez.

2.3.2 Opciones recomendables

- *Opción A.*
    - Uso de tecnología VPN y vigilancia.
    - Información cifrada en tránsito y vigilancia del cliente. Los usuarios trabajan con Procedimientos Operativos Seguros que garantizan el control de la información.

2.4 CASO 4. Sistemas interconectados

2.4.1 Condiciones

En esta casuística se establecen las siguientes necesidades:

- Los usuarios acceden desde un Sistema que ha obtenido una conformidad para el manejo de información con la misma criticidad y en las mismas condiciones de

manejo del Sistema. También cuando dicha conectividad se da con un sistema que está en proceso de conformidad.

2.4.2 Opciones recomendables

- *Opción A.*
  - Uso de tecnología VPN para la interconexión.
  - Los sistemas trabajan en un mismo modo de operación segura y la información es cifrada en tránsito.

3. TABLA RESUMEN

Leyenda:

- (R) Recomendable. Son las opciones más recomendables dada la casuística existente.
- (P) Posible. Las opciones son válidas, pero o bien son excesivas en cuanto a su implementación o bien conllevan un alto coste de mantenimiento.
- (NR) No recomendada. Las opciones son insuficientes para garantizar el cumplimiento de las necesidades existentes dadas las casuísticas.

OPCIONES Condiciones principales	CASO 1 Baja confiabilidad Necesidad de Confinamiento	CASO 2 Baja confiabilidad. Necesidad de flujo de información fuera del Sistema controlado	CASO 3 Confiabilidad, seguridad mejorada y procedimientos consolidados.	CASO 4 Interconexión de sistemas con conformidad y flujo de tráfico con confidencialidad e integridad
VDI Y VIGILANCIA + MEJORA EN SEGURIDAD(1)	(P)	(R)	(P)	(P)
VDI Y VIGILANCIA	(R)	(NR)	(P)	(P)
VPN Y VIGILANCIA + IRM CON MEJORA DE SEGURIDAD(2)	(R)	(R)	(P)	(P)
VPN Y VIGILANCIA + MV + IRM(3)	(NR)	(R)	(P)	(P)
VPN Y VIGILANCIA + IRM	(NR)	(R)	(P)	(P)
VPN Y VIGILANCIA	(NR)	(NR)	(R)	(R)
VPN	(NR)	(NR)	(NR)	(R)

(1) Requiere mecanismos que puedan controlar determinados flujos de información, tal como Procedimientos Operativos de Seguridad adecuados y trazabilidad, que permitan determinar que, en el flujo de información, el equipo destino ofrece las debidas garantías para tratar la información en función de su sensibilidad.

(2) Requiere mecanismos que puedan controlar determinados flujos de información, tal como Procedimientos Operativos de Seguridad adecuados y trazabilidad. Se podrá también implementar tecnología tipo DLP.

(3) Admite, por el uso de una MV, la concurrencia de conexión hacia red pública como Internet. Pueden existir otras alternativas para el aislamiento de la capa de usuario.

4. CONSIDERACIONES: VENTAJAS E INCOVENIENTES DE LAS TECNOLOGÍAS INVOLUCRADAS

TECNOLOGÍA	VENTAJAS	INCONVENIENTES
VPN	- Altamente implantado. - Fácil de mantener. - Información en tránsito cifrada por diferentes mecanismos. - Fácil de desplegar. - Tecnología con bajo coste en su despliegue.	- Por sí mismo no garantiza el control de la información. - No hay aislamiento entre la capa de sesión de usuarios.
VDI	- Fácil de mantener. - Aislamiento de la capa de sesión de usuarios. - La información queda confinada. - Muchas organizaciones ya cuentan esta tecnología. - Permite que un usuario pueda manejar información sensible de diferente índole, de forma aislada y desde un solo puesto de trabajo. - El tránsito de la información se realiza de forma cifrada mediante algoritmos propietarios y con otros canales de comunicación limitada.	- Requiere un mecanismo de control adicional si se necesita que la información salga del Sistema. - Tecnología con alto coste en su despliegue.
VIGILANCIA	- Un mecanismo pasivo. - Monitorizar el tráfico entre el dispositivo remoto y el Sistema. - Permite registrar los metadata para realizar forense / *threat hunting* y trazabilidad. - Monitorizar el tráfico entre un VDI y el Sistema. - Cualquier *metadata* puede servir para aplicar políticas de respuesta para aislar del dispositivo para mitigar el riesgo asociado al mismo. - Identificar tendencias en el comportamiento de las conexiones remotas: servicios consumidos, tiempos de las conexiones, tráfico generado, hora de conexión, etc. - Identificar anomalías en el comportamiento. - Equipos virtuales con otras soluciones de hardware dedicado.	- Requiere dedicación / tiempo para identificar tendencias, sacar provecho de los datos. - En redes complejas puede suponer múltiples sensores.

TECNOLOGÍA	VENTAJAS	INCONVENIENTES
POSTURA DEL PUESTO (MEJORA EN LA SERGURIDAD)	- Fácil de desplegar. - Tecnología con bajo coste en su despliegue. - Puede integrarse con el agente VPN. - Permite establecer la postura de seguridad del dispositivo como elemento crítico a la hora de autorizar el dispositivo. - Centraliza información sobre el estado del dispositivo en el CMDB (Configuration Management DataBase) para análisis forense. - Puede complementar otras medidas; requerimiento de tener un agente de DLP instalado, etc.	- Reglas determinísticas, de denegación por incumplimiento de postura, alteran la comunicación y puede generar necesidad de soporte. - Requiere revisión para asegurar que las políticas contemplan los últimos requisitos de la organización (tipos de software, versiones, etc.).
DLP	- Permite un control de la información. independientemente del entorno y el Sistema. - Es independiente de la tecnología.	- Altamente compleja de implementar y mantener. - No está muy implantado. - Tiene opciones limitadas de confidencialidad.
IRM	- Permite un control de la información independiente del entorno y el Sistema, - Tiene altas opciones de confidencialidad.	- Compleja de implementar y mantener. - Dependiente de la tecnología y los productos asociados.
VM	- Aislamiento de la capa de usuario.	- Su uso puede llegar a confundir al usuario. - Requiere doble mantenimiento de sistema operativo del puesto de trabajo - Requiere doble licenciamiento del puesto de trabajo.

5. MODELO DOCUMENTO DE VALIDACIÓN

Las organizaciones deberán aportar un documento de validación que les permita obtener la declaración de conformidad respectiva por parte del Centro Criptológico Nacional para el manejo de Información Sensible en un Sistema.

El documento de validación debe recoger la evaluación y verificación de la correcta interpretación de las medidas técnicas a implementar, como el análisis de los criterios que hayan derivado en el uso de determinadas tecnologías y las soluciones de vigilancia asociadas para el manejo y tratamiento seguro de la información en el Sistema.

Este documento recogerá las diferentes casuísticas (tabla resumen del apartado 3) que habrá identificado la organización para el acceso, flujos, tratamiento y trazabilidad para el manejo y protección de información sensible, teniendo en consideración como mínimo los siguientes aspectos:

- Descripción del flujo de consumo en el tránsito de la información existente.
- Identificación de los tipos de usuarios que accederán desde puestos de trabajo cliente.

- Tipo de medidas de seguridad interna implementadas.
- Niveles de madurez en procedimientos operacionales de seguridad internos.
- Niveles de confianza en la seguridad que pueden plantear los proveedores.
- Tipo de flujos y casos de uso con interacción hacia redes públicas.
- Tabla resumen de compromisos en la implementación de medidas técnicas, medidas compensatorias y complementarias de vigilancia asociadas a la casuística que haya sido identificada.

Con la información aportada, el Centro Criptológico Nacional evaluará tanto el estado de seguridad actual, como el plan de medidas de mejora continua y determinará, sí procede, las recomendaciones y viabilidad para la obtención de la declaración de conformidad respectiva.

6. GLOSARIO

- **Confinamiento**. Proceso por el cual la información sensible se almacena y trata en un entorno controlado, sin posibilidad de salida fuera de un Sistema, o si esto se produce, se debe garantizar que existen controles que limitan su tratamiento o visualización fuera de un contexto de seguridad requerido.
- **Confiabilidad**. Medida que permite determinar la confianza que tiene una organización en que usuarios internos o externos hagan un correcto uso de la información sensible. También sirve como mecanismo para determinar la existencia de confianza cuando los sistemas de la información, especialmente puestos de trabajo, operan de forma segura.

  Por el contrario, cuando no existe confianza, es debido a la existencia de riesgos que podrían provocar que una amenaza se materializara al no disponer de las medidas de protección adecuadas.
- **Control de la información**. Mecanismos que permiten a una organización controlar el intercambio de información sensible que se consume en un Sistema. Se presenta configurado con la debida conformidad que sea requerida, aplica medidas de seguridad que garantizan el acceso exclusivo de personal autorizado, su tratamiento con las condiciones de seguridad adecuadas y muestra un proceso de almacenamiento que garantiza la confidencialidad de la información.

  También se establece como control de la información, la permisividad de salida de datos no sensibles fuera del Sistema.
- **Madurez**. Proceso que determina en qué medida están implementados y pueden ser evaluados las características técnicas, los procedimientos o los procesos de seguridad del Sistema. La madurez en todos sus niveles (técnico, operacional y procedimental) implica una mayor solidez para el manejo y la protección de la información sensible.
- **Concurrencia de conexión a Internet**. Estado en el cual un equipo operado por un usuario debe estar conectado concurrentemente con un sistema para el

almacenamiento o manejo de información sensible y con una red pública como Internet.

La ausencia de control en la concurrencia podría suponer un riesgo de seguridad añadido, puesto que la interconexión directa que se produce a través de dicho equipo supone una relación entre red pública y el sistema protegido.

- **Vigilancia**. Consiste en la evaluación permanente del estado de la seguridad de los sistemas de las Tecnologías de la Información y la Comunicación. Para ello, es preciso tratar tanto las deficiencias de seguridad técnicas, como las de tipo procedimental, de tipo legislativo/normativo o incluso de tipo humano.
- **Envío de pantallas**. Proceso empleado fundamentalmente por tecnologías de escritorios virtuales o aplicaciones virtualizadas, por el cual, la información para el tratamiento de la información no se realiza nunca sobre el equipo físico, sino en otro sistema.

  Las operaciones que tengan lugar son transferidas al usuario mediante el envío de imágenes, de tal forma que la información tratada nunca es transferida, y, por lo tanto, tampoco se almacena en el equipo físico.
- **Tránsito o flujo de información**. Proceso por el cual una información existente en un sistema es consumida por diferentes partes y por tanto debe salir del Sistema.
- **Equipo asegurado**. Activo tecnológico al cual se le han implementado medidas de protección para el manejo de información sensible basadas en el bastionado de seguridad bajo normativa CCN-STIC.
- **Procedimientos operativos de seguridad**. Procedimientos, que en su mayoría serán manuales, donde se garantice que las acciones de índole técnicas, de gestión, de mantenimiento, de tratamiento o de almacenamiento de la información, se llevan a cabo mediante métodos validados, medibles, repetibles y perdurables en el tiempo.