Orientaciones para el manejo de información clasificada (DIFUSIÓN LIMITADA o equivalente) en entornos ajenos a la organización (teletrabajo)

Abstract: el presente documento describe un marco de referencia para el uso de sistemas para el manejo de información clasificada en entornos ajenos a la organización (teletrabajo), que permitan mantener el nivel de protección requerido, no sustituyendo en ningún caso a lo establecido en la normativa de referencia.

Contenido:

1. INTRODUCCIÓN 1
2. OBJETO 1
3. ALCANCE 2
4. NECESIDAD DE CONOCER 2
5. FORMACIÓN 2
6. MEDIDAS DE PROTECCIÓN 2
7. NORMATIVA DE REFERENCIA 4

1. INTRODUCCIÓN

La acreditación de todo sistema destinado al manejo de Información Clasificada (IC) tiene como finalidad verificar la adecuada protección de la IC cuando es manejada en Sistemas de Tecnologías de la Información y la Comunicación (TIC).

Esta verificación se realizará de acuerdo a los criterios de seguridad (de los sistemas TIC en los procedimientos de seguridad física, del personal y documental) establecidos en la normativa aplicable en cada caso. En el ámbito de competencia de la Autoridad Nacional para la protección de la IC son sus propias normas.

Esta normativa se complementa y desarrolla, en el aspecto técnico, con el conjunto de guías CCN-STIC del Centro Criptológico Nacional (CCN), las cuales establecen los requisitos de seguridad en las Tecnologías de la Información y la Comunicación aplicables a todo sistema que deba manejar IC.

2. OBJETO

Describir un marco de referencia para el uso de sistemas para el manejo IC de grado DIFUSIÓN LIMITADA o equivalente (DL o equivalente) en entornos ajenos a la organización (teletrabajo), que permitan mantener el nivel de protección requerido, no sustituyendo en ningún caso a lo establecido en la normativa de referencia.

3. ALCANCE

Estas orientaciones son de aplicación para todos los sistemas que manejen o vayan a manejar IC de grado DL o equivalente en entornos ajenos a la organización (teletrabajo) cuya protección sea responsabilidad de la Autoridad Nacional.

4. NECESIDAD DE CONOCER

El principio de "Necesidad de Conocer" tiene que ser percibido en un grado significativo y asegurado respectivamente a través de medidas organizativas y técnicas.

5. FORMACIÓN

El Jefe del Servicio de Protección de la Organización deberá establecer los requisitos de seguridad que deben ser entendidos y aceptados de manera formal por el personal que va a manejar la IC. Los requisitos deben estar documentados en la Documentación de Seguridad del Sistema.

Se capacitará de manera periódica a todo el personal que vaya a manejar IC en entornos ajenos a la organización (teletrabajo), insistiendo especialmente en:

- Normativa de seguridad del Sistema.
- Procedimientos de uso seguro de la tecnología/dispositivos.
- Detección y reacción ante incidentes de seguridad o comprometimiento de la IC.
- Manejo y custodia de la IC.

El personal que vaya a utilizar el sistema para el manejo IC de grado DIFUSIÓN LIMITADA o equivalente (DL o equivalente) en entornos ajenos a la organización (teletrabajo) deberá leer y firmar los Procedimientos Operativos de Seguridad (POS) específicos y particulares del sistema antes de utilizar el mismo.

6. MEDIDAS DE PROTECCIÓN

- La información clasificada de grado DIFUSIÓN LIMITADA o equivalente que se maneje en entornos ajenos a la organización (teletrabajo) se llevará a cabo a través de equipos corporativos que cuenten con las medidas de seguridad indicadas para un equipo acreditado e incluyendo adicionalmente, medidas complementarias de vigilancia.
- Se deberán definir adecuadamente las medidas compensatorias de seguridad y complementarias de vigilancia con el objetivo de reducir al mínimo el riesgo de pérdida o comprometimiento de la IC cuando el sistema es utilizado fuera de las Zonas de Seguridad de la organización (POS particulares).

- Fuera de una Zona de Acceso Restringido (ZAR) o de una Zona Administrativa de Protección (ZAP) consideradas Zonas de Seguridad de la organización, el personal debe cumplir todas las medidas compensatorias de seguridad y complementarias de vigilancia definidas en la Documentación de Seguridad del Sistema.
- Tanto el hardware como el software utilizado se protegerá por la organización propietaria del sistema que maneja IC para evitar posibles manipulaciones o exfiltración de información (adecuado control de acceso lógico, utilización de etiquetas de seguridad, etc.).
- Los sistemas no pueden ser utilizados en lugares públicos siempre que no se puedan aplicar medidas compensatorias de seguridad y complementarias de vigilancia acordes a este tipo de escenarios.
- Como norma general los dispositivos portátiles (ordenadores, dispositivos de almacenamiento, etc.) deberán estar protegidos por mecanismos de cifrado aprobados por el CCN. En este caso, los dispositivos portátiles podrán quedar desatendidos (por ejemplo, en la habitación de un hotel) debiéndose aplicar las medidas de seguridad habituales para proteger un artículo de valor.
- Los dispositivos y las líneas de comunicaciones utilizadas para la transmisión de la IC de grado DL o equivalente en entornos ajenos a la organización (teletrabajo) es recomendable que sean propios de la organización. En caso contrario, se limitará el ámbito de operación a la información y servicios imprescindibles.

  Se protegerán los canales de comunicación con productos o herramientas de cifra aprobados que protejan la confidencialidad y la integridad del canal, y provean autenticación extremo a extremo. También es importante que no se implementen soluciones tipo *split-tunneling*, en las cuales el dispositivo pueda conectarse simultáneamente a redes corporativas (confiables) y domésticas (no confiables).

  Desde el Centro Criptológico Nacional se pone a disposición de los Organismos un Catálogo de Productos y Servicios de seguridad TIC (CPSTIC, guía CCN-STIC-105) que contiene un listado de productos y servicios cuyas funcionalidades de seguridad han sido certificadas y se han aprobado para su uso en este tipo de escenarios.
- Los sistemas que manejen IC de grado DL o equivalente deben ser utilizados únicamente para fines corporativos.
- La autenticación del usuario en este tipo de escenarios, en la medida de lo posible, debe realizarse a través de autenticación de doble factor.
- El control de acceso a los recursos corporativos se realizará a través de la asignación de diferentes grados de confianza en función de la configuración de seguridad establecida en el equipo (un nivel alto de bastionado podrá

proporcionar un alto nivel de acceso a dichos recursos). Se podrá restringir el acceso a recursos desde un equipo si éste no cumple con los parámetros definidos (control en tiempo real).

- No pueden ser utilizados dispositivos que utilicen tecnología inalámbrica o infrarrojos (por ejemplo, teclados, dispositivos Bluetooth, etc.).
- Los servicios del Sistema serán segregados de tal forma que solo se expongan aquellos considerados estrictamente necesarios (segmentación).
- Se llevará a cabo por parte de la organización una gestión continua de la seguridad a través de la vigilancia permanente de la configuración de seguridad de los equipos corporativos utilizados para este fin.

El mantenimiento y actualización de los dispositivos portátiles deberá ser realizado por la organización de manera periódica según se indique en sus procedimientos operativos de seguridad.

7. NORMATIVA DE REFERENCIA

- Normas de la Autoridad Nacional para la Protección de la Información Clasificada (http://www.cni.es/ons).
- Guías CCN-STIC del Centro Criptológico Nacional (https://www.ccn-cert.cni.es).
- COUNCIL DECISION 2013/488 on the security rules for protecting EU classified information.
- AGREEMENT between the Member States of the European Union, meeting within the Council, regarding the protection of classified information exchanged in the interests of the European Union 2011/C/202
- NATO Security Policy.

centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2020.12.31 01:05:23 +01'00'