



WISCONSIN SISTEMA TIME

Materiales de capacitación

Departamento de Justicia del Estado de Wisconsin – Oficina del Fiscal General

GUÍA INFORMATIVA DE CONCIENTIZACIÓN SOBRE LA SEGURIDAD DEL SISTEMA TIME

SEGURIDAD DEL SISTEMA

Los sistemas TIME/NCIC (Información de Transacciones para la Gestión del Cumplimiento de la Ley/Centro Nacional de Información Criminal) son redes informáticas de justicia penal que brindan acceso a información sensible y, en ocasiones, confidencial, como registros de licencias de conducir, antecedentes penales, registros de personas buscadas, entre otros. Esta información debe estar protegida de personas que tratan de obtener acceso no autorizado al sistema y de quienes utilicen la información obtenida del sistema para fines no autorizados.

Diversas agencias han acordado poner su información a disposición de las fuerzas del orden y de la justicia penal a través de los sistemas TIME y NCIC con el propósito específico de facilitar la administración de la justicia penal. Cualquier uso indebido de esta información o el incumplimiento de los acuerdos y políticas del sistema pone en peligro la disponibilidad de la información para todas las agencias participantes.

La Política de Seguridad de CJIS del FBI establece los requisitos *mínimos* de seguridad de la información para proteger las fuentes de información, así como la transmisión, el almacenamiento y la creación de información de justicia penal. El sistema TIME ha adoptado la Política de Seguridad de CJIS como la Política de Seguridad del sistema TIME.

Personal autorizado

La información de los sistemas TIME/NCIC solo debe ser utilizada por personal *autorizado* de las fuerzas del orden y de la justicia penal para fines propios de la justicia penal y el cumplimiento de la ley, tal como se describe en la sección PS-3 de la Política de Seguridad de CJIS (CJIS Security Policy Section PS-3 Personnel Screening). El personal autorizado se refiere a quienes han sido sometidos a la verificación de antecedentes obligatoria basada en huellas dactilares, quienes han completado la capacitación en concientización sobre seguridad y figuran en la lista de personal autorizado de la agencia.

Uso del sistema

La información de los sistemas TIME/NCIC **solo** debe ser utilizada por personal autorizado de las fuerzas del orden y de la justicia penal para fines propios de la aplicación de la ley y la justicia penal. Se deben cumplir ambas condiciones. Por ejemplo, un profesional de la justicia penal no puede obtener información sobre placas o registro de vehículos por motivos personales.

Cada agencia de justicia penal autorizada para acceder a los sistemas TIME/NCIC debe contar con una política por escrito para la sanción disciplinaria de quienes infrinjan la política. El uso indebido del sistema TIME o de la información obtenida de él puede constituir una infracción de las leyes estatales o federales, y las infracciones pueden someter a las personas y a las agencias a procesos penales y/u otras sanciones. La solicitud, recepción o divulgación no autorizada de información de los sistemas TIME/NCIC puede dar lugar y *ha* dado lugar a procesos penales o civiles.

Manejo adecuado de la información de justicia penal

La información obtenida a través de los sistemas TIEMPE/NCIC, ya sea en formato físico o digital, debe almacenarse en un área segura accesible únicamente para el personal autorizado. La información de justicia penal obtenida de los sistemas TIME/NCIC debe permanecer en el área segura, a menos que existan autorizaciones y procedimientos específicos para eliminar la información del área segura. Las agencias deben controlar físicamente y almacenar de forma segura los medios digitales y no digitales dentro de las instalaciones físicamente seguras o áreas controladas y cifrar información de justicia penal (CJI, por sus siglas en inglés) en medios digitales cuando las restricciones físicas y de personal no sean viables. Las agencias deben proteger los soportes del sistema hasta que el medio sea destruido o desinfectado.

Cuando la información de TIME/NCIC (en papel o digital) se transporte fuera de las áreas seguras, deberá continuar protegida. Por lo tanto, el traslado de la información TIME/NCIC está restringido únicamente al personal autorizado. Las agencias deben proteger y controlar los medios digitales y no digitales para evitar la vulneración de los datos durante su traslado fuera de las instalaciones físicamente seguras o de las áreas controladas. Los medios digitales se protegerán mediante el uso de cifrado. Los medios físicos deben protegerse con el mismo nivel con el que se protegería la información en formato electrónico. Las agencias deben mantener la responsabilidad de los medios del sistema durante su traslado fuera de las instalaciones físicamente seguras o áreas controladas, así como documentar las actividades asociadas con el transporte de medios del sistema y restringir estas actividades al personal autorizado.

Los medios físicos se eliminarán de forma segura cuando ya no sean necesarios para fines de investigación o de seguridad, lo que ocurra más tarde. Los medios físicos se destruirán mediante trituración cruzada o incineración y las agencias deben emplear mecanismos de eliminación de datos con la eficacia e integridad proporcionales a la categoría de seguridad o clasificación de la información. Los medios digitales que almacenen información de TIME/NCIC (discos duros, memorias USB, CD, etc.) deben borrarse o desmagnetizarse utilizando un software de eliminación de datos aprobado que garantice una limpieza de al menos 3 pasadas. Los medios digitales inoperables deben ser destruidos (cortados, aplastados, triturados, etc.). La eliminación, desintegración y destrucción de la información de TIME/NCIC debe ser presenciada o efectuada por personal autorizado para evitar la posibilidad de una divulgación inadvertida de la información del sistema a personas no autorizadas.

Las agencias deben restringir el uso de medios digitales y no digitales en los sistemas de propiedad de la agencia que hayan sido aprobados para su uso en el almacenamiento, procesamiento o transmisión de información de justicia penal mediante el uso de controles técnicos, físicos o administrativos. Las agencias deben prohibir el uso de dispositivos de medios digitales de propiedad personal en todos los sistemas de propiedad o controlados por la agencia que almacenen, procesen o transmitan CJI. Las agencias deben prohibir el uso de dispositivos de medios digitales en todos los sistemas de propiedad o controlados por la agencia que almacenen, procesen o transmitan CJI cuando dichos dispositivos no tengan un propietario identificable.

Las agencias deben contar con políticas y procedimientos relacionados con la protección de medios de almacenamiento, incluida una política de medios de almacenamiento a nivel

de la agencia que aborde el propósito, el alcance, las funciones, las responsabilidades, el compromiso de la gerencia y la coordinación entre las entidades de la agencia y el cumplimiento, y que sea consistente con las leyes y regulaciones aplicables. Todo el personal de la agencia debe estar al tanto de las políticas y procedimientos de protección de los medios de almacenamiento. Las agencias deben revisar y actualizar estas políticas y procedimientos al menos una vez al año y tras cualquier incidente de seguridad que involucre medios digitales o no digitales. Las agencias deben designar a una persona con responsabilidades de seguridad para gestionar el desarrollo, la documentación y la difusión de la política de protección de los medios de almacenamiento.

Acceso

Las agencias deben controlar todos los accesos al área segura y verificar que la persona califique para acceder antes de autorizar su ingreso. Recuerde que el personal autorizado es aquel que se ha sometido a la verificación de antecedentes basada en huellas dactilares, ha completado la capacitación en la concientización sobre seguridad y figura en la lista de personal autorizado de la agencia. Si una persona no ha cumplido con estos requisitos, solo podrá acceder al área segura si está escoltada por alguien que sí está autorizado.

Antes de conceder a un visitante acceso escoltado al área segura, debe verificar la identidad del visitante. Los visitantes deben ser acompañados en todo momento y la actividad del visitante debe ser monitoreada.

El personal debe estar atento a su entorno y tomar medidas para garantizar que las personas no autorizadas no accedan a la información de justicia penal ni a los sistemas TIME/NCIC. Esto puede incluir interrogar o cuestionar a personas no escoltadas, verificar las credenciales de desconocidos y/o asegurarse de que los visitantes y otros usuarios no autorizados no están observando por encima del hombro de alguien para obtener información.

El personal de la agencia debe asegurarse de que todas las personas cumplan con los procedimientos de entrada y salida, el control de visitantes, los procedimientos de manipulación y los puntos de control de acceso. El personal debe reportar infracciones o sospechas de infracciones, incluidas las áreas que puedan no ser seguras.

Los usuarios del sistema deben estar atentos a las personas que intenten obtener acceso a información confidencial mediante “ingeniería social”. La ingeniería social consiste en manipular a las personas para que hagan algo o divulguen información confidencial. Esto puede incluir correos electrónicos de fuentes desconocidas, archivos adjuntos de correos electrónicos que contengan programas espía, personas que llamen por teléfono haciéndose pasar por representantes de otra agencia autorizada, etc. En caso de duda, los usuarios del sistema deben verificar la fuente o la identidad detrás del correo electrónico, llamada telefónica, etc., antes de hacer un posible uso indebido de los recursos del sistema o proporcionar información de justicia penal a personas no autorizadas.

Respuesta a incidentes

Un incidente de seguridad es una infracción o posible infracción de la política que pone en riesgo la confidencialidad, la integridad o la disponibilidad de la información de TIME/NCIC.

El personal debe saber cómo reportar un incidente de seguridad, a quién reportarlo, cuándo contactar a esa persona y qué acciones básicas tomar en caso de sospechar una vulneración de los sistemas TIME/NCIC o de la información de justicia penal obtenida de ellos.

Concientización sobre seguridad del sistema TIME Declaración de certificación

Certifico que he leído y comprendo el contenido de la guía de acceso físico y concientización sobre seguridad del sistema TIME y acepto cumplir con todos los requisitos de los sistemas de TIME/CJIS respecto al acceso, uso, almacenamiento y eliminación adecuados de la información del sistema TIME/CJIS.

Comprendo que la información de justicia penal puesta a disposición a través de los sistemas TIME/CJIS es de carácter confidencial y podría causar un gran daño si se utiliza de forma indebida; por lo tanto, el acceso a esta información está limitado al personal autorizado. Entiendo que el uso indebido de los sistemas TIME/CJIS o de la información recibida de estos sistemas puede someterme a sanciones o penalizaciones del sistema y también puede constituir una violación de las leyes estatales o federales, lo que me expondría a sanciones penales y/u otras sanciones. El uso indebido de los sistemas TIME/CJIS incluye acceder a los sistemas sin autorización o exceder mi nivel de acceso autorizado, acceder a los sistemas para un propósito no adecuado, usar o difundir información recibida de los sistemas para fines no relacionados con el trabajo o no vinculados con la justicia penal, entre otros.

Su firma: _____

Escriba su nombre con letra legible: _____

Nombre de la agencia: _____

Fecha: _____