

CENTRO DE RECAUDACIÓN DE INGRESOS MUNICIPALES

NÚMERO: 9620

Fecha: 21 de noviembre de 2024

Aprobado: Omar J. Marrero

Secretario de Estado



Departamento de Estado

Gobierno de Puerto Rico

REGLAMENTO DE SEGURIDAD ELECTRÓNICA PARA ADMINISTRACIÓN DEL SISTEMA DE CÁMARAS DE SEGURIDAD Y CONTROL DE ACCESO A FACILIDADES



TABLA DE CONTENIDO

Artículo I – Disposiciones Preliminares.....	2
Sección 1.1 – Título	2
Sección 1.2 – Base Legal	2
Sección 1.3 – Propósito.....	2
Sección 1.4 – Aplicabilidad	2
Sección 1.5 – Definiciones	3
Artículo II – Control de Accesos / Entrada y Salida de las Instalaciones del CRIM	4
Sección 2.1 – Accesos.....	4
Sección 2.2 – Tarjeta de identificación	5
Sección 2.3 – Supervisión y Mantenimiento Diario del Sistema de Seguridad Electrónica.....	6
Artículo III – Sistema de Seguridad Electrónica	6
Sección 3.2 – Operación de las cámaras de vigilancia	7
Sección 3.3 – Funcionamiento	7
Sección 3.4 – Localización	7
Sección 3.5 – Evidencia ante Tribunales	8
Sección 3.6 – Cadena de evidencia.....	8
Sección 3.7 – Responsabilidad de custodia y protección	8
Artículo IV – Seguridad del Sistema	8
Sección 4.1 – Acceso al Sistema de Seguridad Electrónica	8
Sección 4.2 – Almacenamiento de grabaciones	8
Sección 4.3 – Monitores	8
Artículo V – Producción y Conservación de Grabaciones Digitales	9
Sección 5.1 – Período regular de imágenes.....	9
Sección 5.2 – Protección de eventos específicos en el sistema.....	9
Sección 5.3 – Solicitud de inspección y requisito de Orden o <i>subpoena</i>	9
Artículo VI – Duplicidad de imágenes.....	9
Sección 6.1 – Autorización.....	9
Sección 6.2 – Copias de grabaciones.....	9
Sección 6.3 – Registro de revisión de grabaciones.....	10
Artículo VII – Notificación, Publicidad y Reclamaciones.....	10
Sección 7.1 – Notificación	10
Sección 7.2 – Avisos de advertencia	10
Sección 7.3 – Procedimiento de reclamaciones o quejas	10
Artículo VIII – Disposiciones Finales	11
Sección 8.1 – Clausula de Salvedad	11
Sección 8.2 – Enmiendas.....	11
Sección 8.3 – Vigencia	11

REGLAMENTO DE SEGURIDAD ELECTRÓNICA PARA ADMINISTRACIÓN DEL SISTEMA DE CÁMARAS DE SEGURIDAD Y CONTROL DE ACCESO A FACILIDADES

ARTÍCULO I – DISPOSICIONES PRELIMINARES

Sección 1.1 – Título

Este Reglamento se conocerá como “Reglamento de Seguridad Electrónica para Administración del Sistema de Cámaras de Seguridad y Control de Acceso a Facilidades”.

Sección 1.2 – Base Legal

Este Reglamento se adopta y promulga de acuerdo con las facultades conferidas al CRIM a través de la Ley Núm. 107 del 13 de agosto de 2020, según enmendada, conocido como Código Municipal de Puerto Rico. Así mismo, en conformidad con las disposiciones aplicables—en lo que respecta al proceso de Reglamentación—de la Ley Núm. 38 del 30 de junio de 2017, según enmendada, y conocida como *Ley de Procedimiento Administrativo Uniforme del Gobierno de Puerto Rico*.

Sección 1.3 – Propósito

Las instalaciones del CRIM a través de todo Puerto Rico reciben diariamente visitas de contribuyentes, contratistas y otros visitantes. A esos efectos, resulta esencial proteger la seguridad en las áreas de acceso a las instalaciones del CRIM, tal como: ascensores, pasillos, escaleras y otros espacios. Lo anterior, con el objetivo de asegurar la protección de nuestros empleados, contratistas, usuarios, visitantes e invitados. La implementación de cámaras de vigilancia nos brinda la capacidad de documentar en video el acceso a nuestras instalaciones y así prevenir situaciones de riesgo a la seguridad.

En tal virtud, en primer orden, este Reglamento se establece con la finalidad de definir los parámetros y estándares necesarios para regular el control de acceso a las instalaciones del CRIM de forma civilizada y organizada. En segundo orden, este Reglamento regula el uso del Sistema de Seguridad Electrónica mediante cámaras de vigilancia, así como lo relacionado al funcionamiento, custodia, disposición, almacenamiento, acceso, conservación y uso de las grabaciones de este.

El objetivo primordial del uso de cámaras seguridad es garantizar la seguridad de la vida y la propiedad dentro de las instalaciones físicas del CRIM. Se implementa el Sistema de Seguridad Electrónica en todas las instalaciones del CRIM con los objetivos principales de 1) proteger la seguridad del personal y visitantes; 2) auxiliar y colaborar en la detección y prevención de conductas y actos ilegales; 4) reducir la incidencia de actos ilegales; 5) brindar asistencia en situaciones de emergencia, incendios, explosiones; 6) supervisar y proteger la propiedad del CRIM, incluyendo equipos tecnológicos y 7) proveer supervisión ante cualquier evento accidentales, o de cualquier índole, que puedan poner en riesgo la seguridad de la vida o la propiedad.

Sección 1.4 – Aplicabilidad

Este Reglamento aplica a todo empleado, contratistas, inquilinos, suplidor, visitantes o cualquier otra

persona que ingrese a las instalaciones físicas del CRIM.

Sección 1.5 – Definiciones

Las palabras y frases utilizadas en este reglamento serán interpretadas en concordancia con el contexto en el que se utilicen, siguiendo el significado aceptado en el uso común y corriente. Los siguientes términos usados en este Reglamento tendrán el significado que a continuación se expresa:

1. **CRIM** - Se refiere al Centro de Recaudación de Ingresos Municipales.
2. **Oficina de Servicios Administrativos** – Oficina responsable del control y manejo de la gestión de seguridad electrónica en el CRIM.
3. **Director de Servicios Administrativos** – funcionario gerencial con la responsabilidad de supervisar y garantizar la seguridad en las facilidades del CRIM.
4. **Administrador del Sistema de Seguridad Electrónica** – funcionario designado por el Director Ejecutivo para desempeñar las responsabilidades establecidas en este Reglamento en relación con el sistema de Seguridad Electrónica. Este cargo estará adscrito a la Oficina de Servicios Administrativos, bajo la supervisión de su director.
5. **Apoyo técnico:** Personal técnico de la Oficina de Gerencia de Sistema de Informática (OGSI) que proporcionará apoyo tecnológico, según sea necesario, para evaluar el estado y las condiciones de los equipos electrónicos. Asimismo, cuando sea necesario recomendará la sustitución de estos, junto con los servicios y materiales necesarios para mantener en óptimas condiciones el sistema de seguridad electrónica, sin importar su ubicación.
6. **Empleado** - Persona que trabaja o presta servicios en el CRIM a cambio de salario, incluyendo aspirantes a empleo.
7. **Visitante** - Persona que no es empleado ni contratista del CRIM que visita las instalaciones para realizar cualquier gestión.
8. **Inquilino** - Persona que ha suscrito un contrato de arrendamiento para ocupar un espacio dentro de las instalaciones administradas por el CRIM.
9. **Instalaciones** - Estructura que alberga oficinas, áreas, estacionamientos, centros de servicios y cualquier otra propiedad inmueble del CRIM o administrada por este.
10. **Control de acceso** - Los siguientes componentes son las partes esenciales para el funcionamiento del control de acceso:
 - **Panel Control:** Dispositivo que conecta a otros componentes como lectoras, magnetos, botones de salida etc., así como la programación del proceso de autorización y lleva un registro de eventos a manera de bitácora digital.
 - **Servidor:** Equipo tecnológico donde se almacena los datos y centraliza la información.
 - **Lectores:** Componente automatizado que realizará la lectura de una tarjeta o algún biométrico como rostro, huellas digitales o código de barras o QR y enviará la solicitud al panel de control quien a su vez realizará las validaciones según lo programado.
 - **Magnetos:** Son interruptores que van conectados directamente en el panel de control y son utilizados para detectar el estado de la puerta. De esta manera se puede saber si la puerta está abierta o cerrada, y también es posible crear alarmas en caso de que la puerta quede

abierta mucho tiempo.

- **Dispositivos de salida:** Son dispositivos que van conectados en el panel de control y usados para abrir las puertas o accesos en las salidas.
11. **Tarjeta de Identificación:** Tarjeta electrónica emitida con foto y nombre del empleado para acceso a las facilidades.
 12. **Registro de Control de Acceso** - Registro, en formato digital y/o manual, que contiene los eventos cronológicos relacionados a la entrada y salida con el sistema de acceso, así como las solicitudes de cambios en los horarios de entrada y salida a las instalaciones del CRIM y las solicitudes de tarjetas electrónicas por cualquiera de las siguientes razones: Pérdidas, Daño, Devolución y Redistribución, para Empleados del CRIM, incluyendo al personal de mantenimiento, seguridad, inquilinos, asesores y contratistas.
 13. **Sistema de Seguridad Electrónica:** Mecanismo instalado a través de todas las facilidades para proteger a empleados, visitantes, inquilinos, u otros, así como toda la propiedad pública del CRIM.
 14. **Áreas Comunes:** Lugares transitados por empleados, visitantes, inquilinos, contratistas o cualquier otra persona en las instalaciones del CRIM donde no se espera privacidad, como pasillos, espacios de trabajo abiertos, ascensores, entradas y salidas, entre otros.
 15. **Cámara de seguridad:** Dispositivo electrónico que captura imágenes.
 16. **Monitor** - Equipo electrónico que proporciona datos visuales para observar en tiempo real la actividad capturada por las cámaras de seguridad.
 17. **Incidentes:** Hechos como conducta criminal, emergencias médicas, accidentes, incendios, explosiones que amenazan a personas y propiedad.
 18. **Registro de incidencias del sistema de Seguridad Electrónica:** Este registro, ya sea en formato digital y/o manual, administra de manera cronológica todos los eventos o incidentes relacionados con el sistema de cámaras de seguridad que se produzcan durante un periodo específico.
 19. **Registro de revisión de grabaciones** - documento que registra las actividades relacionadas con la revisión y análisis de las grabaciones. Este documento detalla quién fue la persona que realizó la revisión, fecha, hora y propósito.

ARTÍCULO II – CONTROL DE ACCESOS / ENTRADA Y SALIDA DE LAS INSTALACIONES DEL CRIM

Sección 2.1 – Accesos

Todos los empleados del CRIM tendrán acceso a sus respectivas áreas de trabajo mediante el uso de su tarjeta de identificación. No obstante, el Director de Servicios Administrativos proporcionará instrucciones por escrito al Administrador del Sistema de Seguridad Electrónica para definir el acceso de cada empleado a las distintas áreas de las diferentes Oficinas, considerando los criterios de seguridad y confidencialidad, conforme al horario establecido por la Oficina de Recursos Humanos.

Además, en el caso de nuevos empleados que inicien labores en las instalaciones del CRIM, la Oficina de Recursos Humanos determinará el horario de entrada y salida de acuerdo con sus funciones. Se permitirá la modificación de estos horarios mediante autorización por escrito del director de cada unidad administrativa, dirigida al Director de la Oficina de Servicios Administrativos.

En el caso de suplidores, contratistas, subcontractados e inquilinos, la petición de acceso será evaluada y aprobada por el Director de Servicios Administrativos. Este se asegurará de que el Administrador del Sistema de Seguridad Electrónica registre todos los cambios solicitados en el registro de entrada y salida para mantener un control y un histórico conforme a lo establecido en este Reglamento.

Sección 2.2 – Tarjeta de identificación

Las siguientes normas serán de aplicación para todos los empleados en relación con la tarjeta de identificación:

1. Todo empleado, sin excepción, debe ser responsable portar la tarjeta de identificación en un lugar visible de su vestimenta, con el retrato hacia el frente, durante su tiempo en la Oficina o en gestiones oficiales fuera de ella. Esta obligación se extiende a empleados que asistan a la Oficina fuera de sus horas laborables o durante licencias.
2. La posesión de la tarjeta de identificación está autorizada únicamente para el empleado al que se le ha asignado, quien es responsable de mantenerla en buen estado. Queda estrictamente prohibida la prestación o transferencia de la tarjeta a otro empleado o a un tercero.
3. En caso de pérdida, el empleado debe notificar de inmediato a su supervisor, no más tarde del siguiente día laborable, para que este solicite a la Oficina de Servicios Administrativos la expedición de una nueva tarjeta. El reemplazo conlleva un costo de veinte dólares (\$20.00), que deberá cubrir el empleado. En caso de hurto, se debe presentar una declaración escrita, bajo pena de perjurio, describiendo cómo ocurrió el hurto, eximiendo al empleado del costo de reemplazo. La Oficina de Servicios Administrativos podría, a discreción, requerir que el empleado presente una querrela ante la Policía, dependiendo de las circunstancias del hurto.
4. Cuando un empleado olvide su tarjeta, debe notificar al Director de su Unidad, quien solicitará por escrito a la Oficina de Servicios Administrativos una tarjeta provisional registrada a su nombre. Esta tarjeta debe ser devuelta al finalizar la jornada laboral del empleado.
5. En situaciones en las que la apariencia de un empleado experimente cambios significativos, dificultando o imposibilitando su reconocimiento en comparación con la fotografía de su tarjeta de identificación, o si surge algún problema con su registro en el lector, como daño o cualquier otra dificultad, se requiere que el empleado se comunique de inmediato con su supervisor.

El supervisor deberá presentar una solicitud por escrito a la Oficina de Recursos Humanos para obtener una nueva tarjeta, entregando la tarjeta a la Oficina de Servicios Administrativos. En la Oficina de Servicios Administrativos se llevará un registro detallado de los reemplazos y movimientos de tarjetas por cada empleado, para un control efectivo y se procederá a dar de baja la tarjeta con problemas. El registro debe incluir los siguientes detalles:

- Nombre de la persona bajo quien está registrada la tarjeta
- Fecha de la transacción
- Número de la tarjeta que va a ser sustituida
- Número de la nueva tarjeta
- Localización / Ubicación

- Nombre del puesto
 - Quién solicitó el reemplazo
 - Quién autorizó la solicitud
 - Causa del reemplazo
6. La tarjeta de identificación es propiedad del CRIM y debe ser devuelta a la Oficina de Servicios Administrativos cuando surja terminación de empleo por jubilación, cesantía, despido, terminación del empleo o contrato. También se requerirá la devolución de la tarjeta en casos de aplicación de acciones disciplinarias que conlleven suspensión de empleo o destitución.

Sección 2.3 – Supervisión y Mantenimiento Diario del Sistema de Seguridad Electrónica

El Administrador del Sistema de Seguridad Electrónica tendrá la responsabilidad de monitorear a diario el sistema de control de acceso, así como las cámaras de seguridad. En caso de cualquier problema en alguno de estos sistemas, el Administrador notificará inmediatamente a la Oficina de Gerencia de Sistemas de Informática (OGSI) por correo electrónico, solicitando la asistencia del personal de Apoyo Técnico para identificar y solucionar el inconveniente. El Administrador deberá mantener informado a los directores de la Oficina de Servicios Administrativos y de la OGSI para fines de registro y coordinación de los trabajos. Toda incidencia con el sistema de seguridad electrónica deberá estar documentado en el Registro de Incidencias del Sistema de Seguridad Electrónica.

En caso de identificar problemas o irregularidades en el funcionamiento de las cámaras, se podrá realizar la contratación de una compañía externa especializada en mantenimiento de sistemas de seguridad electrónica a través de un proceso competitivo. Esta compañía realizará el mantenimiento preventivo y correctivo del sistema. El Administrador del Sistema de Seguridad Electrónica será el encargado de coordinar y supervisar el trabajo de la compañía externa contratada. Este deberá llevar un registro de todos los mantenimientos realizados en el sistema, que incluya fecha y hora, personal que realizó el servicio, compañía, descripción del servicios realizado y personal del CRIM que estuvo supervisando el trabajo.

ARTÍCULO III – SISTEMA DE SEGURIDAD ELECTRÓNICA

Sección 3.1 – Sistema de Seguridad Electrónica

Como medida de seguridad y para la protección de los empleados, contratistas, visitantes y de la propiedad pública, el CRIM establece un sistema de seguridad y vigilancia electrónica mediante el uso de cámaras de seguridad sin audio.

Las grabaciones de las cámaras de seguridad se utilizarán con el fin primordial de proteger la seguridad en las instalaciones del CRIM. No obstante, las grabaciones de las cámaras podrán ser utilizadas para identificar aquellas personas que puedan haber cometido actos delictivos y/o cometan o incurran en comportamiento y/o actividades dirigidas a la comisión de un delito, aunque éste no se configure, en contra de la propiedad o personal del CRIM, sus empleados, visitantes y contratistas, basadas en conducta criminal. Las grabaciones de la cámara de seguridad se podrán utilizar además para colaborar con las autoridades del orden público en la prevención de actos

criminales y en los procesos investigativos conducentes a esclarecer delitos al igual que en casos de emergencias médicas, incendios, explosiones y accidentes de cualquier naturaleza.

Sección 3.2 – Operación de las cámaras de vigilancia

Las imágenes serán registradas en formato digital únicamente cuando las cámaras de seguridad detecten movimiento en las escenas. Este movimiento activará automáticamente el sistema de grabación digital. En casos de posibles actos ilegales o cuando la situación lo amerite, de manera razonable, se podrá programar la grabación continua.

De surgir la necesidad, se establecerá la autorización por escrito del Director Ejecutivo, Director de Servicios Administrativos y Director de Recursos Humanos, para la programación de la grabación continua.

Las imágenes serán revisadas por el Director de la Oficina de Servicios Administrativos, por cualquier otro personal autorizado mediante este Reglamento o por el Director Ejecutivo, siempre que se cumpla con el proceso de solicitud dispuesto en este Reglamento. En caso de observar actividades que podrían conducir a la comisión de un delito o a la acusación de una persona, se realizará una anotación correspondiente en el Registro de Incidencias sobre la conducta observada, documento al cual solo tendrá acceso dicho personal autorizado.

Esta anotación deberá incluir fecha, hora, lugar y un resumen detallado de lo observado, indicando si se notificó a alguna persona o a la Policía de Puerto Rico. Aunque las cámaras de seguridad cuentan con capacidad para realizar acercamientos digitales ("zoom digital"), se prohíbe la grabación de sonido. Queda expresamente prohibido grabar sonido mediante otros medios electrónicos.

Sección 3.3 – Funcionamiento

Las cámaras de seguridad operarán de manera continua las veinticuatro (24) horas del día, los siete (7) días de la semana, salvo cualquier eventualidad imprevista relacionada con desperfectos mecánicos.

Sección 3.4 – Localización

Las cámaras de seguridad serán estratégicamente ubicadas en lugares visibles dentro y fuera de las instalaciones del CRIM. Específicamente, se situarán en las áreas de recepción, pasillos principales de los distintos pisos y en cualquier otro lugar que justifique su instalación, del Edificio Central del CRIM y en cada Región. No obstante, de surgir la necesidad de mejorar aspectos de seguridad en las instalaciones se podrán instalar cámaras adicionales o reubicar las existentes. En dichas circunstancias se notificará a los empleados sobre la instalación o relocalización de las cámaras de seguridad.

Es importante destacar que, en ninguna circunstancia, se instalarán cámaras de seguridad en oficinas, cubículos, baños u otros espacios donde exista una expectativa razonable de intimidad por parte de empleados, visitantes o invitados. Queda prohibida la instalación de cámaras de vigilancia ocultas que no puedan ser identificadas o detectadas a simple vista.

Sección 3.5 – Evidencia ante Tribunales

Si un incidente acontecido en las instalaciones del CRIM da lugar a un proceso administrativo, civil o criminal, las grabaciones generadas por el Sistema de Seguridad Electrónica podrán ser utilizadas como evidencia en los procedimientos respectivos.

Sección 3.6 – Cadena de evidencia

Es necesario que cualquier proceso vinculado con la operación del Sistema de Seguridad Electrónica, así como la producción y custodia de las grabaciones generadas por este, se lleve a cabo de manera que se asegure la admisibilidad de dichas grabaciones en un proceso ante un foro con jurisdicción, conforme a las Reglas de Evidencia de Puerto Rico.

Sección 3.7 – Responsabilidad de custodia y protección

El Administrador del Sistema de Seguridad Electrónica, será responsable de la custodia y protección de las grabaciones de las cámaras de seguridad que puedan ser empleadas como evidencia en un tribunal de justicia o foro administrativo.

ARTÍCULO IV – SEGURIDAD DEL SISTEMA

Sección 4.1 – Acceso al Sistema de Seguridad Electrónica

El Sistema de Seguridad Electrónica estará bajo el control, la administración y supervisión de la Oficina de Servicios Administrativos. El Director de dicha Oficina y el Administrador del Sistema de Seguridad Electrónica, serán los funcionarios con la responsabilidad de custodia y control de los acceso al sistema. En circunstancias específicas, se permitirá el acceso al Director Ejecutivo o su representante autorizado, al personal de la Policía de Puerto Rico y al personal de Apoyo Técnico de OGSÍ. Lo anterior, bajo la estricta supervisión del Director de la Oficina de Servicios Administrativos o de un empleado designado por este, incluyendo al Administrador del Sistema de Seguridad Electrónica.

Sección 4.2 – Almacenamiento de grabaciones

Las grabaciones generadas por el Sistema de Seguridad Electrónica del CRIM serán almacenadas en una base de datos designada para este propósito en un servidor, la cual contará con acceso restringido en la Oficina de Gerencia de Sistema de Informática (OGSI).

Sección 4.3 – Monitores

Los monitores, mediante los cuales se podrá observar en tiempo real lo captado y grabado por las cámaras de seguridad, se colocarán estratégicamente en las oficinas de los Administradores Regionales, la Caseta de Seguridad de la Oficina Central y en la Oficina de Servicios Administrativos. Solamente podrán tener acceso al monitoreo electrónico los empleados asignados a trabajar en dichas áreas específicas. Estos empleados deberán ser discretos y guardar la absoluta confidencialidad en el ejercicio de su responsabilidad.

ARTÍCULO V – PRODUCCIÓN Y CONSERVACIÓN DE GRABACIONES DIGITALES

Sección 5.1 – Período regular de imágenes

El Sistema de Seguridad Electrónica del CRIM generará grabaciones que se guardarán en el banco de datos del sistema. Estas grabaciones de las cámaras de seguridad se conservarán durante un periodo mínimo de diez (10) días. Una vez transcurrido este plazo, el sistema continuará grabando, sobrescribiendo la imagen más antigua en el banco de datos.

Sección 5.2 – Protección de eventos específicos en el sistema

Cuando se produzca un incidente se registrará en el Registro de Incidencias del Sistema de Seguridad Electrónica, y el Administrador del Sistema de Seguridad Electrónica o la persona designada por el Director de la Oficina de Servicios Administrativos protegerá y conservará en el Sistema de Seguridad Electrónica tanto el lapso del incidente como las grabaciones de las cámaras que lo capturaron. Esto se realiza para evitar que dichas grabaciones sean borradas, alteradas o destruidas al transcurrir el período de los diez (10) días. Las grabaciones de incidentes serán almacenadas hasta que pierdan su utilidad o por un periodo máximo de dos (2) años.

Sección 5.3 – Solicitud de inspección y requisito de Orden o *subpoena*

Si, con el propósito de investigar un incidente ocurrido en cualquiera de las instalaciones del CRIM, se requiere inspeccionar o que se produzca de copia de las imágenes o grabaciones de las cámaras de seguridad del CRIM, la persona o entidad que así lo requiera deberá presentar una solicitud por escrito al Director Ejecutivo. Dicha solicitud deberá de acompañarse por una Orden o *Subpoena*, debidamente emitido por el Tribunal, la entidad administrativa o gubernamental, con facultad y competencia. Disponiéndose que, de ordinario las grabaciones de las cámaras de seguridad, de ordinario, se conservarán durante un periodo mínimo de diez (10) días, con las excepciones dispuestas en este Reglamento, por lo que debe procurarse realizar la solicitud dentro de dicho periodo.

ARTÍCULO VI – DUPLICIDAD DE IMÁGENES

Sección 6.1 – Autorización

En situaciones en las que se necesite acceder al contenido de una copia de las grabaciones de las cámaras de seguridad con fines investigativos, su reproducción será autorizada solo mediante Orden o *Subpoena*. Las copias generadas solo podrán ser entregadas a personas debidamente autorizadas por el Tribunal o la entidad administrativa o gubernamental competente y se escribirá lo gestionado en el Registro de Incidencias del Sistema de Seguridad Electrónica.

Sección 6.2 – Copias de grabaciones

La entrega de copias de grabaciones provenientes de las cámaras de seguridad se formalizará mediante un recibo oficial, el cual será firmado tanto por el empleado de la Oficina que realiza la

entrega como por la persona que recibe la copia. En dicho recibo detallará la fecha, hora y autorización para la entrega. Esta transacción será registrada en el Registro de incidencias del sistema de Seguridad Electrónica.

Sección 6.3 – Registro de revisión de grabaciones

El Administrador del Sistema de Seguridad Electrónica, o cualquier otro empleado designado por el Director de la Oficina de Servicios Administrativos, llevará a cabo un "Registro de Revisión de Grabaciones". En dicho Registro se deberá consignar el día, la fecha y la hora de cada revisión de grabaciones, copia de la Orden o *Subpoena* que autorice la revisión, incluyendo el nombre e identificación de las personas que participen en la observación de las imágenes, así como el propósito de la revisión y los archivos eliminados, en caso de haberlos.

ARTÍCULO VII – NOTIFICACIÓN, PUBLICIDAD Y RECLAMACIONES

Sección 7.1 – Notificación

Previo a la implementación del Sistema de Seguridad Electrónica se colocará un aviso público en un lugar de acceso público en las instalaciones del CRIM donde se estará utilizando dicho sistema, tal como un tablón de edictos o área similar. El Sistema de Seguridad Electrónica debe ser notificado a los empleados del CRIM para informar sobre lo siguiente, pero sin limitarse a:

- a) Tipo de seguridad electrónica
- b) Naturaleza de los datos a recopilar
- c) Frecuencia de uso del medio de Seguridad
- d) Ubicación del sistema de Seguridad Electrónica
- e) Emplazamiento del equipo de monitoreo
- f) Grupo de empleados sujeto a observación
- g) Mecanismo administrativo para gestionar situaciones de los empleados

Sección 7.2 – Avisos de advertencia

Todas las áreas del CRIM, donde estén en funcionamiento las cámaras de seguridad, deberá tener un aviso que informe sobre la operación de un sistema de grabación sin audio, las veinticuatro (24) horas del día, siete (7) días de la semana.

Sección 7.3 – Procedimiento de reclamaciones o quejas

Todo tipo de reclamación o queja derivada de la aplicación e interpretación de este Reglamento deberá ser formalizada por escrito y dirigida al Director Ejecutivo. La documentación de la reclamación debe contener detalles del evento o situación específica que la fundamenta. El Director Ejecutivo podrá designar a una persona quien investigará la queja o reclamación. El Director Ejecutivo procederá a tomar la determinación correspondiente de acuerdo con las disposiciones de

este Reglamento y las facultades conferidas mediante el Código Municipal. La determinación será notificada al querellante en un término razonable.

Sección 7.4 – Prohibición

1. Ninguna persona podrá darles a las cámaras de seguridad un uso ilegal, inapropiado o que contravenga las disposiciones en este Reglamento.
2. Se prohíbe la cesión o copia de imágenes obtenidas de conformidad con lo dispuesto en este Reglamento.
3. Se prohíbe el uso del Sistema de Seguridad Electrónica en manera alguna que infrinja el derecho constitucional a la intimidad que tienen nuestros empleados o los ciudadanos.

ARTÍCULO VIII – DISPOSICIONES FINALES

Sección 8.1 – Clausula de Salvedad

La declaración de inconstitucionalidad o nulidad de cualquiera de los Artículos o partes de ellos no afectara la validez de los Artículos restantes.

Sección 8.2 – Enmiendas

Toda enmienda o cambio a este Reglamento, deberá efectuarse conforme las disposiciones de la Ley Núm. 107-2020, según enmendada, mejor conocida como “Código Municipal de Puerto Rico” y la Ley Núm. 38 del 30 de junio de 2017, según enmendada, conocida como “Ley de Procedimiento Administrativo Uniforme del Gobierno de Puerto Rico” (LPAU).

Sección 8.3 – Vigencia

Este Reglamento entrará en vigor luego de su radicación y promulgación por el Departamento de Estado, de conformidad con la Ley Núm. 38 del 30 de junio de 2017, según enmendada, conocida como “Ley de Procedimiento Administrativo Uniforme del Gobierno de Puerto Rico” (LPAU).

Aprobado en reunión ordinaria de la Junta de Gobierno del CRIM, Resolución 2024-54, el 25 de abril de 2024



Reinaldo J. Paniagua Látimer
Director Ejecutivo

Presentado en el Departamento de Estado el 21 de noviembre de 2024.