



Proceso de Gestión de la Seguridad Institucional

Subproceso de Seguridad Electrónica

Procedimiento para creación, autorización y control de accesos a sistemas VMS

Versión: 01	Fecha de elaboración: Agosto - 2026
-------------	-------------------------------------

Elaborado por:	
Lic. Adrián Murillo Sánchez	Subproceso Especializado de Seguridad Electrónica

Revisado por:	
Msc. Armando Brenes Morales	Subproceso Especializado de Seguridad Electrónica

Aprobado por:	
Lic. Edward Rodríguez Rodríguez	Gestión de la Seguridad Institucional



seguridad@poder-judicial.go.cr



(506) 2295-3841



4to. Piso, Edificio de la Plaza de la Justicia, I Circuito Judicial
Barrio González Lahamann, San José Costa Rica.



1. Introducción

La seguridad de los sistemas de videovigilancia institucional constituye un componente fundamental para la protección de la información, la infraestructura y los recursos tecnológicos utilizados en el cumplimiento de las funciones institucionales. Los sistemas de gestión de video (VMS) permiten el acceso a imágenes en vivo y, de acuerdo con los permisos otorgados, a grabaciones de las cámaras institucionales, por lo que resulta necesario establecer controles que garanticen que dicho acceso sea realizado únicamente por personas debidamente autorizadas y de acuerdo con las funciones que desempeñan.

En este contexto, el presente procedimiento establece los lineamientos para la creación, autorización, asignación, administración, revisión, modificación y retiro de los accesos a los sistemas VMS institucionales. Asimismo, define las responsabilidades de las jefaturas, oficinas, administraciones, personas usuarias y del Subproceso Especializado de Seguridad Electrónica, procurando mantener una adecuada separación entre las responsabilidades administrativas de autorización, la administración técnica de los sistemas y el uso de las credenciales.

2. Objetivo

Establecer los lineamientos para la creación, asignación, administración, uso, control, revisión y deshabilitación de las credenciales de acceso a los sistemas VMS institucionales, utilizados para el monitoreo de cámaras institucionales, con el propósito de fortalecer la seguridad de la información, preservar la confidencialidad de las credenciales, garantizar la trazabilidad de los accesos y reducir el riesgo de accesos no autorizados o de uso inadecuado del sistema.



seguridad@poder-judicial.go.cr



(506) 2295-3841



4to. Piso, Edificio de la Plaza de la Justicia, I Circuito Judicial
Barrio González Lahamann, San José Costa Rica.

3. Alcance

Este procedimiento aplica a todas las personas funcionarias que requieran acceso a los sistemas VMS institucionales para el cumplimiento de sus funciones institucionales, independientemente de la dependencia a la que pertenezcan.

Comprende la administración de los siguientes tipos de personas usuarias:

- Personas usuarias del Departamento de Seguridad.
- Personas usuarias administrados por Administraciones Regionales.
- Personas usuarias del Organismo de Investigación Judicial (OIJ).

Asimismo, contempla tanto las cuentas administradas directamente dentro de los sistemas VMS institucionales como aquellas que, cuando las capacidades técnicas del sistema lo permitan, sean autenticadas mediante integración con Directorio Activo institucional.

4. Definiciones

Palabra/Término	Definición
VMS	Sistema de gestión de video (Video Management System) utilizado para la administración, visualización y gestión de las cámaras de videovigilancia.
Credencial de acceso	Conjunto de datos compuesto por un nombre de usuario y una contraseña que permite la autenticación de una persona usuaria en el sistema VMS
Persona usuaria	Persona funcionaria autorizada para acceder al sistema VMS mediante una cuenta individual.



Departamento de Seguridad

Proceso de Gestión de la Seguridad Institucional

Dirección Ejecutiva – Poder Judicial



Persona usuaria Departamento de Seguridad	Persona funcionaria cuyo acceso al sistema VMS es autorizado por una de las jefaturas del Departamento de Seguridad. La jefatura correspondiente determina las cámaras a las que tendrá acceso la persona usuaria y establece si contará con permisos para consultar grabaciones o únicamente para realizar visualización en vivo.
Persona usuaria Administración regional	Persona funcionaria cuyo acceso es autorizado y administrado por una Administración Regional para la visualización de las cámaras correspondientes a los edificios bajo su administración. Este tipo de usuario tendrá, como regla general, permisos exclusivamente para visualización en vivo.
Persona usuaria OIJ	Persona funcionaria del Organismo de Investigación Judicial cuyo acceso es autorizado por la jefatura de la Delegación correspondiente. El acceso comprende las cámaras propias del OIJ y, cuando corresponda, determinadas cámaras ubicadas en zonas comunes de edificios compartidos con otras administraciones. La visualización será, como regla general, en vivo, con las excepciones que expresamente determine la jefatura de la Delegación.
Usuario de red	Cuenta institucional utilizada para la autenticación de una persona funcionaria en los servicios tecnológicos integrados con Directorio Activo.



seguridad@poder-judicial.go.cr



(506) 2295-3841



4to. Piso, Edificio de la Plaza de la Justicia, I Circuito Judicial
Barrio González Lahamann, San José Costa Rica.

Departamento de Seguridad

Proceso de Gestión de la Seguridad Institucional

Dirección Ejecutiva – Poder Judicial



	Cuando el VMS institucional se encuentre integrado con Directorio Activo, las credenciales utilizadas para ingresar corresponderán a las credenciales institucionales de red de la persona funcionaria.
Directorio Activo	Servicio institucional utilizado para la administración y autenticación de las cuentas de usuario de red, incluyendo los mecanismos relacionados con sus credenciales.
Oficina o administración responsable	Dependencia que autoriza el acceso de la persona funcionaria y que tiene la responsabilidad de comunicar oportunamente cualquier cambio que implique que la persona usuaria deje de requerir el acceso al sistema.
Deshabilitación	Acción mediante la cual se inactiva una cuenta de usuario en el VMS o se retiran los permisos que permiten su acceso al VMS, según el mecanismo de autenticación utilizado.
Trazabilidad	Capacidad de determinar, mediante los registros disponibles en el sistema, la cuenta de usuario asociada a los accesos y acciones efectuadas en el VMS.
Credenciales	Corresponde al nombre de usuario y la contraseña utilizados para acceder al VMS, sean estas administradas propiamente por el VMS o por el Directorio Activo.

5. Responsabilidades

Responsable	Responsabilidad
Jefatura del Subproceso Especializado de Seguridad Electrónica, Coordinación del Centro de Operaciones de Seguridad o Electrónica o la persona designada por estos.	• Administrar técnicamente las cuentas de usuario en los sistemas VMS institucionales. • Crear las cuentas únicamente cuando exista la autorización correspondiente de la jefatura, administración u oficina responsable. • Configurar los permisos de acceso de acuerdo con lo expresamente autorizado. • Generar contraseñas robustas mediante herramientas destinadas para tal fin cuando las cuentas sean administradas directamente en los sistemas VMS institucionales. • Comunicar las credenciales directamente a la persona usuaria autorizada cuando se trate de cuentas administradas directamente en los VMS institucionales, evitando intermediarios durante la entrega de la contraseña. • Mantener los registros administrativos relacionados con la creación, modificación y deshabilitación de las cuentas. • Atender las solicitudes de cambio de permisos, modificación de cuentas o deshabilitación. • Atender los reportes relacionados con pérdida, divulgación, compromiso o uso indebido de credenciales. • Realizar revisiones periódicas de las cuentas existentes, de acuerdo con las posibilidades operativas y técnicas disponibles.

Departamento de Seguridad

Proceso de Gestión de la Seguridad Institucional

Dirección Ejecutiva – Poder Judicial



	• Aplicar las medidas correspondientes cuando se determine que una credencial ha sido comprometida o utilizada de manera indebida. • Administrar los roles y permisos dentro del VMS cuando la autenticación se realice mediante Directorio Activo.
Jefaturas del Proceso y Subproceso Administrativo y Operativo del Departamento de Seguridad	• Autorizar la creación de cuentas de usuario pertenecientes al Departamento. • Determinar las cámaras que cada persona usuaria podrá visualizar. • Determinar si la persona usuaria tendrá acceso a grabaciones o únicamente a visualización en vivo. • Solicitar las modificaciones de permisos cuando cambien las funciones o necesidades de acceso de la persona usuaria. • Comunicar oportunamente cuando una persona deje de requerir el acceso al sistema.
Administraciones Regionales	• Autorizar la creación de cuentas de usuario que requieran acceso a cámaras de los edificios bajo su administración. • Identificar a las personas funcionarias que requieren el acceso. • Determinar los edificios o cámaras que corresponden al ámbito de acceso autorizado. • Solicitar oportunamente cualquier modificación de los accesos autorizados. • Comunicar al Subproceso Especializado de Seguridad Electrónica cuando una persona usuaria deje de requerir el acceso, sea trasladada, cambie de funciones o cese sus funciones.

Departamento de Seguridad

Proceso de Gestión de la Seguridad Institucional

Dirección Ejecutiva – Poder Judicial



Jefaturas de las Delegaciones del OIJ	• Autorizar la creación de cuentas de usuario pertenecientes a la Delegación. • Determinar las cámaras propias del OIJ a las que podrá acceder cada persona usuaria. • Determinar, cuando corresponda, el acceso a cámaras ubicadas en zonas comunes de edificios compartidos. • Establecer las excepciones a la visualización en vivo que considere necesarias de acuerdo con las funciones de la persona usuaria. • Solicitar oportunamente cualquier modificación o eliminación de los permisos otorgados. • Comunicar cuando una persona usuaria deje de requerir el acceso al sistema.
Personas usuarias	• Mantener la confidencialidad de sus credenciales. • Utilizar exclusivamente sus propias credenciales. • No compartir, prestar, divulgar o facilitar sus credenciales a terceras personas. • No permitir que otra persona utilice su sesión o cuenta. • Utilizar el sistema únicamente para el cumplimiento de las funciones institucionales para las cuales fue autorizada. • Informar inmediatamente cualquier sospecha de pérdida, divulgación, compromiso o uso indebido de sus credenciales. • Abstenerse de almacenar o comunicar su contraseña de manera que pueda quedar disponible para personas no autorizadas.

6. Procedimiento

6.1 Solicitud y autorización

La creación de una cuenta deberá originarse en una solicitud de la dependencia responsable de la persona funcionaria.

La solicitud deberá identificar como mínimo:

- Nombre de la persona funcionaria.
- Nombre del usuario de red de la persona funcionaria.
- Dependencia a la que pertenece.
- Tipo de usuario.
- Justificación o necesidad de acceso.
- Cámaras, edificios o áreas que requiere visualizar.
- Tipo de visualización requerida.
- Si requiere acceso a grabaciones, cuando corresponda.
- Nombre de la jefatura o administración que autoriza.
- Para el plazo de vigencia de los permisos solicitados, corresponde a la dependencia responsable indicar el tiempo por el cual será requerido el acceso. (será empleado en los VMS que lo permitan)

El Subproceso Especializado de Seguridad Electrónica verificará que la solicitud cuente con la autorización correspondiente antes de proceder con la creación de la cuenta.

La jefatura inmediata deberá remitir la solicitud al siguiente correo Centro_Operaciones_Seguridad@Poder-Judicial.go.cr del Departamento de Seguridad.



seguridad@poder-judicial.go.cr



(506) 2295-3841



4to. Piso, Edificio de la Plaza de la Justicia, I Circuito Judicial
Barrio González Lahamann, San José Costa Rica.

6.2 Creación de la cuenta

Una vez validada la autorización, se procederá con la creación de una cuenta por parte del Subproceso Especializado de Seguridad Electrónica individual para la persona usuaria.

No se deberán crear cuentas genéricas o compartidas cuando la plataforma permita la asignación de cuentas individuales.

Los permisos serán configurados conforme a la autorización recibida, aplicando únicamente los accesos necesarios para el cumplimiento de las funciones de la persona usuaria.

6.3 Generación de la contraseña

Cuando la cuenta sea administrada directamente en el VMS institucional, la contraseña será generada mediante una herramienta destinada para la generación de contraseñas robustas.

Se procurará que las contraseñas cumplan criterios de seguridad relacionados con:

- Longitud adecuada.
- Complejidad.
- Combinación de diferentes tipos de caracteres.
- Ausencia de información personal fácilmente identificable.
- Imposibilidad de asociación directa con el nombre o usuario de la persona.

No se utilizarán contraseñas predecibles, patrones simples o claves compartidas entre diferentes personas usuarias.

Las contraseñas deberán ser modificadas cuando exista sospecha de compromiso, divulgación, pérdida de confidencialidad o cuando corresponda realizar una renovación periódica conforme a las capacidades de la plataforma y las disposiciones institucionales aplicables.



seguridad@poder-judicial.go.cr



(506) 2295-3841



4to. Piso, Edificio de la Plaza de la Justicia, I Circuito Judicial
Barrio González Lahamann, San José Costa Rica.

6.4 Entrega de las credenciales

Cuando las cuentas sean administradas directamente en el VMS institucional, las credenciales serán comunicadas directamente a la persona usuaria autorizada.

La contraseña no será entregada a jefaturas, compañeros de trabajo, intermediarios, personal administrativo ni terceras personas para que posteriormente sea comunicada al usuario final.

El objetivo de esta medida es preservar la confidencialidad de la contraseña desde el momento de su generación hasta su recepción por la persona a quien pertenece.

La persona usuaria deberá mantener bajo su responsabilidad y custodia la contraseña recibida.

6.5 Administración de credenciales mediante Directorio Activo

En aquellos sistemas VMS que permitan la integración con Directorio Activo institucional, la autenticación de las personas usuarias se realizará mediante las credenciales de red institucionales asignadas por la dependencia competente.

En estos casos, el nombre de usuario y la contraseña utilizados para acceder al VMS corresponderán a las credenciales institucionales de red de la persona usuaria, por lo que el Subproceso Especializado de Seguridad Electrónica no generará, asignará, conocerá ni administrará dichas contraseñas.

La administración de las credenciales de red, incluyendo su creación, modificación, cambio, restablecimiento, bloqueo y demás controles asociados a las contraseñas, corresponderá a la instancia institucional responsable de la administración de Directorio Activo y de las cuentas de usuario de red.



seguridad@poder-judicial.go.cr



(506) 2295-3841



4to. Piso, Edificio de la Plaza de la Justicia, I Circuito Judicial
Barrio González Lahamann, San José Costa Rica.

Departamento de Seguridad

Proceso de Gestión de la Seguridad Institucional

Dirección Ejecutiva – Poder Judicial



El Subproceso Especializado de Seguridad Electrónica será responsable, dentro del VMS, de:

- Validar que la persona usuaria cuente con la autorización correspondiente para acceder al sistema.
- Incorporar o habilitar la cuenta de red autorizada dentro del VMS, conforme a las capacidades de integración disponibles.
- Asignar los roles y permisos correspondientes de acuerdo con la autorización emitida por la jefatura, oficina o administración responsable.
- Determinar y configurar, cuando las capacidades del VMS lo permitan, las cámaras, grupos de cámaras, funcionalidades y niveles de acceso que correspondan a la persona usuaria.
- Modificar o retirar los roles y permisos dentro del VMS cuando exista una solicitud de la dependencia responsable o cuando corresponda como resultado de una revisión de los accesos.

En este esquema, la responsabilidad sobre la confidencialidad y el uso de las credenciales de red continuará correspondiendo a la persona usuaria y a las instancias responsables de la administración de las cuentas institucionales, mientras que el Subproceso Especializado de Seguridad Electrónica será responsable de la correcta asignación y administración de los permisos y roles dentro del VMS.

Cuando una persona funcionaria deje de requerir acceso al VMS, la dependencia responsable deberá comunicarlo a las instancias correspondientes. El Subproceso Especializado de Seguridad Electrónica procederá a retirar o modificar los roles y permisos asignados dentro del VMS, según corresponda. La deshabilitación de la cuenta de red continuará siendo responsabilidad de la instancia administradora de Directorio Activo.



seguridad@poder-judicial.go.cr



(506) 2295-3841



4to. Piso, Edificio de la Plaza de la Justicia, I Circuito Judicial
Barrio González Lahamann, San José Costa Rica.

7. Control y registro de las cuentas

El Subproceso Especializado de Seguridad Electrónica mantendrá un registro administrativo de las cuentas creadas en los sistemas VMS institucionales.

El registro deberá permitir identificar, según la información disponible:

- Persona usuaria.
- Nombre de red de la persona usuaria.
- Dependencia.
- Tipo de usuario.
- Fecha de creación.
- Dependencia o jefatura que autorizó.
- Cámaras o edificios autorizados.
- Nivel de acceso autorizado.
- Modificaciones realizadas.
- Fecha de deshabilitación o retiro de permisos, cuando corresponda.
- Tipo de autenticación utilizado, cuando resulte necesario para efectos de control.

El registro administrativo de las cuentas deberá mantenerse actualizado para facilitar las labores de control y revisión.

La trazabilidad de los accesos y acciones efectuadas dentro del sistema VMS institucional será determinada mediante los mecanismos de registro y auditoría disponibles en la propia plataforma, de forma que las acciones puedan asociarse con la cuenta individual que las efectuó.

Cuando exista integración con Directorio Activo, la trazabilidad dentro del VMS deberá asociarse con la cuenta institucional utilizada para la autenticación.



seguridad@poder-judicial.go.cr



(506) 2295-3841



4to. Piso, Edificio de la Plaza de la Justicia, I Circuito Judicial
Barrio González Lahamann, San José Costa Rica.

8. Deshabilitación de cuentas y retiro de accesos

8.1 Responsabilidad de las oficinas, administraciones y jefaturas

El Subproceso Especializado de Seguridad Electrónica no determina por sí mismo los cambios de funciones, traslados o cese de las personas funcionarias pertenecientes a otras dependencias.

Por lo tanto, corresponde a la oficina, administración o jefatura responsable comunicar oportunamente cuando una persona deje de requerir acceso al sistema, cambie de funciones, sea trasladada o cese sus funciones.

La responsabilidad de comunicar oportunamente estas situaciones corresponde a la dependencia responsable de la persona usuaria.

Una vez recibida la comunicación correspondiente, el Subproceso Especializado de Seguridad Electrónica procederá técnicamente con el retiro o modificación del acceso dentro del VMS, de acuerdo con el mecanismo de autenticación utilizado.

La jefatura inmediata deberá remitir la solicitud al siguiente correo [Centro Operaciones Seguridad@Poder-Judicial.go.cr](mailto:Centro_Operaciones_Seguridad@Poder-Judicial.go.cr) del Departamento de Seguridad.

En consecuencia, las responsabilidades se distribuyen de la siguiente manera:

- **Oficina, administración o jefatura responsable:** comunica oportunamente que el acceso ya no es requerido.
- **Subproceso Especializado de Seguridad Electrónica:** retira o modifica técnicamente el acceso dentro del VMS.

Esta distribución permite mantener claramente diferenciadas las responsabilidades administrativas, técnicas y de administración de las credenciales institucionales.

La forma de retirar el acceso dependerá del mecanismo de autenticación utilizado.

8.2 Cuentas administradas directamente en el sistema VMS institucional

Cuando la cuenta sea administrada directamente en el sistema VMS institucional, la deshabilitación será realizada técnicamente por el Subproceso Especializado de Seguridad Electrónica una vez recibida la solicitud formal de la oficina, administración o jefatura responsable.

La solicitud deberá indicar, cuando corresponda, la persona usuaria y la razón por la cual deja de requerir el acceso.

Una vez recibida la solicitud, el Subproceso Especializado de Seguridad Electrónica procederá con la inactivación de la cuenta de manera inmediata o con la mayor prontitud operativa posible.

8.3 Cuentas autenticadas mediante Directorio Activo

Cuando el VMS se encuentre integrado con Directorio Activo, el retiro del acceso al sistema se efectuará mediante la eliminación, modificación o desasignación de los roles y permisos correspondientes dentro del VMS.

En este escenario, el Subproceso Especializado de Seguridad Electrónica será responsable de retirar o modificar los permisos y roles asignados a la persona usuaria dentro del VMS.

La deshabilitación, bloqueo o eliminación de la cuenta institucional de red no corresponderá al Subproceso Especializado de Seguridad Electrónica, sino a la instancia responsable de la administración de Directorio Activo.



seguridad@poder-judicial.go.cr



(506) 2295-3841



4to. Piso, Edificio de la Plaza de la Justicia, I Circuito Judicial
Barrio González Lahamann, San José Costa Rica.

9. Pérdida o uso indebido de credenciales que comprometa la seguridad de los sistemas.

Cuando una persona usuaria tenga conocimiento o sospecha de que su contraseña ha sido conocida por otra persona, perdida, divulgada o utilizada de manera indebida, será responsable de comunicarlo inmediatamente al Subproceso Especializado de Seguridad Electrónica.

Cuando se trate de una cuenta administrada directamente en los sistemas VMS institucionales, se valorará la aplicación de medidas como:

- Cambio de contraseña.
- Deshabilitación temporal de la cuenta.
- Revisión de los accesos efectuados.
- Verificación de los registros disponibles en el VMS.
- Modificación de los permisos.
- Deshabilitación definitiva de la cuenta cuando corresponda.

Cuando se trate de una cuenta autenticada mediante Directorio Activo, el Subproceso Especializado de Seguridad Electrónica podrá retirar a solicitud de la persona afectada o su jefatura de manera temporalmente los roles o permisos dentro del VMS y deberá comunicar la situación a la instancia responsable de la administración de la cuenta institucional, cuando corresponda, será responsabilidad de la persona afectada o su jefatura gestionar lo correspondiente ante la entidad responsable del Directorio Activo.

La medida aplicable dependerá de la naturaleza y gravedad de la situación reportada.



seguridad@poder-judicial.go.cr



(506) 2295-3841



4to. Piso, Edificio de la Plaza de la Justicia, I Circuito Judicial
Barrio González Lahamann, San José Costa Rica.

10. Modificación de permisos

Los permisos de una cuenta no deberán modificarse sin la autorización de la dependencia responsable.

Para los usuarios del Departamento de Seguridad, las modificaciones deberán ser autorizadas por la jefatura correspondiente.

Para los usuarios administrados por las Administraciones Regionales, las modificaciones deberán ser solicitadas por la Administración Regional correspondiente.

Para los usuarios del OIJ, las modificaciones deberán ser autorizadas por la jefatura de la Delegación correspondiente.

El Subproceso Especializado de Seguridad Electrónica realizará técnicamente la modificación de los permisos conforme a la autorización recibida y dejará constancia de la modificación en el registro correspondiente.

Cuando el VMS utilice Directorio Activo, las modificaciones se efectuarán mediante la asignación, modificación o retiro de los roles y permisos correspondientes dentro del VMS.

11. Matriz general de autorización y acceso

Tipo de usuario	Quién autoriza	Cámaras a las que puede acceder	Visualización	Grabaciones
Departamento de Seguridad	Jefaturas del Proceso y Subproceso Administrativo y Operativo del Departamento de Seguridad	Las definidas por la jefatura	En vivo	Según autorización de la jefatura



seguridad@poder-judicial.go.cr



(506) 2295-3841



4to. Piso, Edificio de la Plaza de la Justicia, I Circuito Judicial
Barrio González Lahamann, San José Costa Rica.

Departamento de Seguridad

Proceso de Gestión de la Seguridad Institucional

Dirección Ejecutiva – Poder Judicial



COSE	Coordinador del COSE	Todas las definidas por el Coordinador	En vivo	Autorizado
Administración Regional	Administración Regional correspondiente	Cámaras de los edificios bajo su administración	En vivo	No autorizado como regla general
TI	Administración Regional correspondiente	Cámaras autorizadas por la Administración.	En vivo	Autorizado
OIJ	Jefatura de la Delegación del OIJ	Cámaras propias del OIJ y, cuando corresponda, zonas comunes autorizadas	En vivo	No autorizado como regla general, salvo excepciones definidas por la jefatura

Nota: Los niveles de acceso indicados estarán sujetos a las autorizaciones específicas emitidas por las jefaturas o administraciones responsables y a las capacidades técnicas del VMS utilizado.

12. Disposiciones de seguridad

Como parte de la administración de las credenciales se establecen los siguientes controles:

- **Cuentas individuales:** cada persona usuaria deberá disponer de sus propias credenciales o cuenta institucional individual.
- **Contraseñas robustas:** las contraseñas administradas directamente en el VMS serán generadas mediante herramientas destinadas para este propósito.
- **Confidencialidad:** las contraseñas administradas en el VMS serán entregadas directamente a la persona usuaria, sin intermediarios.
- **Uso personal e intransferible:** queda prohibido compartir o facilitar las credenciales.
- **Autenticación institucional:** cuando exista integración con Directorio Activo, se utilizarán las credenciales institucionales de red de la persona funcionaria.
- **Asignación según autorización:** los permisos se configurarán conforme a la autorización de la jefatura, oficina o administración correspondiente.
- **Principio de necesidad:** se asignarán únicamente los accesos necesarios para el cumplimiento de las funciones autorizadas.
- **Registro administrativo:** se mantendrá información sobre las cuentas, autorizaciones y modificaciones realizadas.
- **Trazabilidad:** se utilizarán los mecanismos de registro disponibles en el VMS institucional para identificar las cuentas asociadas con los accesos y acciones efectuadas.
- **Revisión periódica:** se realizarán revisiones de las cuentas y permisos existentes.
- **Retiro de acceso:** los accesos serán retirados cuando la dependencia responsable comunique que la persona ya no requiere el acceso.
- **Atención de incidentes de seguridad:** las credenciales comprometidas o utilizadas indebidamente serán sometidas a las medidas de seguridad correspondientes.



seguridad@poder-judicial.go.cr



(506) 2295-3841



4to. Piso, Edificio de la Plaza de la Justicia, I Circuito Judicial
Barrio González Lahamann, San José Costa Rica.

13. Responsabilidad sobre la información de los accesos

La autorización del acceso a las cámaras y la determinación de los permisos corresponde a las jefaturas, oficinas y administraciones responsables de cada tipo de usuario, de acuerdo con lo establecido en este procedimiento.

La administración técnica de las cuentas dentro del sistema VMS institucional corresponde al Subproceso Especializado de Seguridad Electrónica.

Cuando las cuentas sean administradas directamente en el VMS, el Subproceso será responsable de la generación y entrega directa de las contraseñas a las personas usuarias.

Cuando exista integración con Directorio Activo, la administración de las contraseñas y cuentas institucionales de red corresponderá a la instancia responsable de Directorio Activo, mientras que el Subproceso Especializado de Seguridad Electrónica será responsable de la asignación y administración de los roles y permisos dentro del VMS.

La persona usuaria es responsable del uso y resguardo de sus propias credenciales.

La separación de estas responsabilidades permite establecer claramente quién autoriza el acceso, quién administra técnicamente los permisos dentro del VMS y quién es responsable del uso de las credenciales.



seguridad@poder-judicial.go.cr



(506) 2295-3841



4to. Piso, Edificio de la Plaza de la Justicia, I Circuito Judicial
Barrio González Lahamann, San José Costa Rica.

14. Incumplimiento

El incumplimiento de las disposiciones establecidas en este procedimiento podrá generar la aplicación de las medidas administrativas o legales que correspondan, de acuerdo con la normativa institucional vigente o leyes que así lo determinen.

En particular, el uso de credenciales de otra persona, la divulgación de contraseñas, el acceso a cámaras no autorizadas o el uso del sistema para fines distintos de los relacionados con las funciones institucionales deberán ser reportados a la jefatura correspondiente para la valoración de las acciones procedentes.

15. Contacto

Consultas respecto al Procedimiento para creación, autorización y control de accesos a sistemas VMS a la extensión 01-3023, número directo 2295-3023 o al correo Centro_Operaciones_Seguridad@Poder-Judicial.go.cr



seguridad@poder-judicial.go.cr



(506) 2295-3841



4to. Piso, Edificio de la Plaza de la Justicia, I Circuito Judicial
Barrio González Lahamann, San José Costa Rica.