INFORME ESPECIAL RELACIONADO CON LA INSPECCIÓN DEL CUARTO DE TI Y FUNCIONAMIENTO DEL SISTEMA DE GRABACIÓN EN EL CEAAM HUETAR CARIBE, DURANTE EL PRIMER SEMESTRE 2025.

INAMU-JD-AI-In-011-2025

(Remitido con oficio INAMU-JD-AI-172-2025)

Firmas de validación del informe	
Realizado por	**Revisado por**
DAVID ANTONIO SOBALBARRO RODRIGUEZ (FIRMA) Firmado digitalmente por DAVID ANTONIO SOBALBARRO RODRIGUEZ (FIRMA) Fecha: 2025.07.30 15:01:25 -06'00'	RANDALL ALONSO UMAÑA VILLALOBOS (FIRMA) Firmado digitalmente por RANDALL ALONSO UMAÑA VILLALOBOS (FIRMA) Fecha: 2025.07.30 14:23:13 -06'00'
David Sobalbarro Rodríguez Profesional Ejecutivo encargado del estudio Auditoría Interna	Randall Umaña Villalobos Auditor Interno Auditoría Interna

INSTITUTO NACIONAL DE LAS MUJERES.

INFORME DE ESTUDIO DE CONTROL INTERNO RELACIONADO CON LA INSPECCIÓN DEL CUARTO DE TI Y FUNCIONAMIENTO DEL SISTEMA DE GRABACIÓN EN EL CEAAM HUETAR CARIBE, DURANTE EL PRIMER SEMESTRE 2025.

El presente estudio de auditoría se realizó en cumplimiento del Plan de Trabajo de la Auditoría Interna para el periodo 2025, el objetivo consistió en realizar una visita al cuarto de TI y revisar el funcionamiento del sistema de video vigilancia del ***Centro Especializado de Atención y Albergue Temporal para Mujeres Afectadas por Violencia*** ubicado en la Región Huetar Caribe, en adelante denominado ***CEAAM Huetar Caribe***.

La auditoría se enfocó en realizar una revisión de los aspectos de seguridad física y condiciones del cuarto de TI, así como revisión de la funcionalidad del sistema de grabación o videovigilancia, entre otros aspectos relacionados con la administración y/o operación de ambos.

Julio, 2025.

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

ÍNDICE DE FIGURAS

TABLA DE NOMENCLATURAS

Nomenclatura	Significado
INAMU	Instituto Nacional de las Mujeres.
CEAAM	Centro Especializado de Atención y Albergue Temporal para Mujeres Afectadas por Violencia.
CGR	Contraloría General de la Republica.
COBIT	Marco de referencia de buenas prácticas de tecnología.
CONCIENTIZACIÓN	Adquirir conciencia de algún tema en específico.
CONTROL INTERNO	Procesos y prácticas empresariales de control.
CUARTO DE TI	Espacio físico o sala con equipos de TI (Informática).
INFRAESTRUCTURA	Estructura tecnológica.
ISO	Norma o estándar internacional.
LGCI	Ley General de Control Interno.
CCTV	Circuito Cerrado de Televisión
NTPP	Normas Técnicas de Presupuesto Público.
TI	Tecnologías de la Información.

1 RESUMEN EJECUTIVO

¿QUÉ EXAMINAMOS?

El estudio es de carácter especial, y tuvo como propósito hacer una revisión de las condiciones del cuarto de TI y el funcionamiento del sistema de grabación de cámaras de seguridad del CEAAM Huetar Caribe para el periodo 2025, lo anterior se realiza en cumplimiento al programa de trabajo de Auditoría Interna del presente año.

Dentro de los aspectos a revisar se consideró la seguridad física y ambiental de los equipos, los procedimientos de administración, control interno y el análisis de la información, también, se examinó la funcionalidad del sistema de videovigilancia su operación y monitoreo, con eso, aspectos de parametrización, características de la aplicación, funcionalidad, entre otros.

¿POR QUÉ ES IMPORTANTE?

La auditoría especial de cumplimiento permite garantizar la calidad, la protección de la información y activos Institucionales, al mismo tiempo, permite identificar oportunidades de mejora y/o riesgos que pueden afectar las operaciones e imagen de la Institución, siendo así, que este tipo de estudio permitirá tomar decisiones basadas en la información y con esto una buena gestión empresarial.

Anudado a esto, su importancia radica en el seguimiento a las recomendaciones realizadas en informes anteriores, de tal forma que, el inspeccionar nuevamente el sitio nos permite evidenciar la situación actual de los elementos señalados con anterioridad, si los aspectos se mantienen o, por el contrario, los avances de la gestión e incluso, situaciones nuevas que pueden aparecer durante la nueva revisión.

¿QUÉ ENCONTRAMOS?

Como parte del estudio realizado en el CEAAM Huetar Caribe, se identificaron debilidades asociadas a las actividades de control interno relacionadas con el cuarto de TI, una constante y frecuente activación del sistema de alarma contra incendios que genera múltiples ingresos de personal no calificado a la sala de telecomunicaciones de este centro el cual es un área de acceso restringido y deficiencias acerca del funcionamiento del sistema de grabación y monitoreo de videovigilancia.

De los aspectos encontrados y señalados anteriormente, se identificaron deficiencias asociadas al cumplimiento de los plazos establecidos para la ejecución de las recomendaciones, así como debilidades del funcionamiento, operación y control interno, de tal manera que se establecieron 3 hallazgos, 3 conclusiones y 2 recomendaciones.

¿QUÉ SIGUE?

La Unidad de Servicios Generales y Transportes debe establecer acciones que les permita atender a las recomendaciones planteadas en el presente informe con el fin de subsanar las debilidades señaladas y con esto contribuir a la protección de los activos del INAMU, también, a las actividades asociadas con el control interno y funcionamiento de los sistemas y mecanismos de protección.

La Unidad de Informática se encargará de atender a las recomendaciones que se efectúan en este estudio referentes a las políticas y lineamientos de control del acceso físico a las áreas restringidas de Tecnologías de la Información, así como, las acciones necesarias para la atención de recomendaciones anteriores en torno a los sistemas de seguridad y protección con el fin de ayudar y contribuir al INAMU en el buen funcionamiento de las aplicaciones y con esto el logro de los diferentes objetivos institucionales y el control interno.

2 INTRODUCCIÓN

El presente estudio de auditoría se realizó en cumplimiento del Plan de Trabajo de la Auditoría Interna para el periodo 2025[1], el objetivo consistió en validar las condiciones de administración, seguridad física y protección del cuarto de TI[2], también, la funcionalidad, parametrización y operación del sistema de grabación o videovigilancia del CEAAM Huetar Caribe.

2.1 ORIGEN DEL ESTUDIO

El estudio se realizó de conformidad con el artículo 20 de la Ley 7801 de Creación del Instituto Nacional de la Mujer[3], el artículo 21 y el 22 de la Ley 8292, Ley General de Control Interno[4], las Normas de Control Interno para el Sector Público[5], Política para la Gestión Operativa de Tecnologías de Información, Marco de Referencia Internacional COBIT 2019, la norma ISO 27001 de Seguridad de la Información: Técnicas de Seguridad- Sistemas de Gestión de la Seguridad de la Información-Requisitos (INTE/ISO/IEC 27001:2014) y la norma ISO 27002 de Seguridad de la Información: Tecnología de la información. Técnicas de seguridad. Código de buenas prácticas para controles de seguridad de la información (INTE/ISO/IEC 27002:2016).

2.2 OBJETIVO DEL ESTUDIO

Validar las condiciones de administración, seguridad física y protección del cuarto de TI, también, la funcionalidad, parametrización y operación del sistema de grabación o videovigilancia del CEAAM Huetar Caribe.

Para la consecución del objetivo general del estudio fueron necesarios los siguientes objetivos específicos de auditoría:

[1] Acuerdo por la Junta Directiva del INAMU, Acuerdo No. 04, Acta No. 41-2024 de fecha 18 de noviembre de 2024.
[2] Comúnmente se refiere a una sala de equipos tecnológicos, telecomunicaciones o de infraestructura informática.
[3] Ley del 29 de abril de 1998, publicada en La Gaceta No. 94 del 18 de mayo de 1998.
[4] Ley del 30 de julio de 2002, publicada en La Gaceta No. 169 del 04 de setiembre de 2002.
[5] Norma del 26 de enero de 2009 Publicada en La Gaceta No. 26 del 6 de febrero de 2009.

- Realizar una inspección física de las condiciones del cuarto de TI del CEAAM Huetar Caribe.

- Validar la información incluida en las bitácoras de acceso al cuarto de TI del CEAAM Huetar Caribe.

- Revisar el funcionamiento y operación del sistema de videovigilancia instalado en la computadora de la oficial de seguridad del CEAAM Huetar Caribe.

- Hacer un recorrido por las instalaciones del CEAAM Huetar Caribe validando las ubicaciones de las cámaras de seguridad y sus condiciones.

- Entrevistar a la encargada del CEAAM Huetar Caribe aplicando una serie de preguntas sobre el cuarto de TI y el sistema de videovigilancia obteniendo información adicional de la administración, operación y aspectos encontrados durante la inspección de ambos.

2.3 ALCANCE DEL ESTUDIO

El estudio es de carácter especial y comprendió la evaluación de la gestión administrativa y de control interno mediante la verificación del correcto funcionamiento y de las condiciones de seguridad física y operativas, como resultado de la inspección realizada al cuarto de TI y al sistema de videovigilancia (CCTV) del CEAAM Huetar Caribe, en busca de la protección de la información, seguridad y protección de estos activos tecnológicos.

2.4 METODOLOGÍA APLICADA

De acuerdo con los criterios anteriormente indicados, la Auditoría Interna realizó una inspección física del cuarto de TI, validó el funcionamiento y operación del sistema de videovigilancia del CEAM Huetar Caribe, analizó información documentada de la Unidad de Informática y verificó los procedimientos ejecutados en relación con los

lineamientos de seguridad física de los activos de tecnología del INAMU y las buenas prácticas internacionales en esta materia.

Las acciones anteriores fueron llevadas a cabo mediante distintas pruebas de cumplimiento y de control, también, se realizó una reunión de forma presencial con la jefatura de este Centro la Sra. Carol Monge Torres aplicando consultas específicas, en complemento, se obtuvo información a través de preguntas directas al personal de planta o en sitio, y finalmente, se realizó el análisis de los datos con la ayuda de la aplicación de varios instrumentos como entrevistas, cuestionarios, inspección de equipos y ubicaciones, entre otros.

2.5 LIMITANTES DEL ESTUDIO

Al momento de realizar la revisión in situ del sistema de videovigilancia no se tuvo acceso a poder realizar la validación y comprobación de su funcionamiento y/o parametrización debido a múltiples errores que presentó el equipo desde donde se opera el mismo, situación que se pone en evidencia más adelante en este informe.

2.6 COMUNICACIÓN PRELIMINAR DE LOS RESULTADOS DE LA AUDITORÍA INTERNA.

En cumplimiento de la norma 2.10 “Comunicación de los resultados” de las “Normas para el ejercicio de la auditoría interna en el Sector Público” y, de conformidad con la norma 205 del “Manual de normas generales de auditoría para el Sector Público”, que establecen que “Las instancias correspondientes deben ser informadas, verbalmente y por escrito, sobre los principales resultados, las conclusiones y las disposiciones o recomendaciones producto de la auditoría que se lleve a cabo…” y que “El auditor debe efectuar una conferencia final con la Administración de la entidad u órgano auditado, antes de emitir la respectiva comunicación por escrito”.

La comunicación de los resultados obtenidos se realizó el 24 de julio de 2025 en forma virtual, mediante la plataforma institucional Teams, y se contó con la participación las personas funcionarias que se detallan a continuación:

- Zaida Barboza Hernández, directora ai, Dirección Administrativa Financiera.
- Adina Castro García, coordinadora, Departamento de Violencia de Género.
- Abdenago Lopez Chacón, coordinador, Departamento de Servicios Generales y Transportes.
- Ingrid Trejos Marín, jefatura, Unidad de Informática.
- Cristian Valverde Loaiza, profesional especialista, Dirección Administrativa Financiera.
- Randall Umaña Villalobos, auditor interno, Auditoría Interna.
- David Sobalbarro Rodríguez, profesional ejecutivo, Auditoría Interna.

En dicha sesión de trabajo se consideraron las observaciones expuestas por parte de los presentes en función de las conclusiones y recomendaciones expuestas.

2.7 IMPLANTACIÓN DE LAS RECOMENDACIONES DE LA AUDITORÍA INTERNA

En la misma Ley 8292 el Artículo 36. Informes dirigidos a los titulares subordinados, establece lo siguiente:

> *Artículo 36.* ***Informes dirigidos a los titulares subordinados****. Cuando los informes de auditoría contengan recomendaciones dirigidas a los titulares subordinados, se procederá de la siguiente manera:*
>
> *a) El titular subordinado, en un plazo improrrogable de diez días hábiles contados a partir de la fecha de recibido el informe, ordenará la implantación de las recomendaciones. Si discrepa de ellas, en el transcurso de dicho plazo elevará el informe de auditoría al jerarca, con copia a la auditoría interna, expondrá por escrito las razones por las cuales objeta las recomendaciones del informe y propondrá soluciones alternas para los hallazgos detectados.*
>
> *b) Con vista de lo anterior, el jerarca deberá resolver, en el plazo de veinte días hábiles contados a partir de la fecha de recibo de la documentación remitida por el titular subordinado; además, deberá ordenar la implantación*

de recomendaciones de la auditoría interna, las soluciones alternas propuestas por el titular subordinado o las de su propia iniciativa, debidamente fundamentadas. Dentro de los primeros diez días de ese lapso, el auditor interno podrá apersonarse, de oficio, ante el jerarca, para pronunciarse sobre las objeciones o soluciones alternas propuestas. Las soluciones que el jerarca ordene implantar y que sean distintas de las propuestas por la auditoría interna, estarán sujetas, en lo conducente, a lo dispuesto en los artículos siguientes.

c) *El acto en firme será dado a conocer a la auditoría interna y al titular subordinado correspondiente, para el trámite que proceda.*

En relación con lo anterior, la normativa promulgada por la Contraloría General de la República señala que el esquema de implementación de recomendaciones debe contener los planes y proyectos para las acciones correctivas que debe de incorporar, además, la definición de un plazo de referencia para el cumplimiento de la recomendación. En este sentido, el artículo 12 de la citada Ley 8292 establece, respecto a los deberes del jerarca y de los titulares subordinados en el sistema de control interno, lo siguiente:

"Artículo 12. —*Deberes del jerarca y de los titulares subordinados en el sistema de control interno. En materia de control interno, al jerarca y los titulares subordinados les corresponderá cumplir, entre otros, los siguientes deberes:*

a) *Velar por el adecuado desarrollo de la actividad del ente o del órgano a su cargo.*

b) Tomar de inmediato las medidas correctivas, ante cualquier evidencia de desviaciones o irregularidades. (El texto en negrita no forma parte del texto original).

c) Analizar e implantar, de inmediato, las observaciones, recomendaciones y disposiciones formuladas por la auditoría interna, la Contraloría General de la República, la auditoría externa y las demás instituciones de control y fiscalización que correspondan. (El texto en negrita no forma parte del texto original).

d) Asegurarse de que los sistemas de control interno cumplan al menos con las características definidas en el artículo 7 de esta Ley.

e) Presentar un informe de fin de gestión y realizar la entrega formal del ente o el órgano a su sucesor, de acuerdo con las directrices emitidas por la Contraloría General de la República y por los entes y órganos competentes de la administración activa."

Por su parte, las "Normas para el ejercicio de la auditoría interna en el Sector Público" señalan en la norma 2.11 lo siguiente:

"El auditor interno debe establecer, mantener y velar porque se aplique un proceso de seguimiento de las recomendaciones, observaciones y demás resultados derivados de los servicios de la auditoría interna, para asegurarse de que las acciones establecidas por las instancias competentes se hayan implementado eficazmente y dentro de los plazos definidos por la administración. Ese proceso también debe contemplar los resultados conocidos por la auditoría interna, de estudios de auditores externos, la Contraloría General de la República y demás instituciones de control y fiscalización que correspondan". (…)

2.8 RIESGOS DE AUDITORÍA

La Auditoría Interna debido a la naturaleza de la labor que realiza se ve expuesta a los siguientes riegos:

Riesgo Inherente.

Es la susceptibilidad del saldo de una cuenta o clase de transacciones a una representación errónea que pudiera ser de importancia relativa, individualmente o cuando se agrega con representaciones erróneas en otras cuentas o clases, asumiendo que no hubo controles internos relacionados.

Riesgo de Control.

El riesgo de control es el riesgo de que una representación errónea, que pudiera ser de importancia relativa individualmente o en conjunto con otras, no sea prevenida o detectada y corregida oportunamente por los sistemas de contabilidad y de control interno.

Riesgo de Detección.

Este tipo de riesgo está directamente relacionado con los procedimientos de auditoría por lo que se trata de la posibilidad que existe en todo tipo de estudio, de no detectar la existencia de errores en el proceso realizado.

2.9 EQUIPO DE TRABAJO A CARGO DEL ESTUDIO

El trabajo de campo, la aplicación de los procedimientos de auditoría y la redacción del informe final de estudio estuvo a cargo de la Profesional Ejecutivo de Auditoría Interna, David Sobalbarro Rodríguez, y la revisión por parte de Randall Umaña Villalobos, Auditor Interno.

2.10 GENERALIDADES DEL ESTUDIO

El presente informe de estudio se ejecutó con el fin de validar las condiciones del cuarto de TI y la funcionalidad del sistema de videovigilancia del CEAAM Huetar Caribe, producto de los proyectos de la Auditoría Interna y como parte de sus funciones orgánicas, entre las cuales están el establecer revisiones, velar por el seguimiento y cumplimiento de las políticas institucionales, validar el correcto funcionamiento de las actividades de Control Interno, entre otras.

Adicionalmente, este estudio se realizó en complemento de otro estudio relacionado la revisión de la caja auxiliar y del fondo de personas usuarias de este Centro, para lo cual se realizó una visita presencial y en adición a esto, la inspección mencionada en el párrafo anterior.

Es fundamental que este estudio coadyuve a la Administración Activa a gestionar de forma oportuna las conclusiones y recomendaciones que se han emitido en este informe producto de este análisis y poder contribuir con la toma de decisiones de relevancia e impacto Institucional.

3 RESULTADOS DE LA AUDITORÍA.

El presente informe muestra los resultados del proyecto de auditoría realizado al proceso de revisión del **CEAAM Huetar Caribe**. El estudio se centró en la inspección del cuarto de TI y las condiciones de éste, también, en la revisión del sistema de videovigilancia utilizado en este Centro.

3.1 INSPECCIÓN DEL CUARTO DE TI

En el marco de la revisión técnica y operativa realizada por la Auditoría Interna al CEAAM Huetar Caribe, se evaluaron las condiciones actuales del cuarto de TI (***Ver conclusión 01, 02, además, recomendación 01 y 02***), con el propósito de verificar y validar temas de acceso, seguridad y protección de los activos tecnológicos que este alberga, para asegurar que estos aspectos y cualquier otro detalle que pudiera observarse en la revisión, responden correctamente a las necesidades y objetivos institucionales.

Esta evaluación permitió identificar debilidades de seguridad física y protección de los activos necesarias de subsanar, ya que así lo dicta la normativa interna y las buenas prácticas internacionales acerca de la gestión de estos procesos.

A continuación, se detalla los hallazgos identificados que evidencian las debilidades anteriormente mencionadas, que pueden comprometer la continuidad, seguridad y protección de los activos institucionales.

3.1.1 HALLAZGO 1: ACCESSO IRRESTRICTO AL CUARTO DE TI. (*Ver conclusión 01 y recomendación 01*)

Nivel de exposición de riesgo vinculado al hallazgo

Crítico	Alto	Medio	Bajo	Informativo
				

CONDICIÓN:

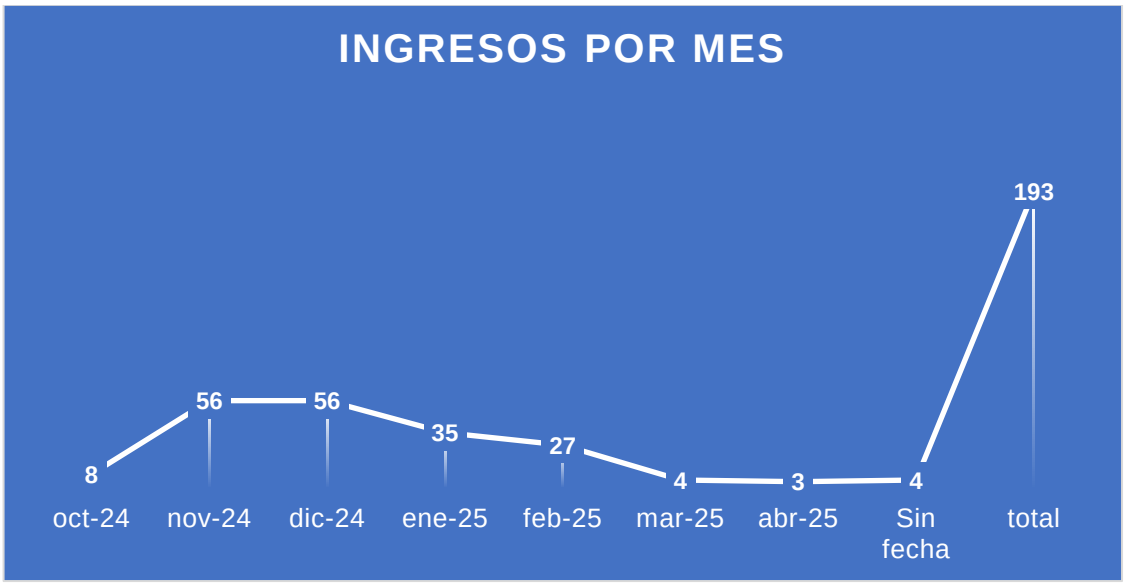
Durante la inspección realizada por la Auditoría Interna, se puede observar en la bitácora de acceso al cuarto de TI una gran cantidad de ingresos a este sitio restringido, el cual se cataloga así por la criticidad, importancia, valor y tipo de infraestructura de los activos que ahí se encuentran, siendo estos solamente algunos factores importantes por los que estos cuartos son de acceso regulado, ya que los bienes y servicios que se generan ahí, son vitales para la continuidad de las operaciones del Instituto y que su manipulación o gestión requiere de cuidado y conocimiento técnico especializado para no comprometer la operación u otro aspecto.

Siendo así que, se elabora un análisis de los datos incluidos en la bitácora mencionada durante los últimos 6 meses anteriores a la visita, con exactitud, se toman los registros desde el 30 de octubre de 2024 al 30 de abril de 2025 fecha en la que se hizo la visita.

Obteniendo de esta información los siguientes detalles:

- **Cantidad de ingresos por mes:** A continuación, se presenta el **Gráfico 1** donde se muestra que durante los últimos 6 meses anteriores a la visita se ingresó al cuarto de TI 193 veces según bitácora, siendo noviembre y diciembre de 2024 los meses con más accesos a esta sala, de la totalidad, hubo 4 registros de ingresos sin fecha.

Gráfico 1. Ingresos al cuarto de TI del CEAAM Huetar Caribe en los últimos 6 meses.



Fuente: Elaborado por la Auditoría Interna, con datos de la bitácora de ingresos al cuarto de TI.

- **Motivo de ingresos por mes:** Se diseña y se presenta a continuación, la **Tabla 1**, la cual recolecta los datos con todos los motivos de ingreso al cuarto de TI y los agrupa por mes, logrando plasmar en la misma que la actividad que se realiza con mayor regularidad y frecuencia es la acción de apagar o desactivar la alarma, en donde los meses con más ingresos son noviembre y diciembre 2024, con 56 accesos cada uno, le siguen los meses de enero y febrero 2025 con 34 y 25 ingresos, todos los anteriores para desactivación de alarma respectivamente.

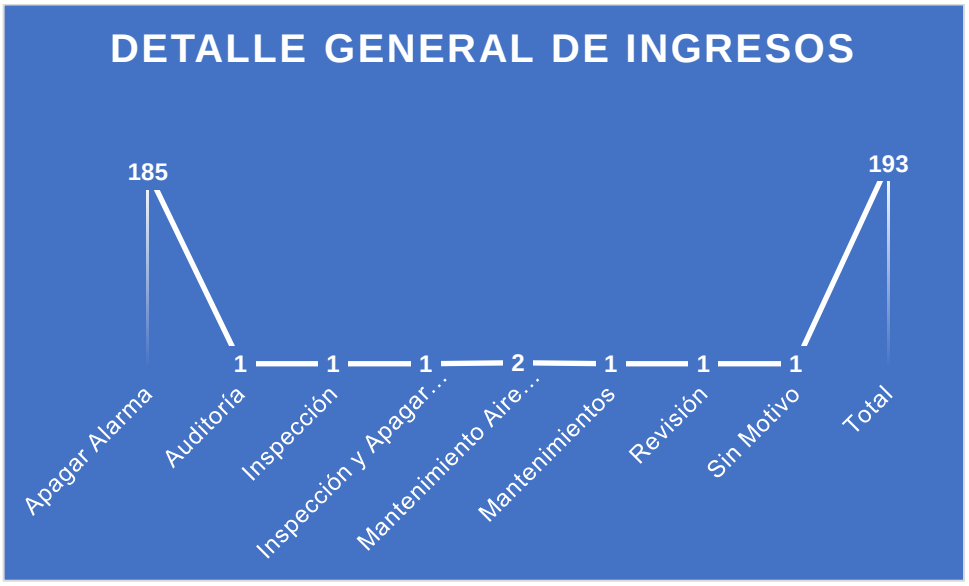
Tabla 1. Motivos de ingreso al cuarto de TI del CEAAM Huetar Caribe por mes.

Motivo de Ingreso		
Mes	**Motivo**	**Cantidad**
oct-24	Apagar Alarma	6
	Mantenimiento Aire	2
nov-24	Apagar Alarma	56
dic-24	Apagar Alarma	56
ene-25	Apagar Alarma	34
	Inspección y Apagar Alarma	1
feb-25	Apagar Alarma	25
	Inspección	1
	Revisión	1
mar-25	Apagar Alarma	4
abr-25	Mantenimientos	1
	Apagar Alarma	1
	Auditoría	1
Sin fecha	Apagar Alarma	3
	Sin Motivo	1
	Total	**193**

Fuente: Elaborado por la Auditoría Interna, con datos de la bitácora de ingresos al cuarto de TI.

- **Detalle general de ingresos al cuarto de TI:** Se muestra el **Gráfico 2** con datos generales y agrupados por el motivo de ingreso a la sala de servidores durante los últimos 6 meses, donde se puede analizar que del total de 193 ingresos que hubo en ese periodo, solamente la actividad de apagar la alarma suma un total de 185 ingresos a esta sala.

Gráfico 2. Detalle general de ingresos al cuarto de TI del CEAAM Huetar Caribe, últimos 6 meses.



Fuente: Elaborado por la Auditoría Interna, con datos de la bitácora de ingresos al cuarto de TI.

Con la información recolectada y los datos analizados anteriormente, se puede dejar en evidencia que la actividad de **"apagar la alarma"** en el CEAAM Huetar Caribe representa un 95,85% de todos los ingresos al cuarto de TI en los últimos 6 meses, mientras que, las demás razones de acceso representan en su mayoría menos del 1%, siendo lo anterior una situación que preocupa por los criterios inicialmente expuestos en este hallazgo, sumado a que no es normal que un sistema de alarmas tenga el comportamiento que anteriormente se refleja en las bitácoras.

Es sumamente importante mencionar que durante la visita a las instalaciones del CEAAM Huetar Caribe, se pudo vivir cómo se dio la activación de la alarma en dos ocasiones durante esta estancia, también, se pueden consultar la evidencia de las bitácoras en la sección 6 llamada anexos de este informe.

CRITERIO

Dentro de las actividades de control interno que se deben garantizar en las instituciones no sólo está la protección de los bienes, también está el buen

funcionamiento de los sistemas, controles y/o la operación en sí. En el **Capítulo II** de la **Ley 8292 de Control Interno** se aclara que es el control interno institucional:

> **Artículo 8º—Concepto de sistema de control interno.** Para efectos de esta Ley, se entenderá por sistema de control interno la serie de acciones ejecutadas por la administración activa, diseñadas para proporcionar seguridad en la consecución de los siguientes objetivos:
> a) Proteger y conservar el patrimonio público contra cualquier pérdida, despilfarro, uso indebido, irregularidad o acto ilegal.
> b) Exigir confiabilidad y oportunidad de la información.
> c) Garantizar eficiencia y eficacia de las operaciones.
> d) Cumplir con el ordenamiento jurídico y técnico.

Las **Normas de Control Interno para el Sector Público** también indican la importancia que proporcionan los sistemas de control al brindar información veraz y oportuna sobre su funcionamiento y evaluar que esta información sea correcta y de calidad:

> **4.4 Exigencia de confiabilidad y oportunidad de la información**
>
> El jerarca y los titulares subordinados, según sus competencias, deben diseñar, adoptar, evaluar y perfeccionar las actividades de control pertinentes a fin de asegurar razonablemente que se recopile, procese, mantenga y custodie información de calidad sobre el funcionamiento del SCI y sobre el desempeño institucional…

En el INAMU también se incorporan lineamientos sobre Control Interno en materia de Tecnología mediante la Unidad de Informática, donde la política de TI llamada **Políticas para la Gestión Operativa de Tecnologías de Información** en el apartado **19. Políticas para seguimiento y evaluación del control interno en TI.**, el cual tiene como propósito brindar seguridad con una operación eficiente y efectiva en el tema de cumplimiento y regulación, acá se indica:

19.3.2. Monitoreo y evaluación del control interno

(…)

La Unidad de Informática será la responsable de revisar y analizar cualquier informe emitido por terceros sobre la situación de la Unidad, y definirá y desarrollará las acciones correspondientes, que serán elevadas a la Comisión de Tecnologías de Información.

La Jefatura de la Unidad de Informática será la responsable de evaluar la necesidad de implementar acciones correctivas para asegurar que se corrija cualquier incumplimiento y/o situación negativa detectada por las revisiones periódicas.

Las buenas prácticas internacionales como el marco de referencia **COBIT 2019** incorpora un objetivo de gestión llamado **MEA02** dedicado a la gestión del sistema de control interno, dentro de sus prácticas de gestión incorpora una específica para que las instituciones validen el buen y óptimo funcionamiento de sus sistemas, procesos y mecanismos de control, está práctica indica:

MEA02.02 Revisar la eficacia de los controles del proceso de negocio. Revisar la operación de los controles, incluidas la supervisión y la evidencia de las pruebas, para asegurar que los controles de los procesos de negocio operan eficazmente. Incluir actividades para mantener evidencia de la operación efectiva de los controles mediante mecanismos, como pruebas periódicas, supervisión continua, evaluaciones independientes, centros de mando y control, y centros de operaciones de red. Estas evidencias garantizan al negocio que los controles cumplen con los requisitos relacionados con las responsabilidades de negocio, regulatorias y sociales.

En la misma línea de las buenas prácticas internacionales, la norma de seguridad de la información **ISO 27001** cuenta con el domino **A.12 Seguridad de las operaciones** el cual incluye el apartado **A.12.6 Gestión de vulnerabilidades técnicas** que busca que las empresas validen sus debilidades de índole técnico en las operaciones, con el fin de analizarlas, evaluarlas para finalmente resolverlas, como se puede leer a continuación:

A.12.6 Gestión de vulnerabilidades técnicas
Objetivo: Prevenir la explotación de vulnerabilidades técnicas.

A.12.6.1 Gestión de vulnerabilidades técnicas

Control: Se debe obtener información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información usados, se debe evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para abordar el riesgo asociado.

CAUSA:

El origen de este hallazgo relacionado con los múltiples accesos al cuarto de TI se debe a dos factores principales, el primero de ellos es que el panel de la alarma contra incendios lo ubicaron en el cuarto de TI y la desactivación de la misma sólo se puede realizar desde este panel principal, no existe otra estación de desactivación de alarma en ninguna otra ubicación del CEAAM Huetar Caribe, generando que cada vez que la misma comienza a sonar, se deba desplazar personal del CEAAM para apagarla a esta sala y de esa manera ejecutar el procedimiento de apagado.

Al mismo tiempo, el segundo motivo de los números ingresos a este cuarto de TI, el cual es muy importante, es la frecuencia con la que se activan las alarmas de incendio de este Centro, las cuales se experimentaron durante la visita, además, que al revisar los registros en las bitácoras se puede ver que estos accesos por activación de la alarma son bastantes.

Sobre estos eventos de activación de alarmas e indagando con las personas colaboradoras, en las conversaciones ellos expresan y consideran las mismas como anormales, incluso indicaron, que no son producto de una activación manual por alguna de las personas usuarias o de los niños que también están en las instalaciones de este albergue.

EFECTO:

Existe impacto en las condiciones específicas en las que deben operar los activos tecnológicos albergados en esta sala, ya que, al estar ingresando frecuentemente a

esta sala, se generan muchos cambios de las condiciones medioambientales del cuarto de TI, esta sala se caracteriza por tener que conservar una temperatura y condiciones de ambiente definidas las cuales son óptimas para la conservación de los recursos o equipos informáticos y el buen funcionamiento de estos.

También, existen riesgos de daño de equipo por un accidente o indebida manipulación de los activos de forma involuntaria por parte del personal que ingresa a desactivar la alarma, lo que puede afectar o interrumpir la continuidad de las operaciones del servicio que se brinda en el CEAAM Huetar Caribe, especialmente por el ingreso de personal no técnico a estas áreas. ***(Ver conclusión 01 y recomendación 01)***

3.1.2 HALLAZGO 2: OMISIÓN DE PROCEDIMIENTOS EN CONTROLES DE ACCESO. (*Ver conclusión 02 y recomendación 02*)

Nivel de exposición de riesgo vinculado al hallazgo

Crítico	Alto	Medio	Bajo	Informativo
				

CONDICIÓN:

Durante la visita y recorrido de las instalaciones en este Centro cuando se ejecutaban las respectivas revisiones, la alarma se activó en dos ocasiones, lo que generó que personal del CEAAM se dirigiera al cuarto de TI para hacer la desactivación de la misma, cuando sucedió la segunda activación, se observó a la auxiliar en turno Aurora Chavarría Acevedo afueras del cuarto de TI realizando el apagado de la alarma, quien contaba con llaves para acceder a esta sala, se conversó con ella, indicó que esto sucede frecuentemente y sin motivo aparente.

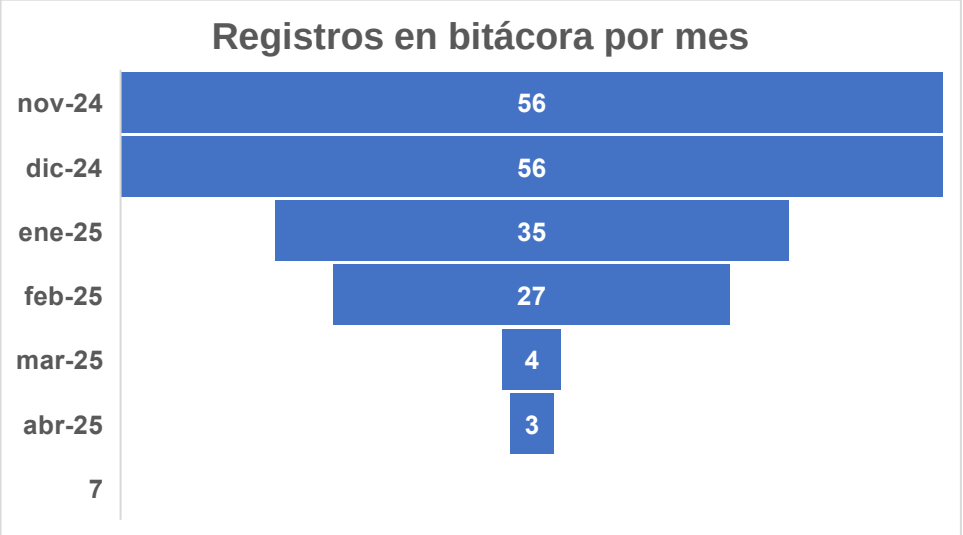
Mientras se hacía un recorrido por el edificio o instalaciones, y se revisaba la ubicación de las cámaras de seguridad, se logró observar al personal de limpieza en esta sala

de TI, realizando las respectivas labores de aseo de este cuarto, la puesta estaba abierta y la persona estaba limpiando en ese momento en el interior del recinto.

Luego de ver los dos ingresos anteriormente descritos, y se accedió nuevamente al recinto para validar que en la bitácora estuviera el registro de estos dos últimos accesos, pero no fue así, lo que demuestra que el personal no siempre hace el registro de ingreso en la bitácora, lo anterior anudado al siguiente análisis, se puede intuir que existen muchos ingresos no registrados, controlados ni supervisados.

En el **Gráfico 3** se puede observar la cantidad de registros en bitácora por mes, al comparar estos con el testimonio del personal del CEAAM donde indican que las activaciones de alarma suceden frecuentemente, la observación de los eventos en sitio, la validación de la omisión en el registro de la bitácora durante la visita y el comportamiento de los meses anteriores, se puede constatar que no se ha seguido el procedimiento y medida de control relacionada con anotar cada ingreso al Cuarto de TI en el respectivo formulario físico.

Gráfico 3. Cantidad de registros en bitácora por mes al cuarto de TI del CEAAM Huetar Caribe.



Fuente: Elaborado por la Auditoría Interna, con datos de la bitácora de ingresos al cuarto de TI.

Visualizando el gráfico anterior se puede evidenciar el movimiento de los últimos meses, donde en marzo y abril de 2025 solamente hubo 4 y 3 ingresos respectivamente, sin embargo, noviembre y diciembre de 2024, enero y febrero de 2025 presentan una gran cantidad registros de ingresos a esta sala.

CRITERIO:

Las políticas y los procedimientos de la organización juegan un papel relevante en el cumplimiento del control interno. En el **Capítulo III: La Administración Activa** en la **Sección I: Deberes del jerarca y los titulares subordinados** de la **Ley 8292 de Control Interno** se indica:

> **Artículo 15. Actividades de control.** Respecto de las actividades de control, serán deberes del jerarca y de los titulares subordinados, entre otros, los siguientes:
>
> a) Documentar, mantener actualizados y divulgar internamente, las políticas, las normas y los procedimientos de control que garanticen el cumplimiento del sistema de control interno institucional y la prevención de todo aspecto que conlleve a desviar los objetivos y las metas trazados por la institución en el desempeño de sus funciones.
> b) Documentar, mantener actualizados y divulgar internamente tanto las políticas como los procedimientos que definan claramente, entre otros asuntos, los siguientes:
>
> i. La autoridad y responsabilidad de los funcionarios encargados de autorizar y aprobar las operaciones de la institución.
> ii. La protección y conservación de todos los activos institucionales.
> iii. El diseño y uso de documentos y registros que coadyuven en la anotación adecuada de las transacciones y los hechos significativos que se realicen en la institución. Los documentos y registros deberán ser administrados y mantenidos apropiadamente.
> iv. La conciliación periódica de registros, para verificar su exactitud y determinar y enmendar errores u omisiones que puedan haberse cometido.
> v. Los controles generales comunes a todos los sistemas de información computarizados y los controles de aplicación específicos para el procesamiento de datos con software de aplicación.

Cuando se habla de activos críticos, especialmente esos que se encuentran en lugares de acceso restringido por temas de seguridad por el alto valor e importancia de estos, las actividades de prevención, registro de eventos y control se vuelven una necesidad institucional, las **Normas de Control Interno para el Sector Público** así lo indican:

> **4.3.3 Regulaciones y dispositivos de seguridad**
>
> El jerarca y los titulares subordinados, según sus competencias, deben disponer y vigilar la aplicación de las regulaciones y los dispositivos de seguridad que se estimen pertinentes según la naturaleza de los activos y la relevancia de los riesgos asociados, para garantizar su rendimiento óptimo y su protección contra pérdida, deterioro o uso irregular...

La Unidad Informática incorpora controles de seguridad de acceso físico mediante las **Políticas para la Gestión Operativa de Tecnologías de Información,** la cual contiene lineamientos específicos llamados **Políticas para la seguridad física de las instalaciones de tecnologías de información** que buscan regular los ingresos y los factores medioambientales de los activos tecnológicos, y aunque estos lineamientos refieren en el texto al Centro de Datos del INAMU, son los mismos principios que deben operar en cualquier cuarto de TI de acceso restringido por la naturaleza de sus activos, este lineamiento indica:

> **16.3.1. Acceso físico**
>
> El acceso físico de las personas colaboradoras al Centro de Datos del INAMU, en donde se ubican los equipos principales de la plataforma tecnológica de La Institución, será exclusivo para las personas autorizadas.
>
> Las personas autorizadas para ingresar al Centro de Datos del INAMU son las relacionadas con la Unidad de Informática, terceros autorizados y/o contratados por dicha Unidad para realizar cualquier servicio relacionado a los equipos principales y personal de limpieza de forma controlada.
>
> La Unidad de Informática deberá llevar una bitácora de registro de accesos de personal ajeno a dicha Unidad al Centro de Datos del INAMU…

El marco de referencia internacional **COBIT 2019** provee una práctica de gestión **DSS05.05** que se llama **Gestionar el acceso físico a los activos de I&T** la cual orienta a las instituciones a incorporar procesos para ingreso a los sitios de la organización de acuerdo con el negocio y las necesidades. Esta buena práctica indica que el ingreso físico a estas ubicaciones debe contar con justificación, autorización, registro y supervisión. Dentro de sus activades de gestión recomienda:

> 1. Registrar y monitorizar todos los puntos de entrada a las instalaciones de TI. Registrar a todos los visitantes al sitio, incluidos contratistas y proveedores.
> (…)
> 4. Restringir y monitorizar el acceso a instalaciones sensibles de TI, mediante el establecimiento de restricciones al perímetro, como vallas, paredes y dispositivos de seguridad en puertas interiores y exteriores.
> 5. Gestionar solicitudes para permitir el acceso debidamente autorizado a las instalaciones de cómputo.
> 6. Garantizar que los perfiles de acceso permanezcan actualizados. Basar el acceso a las instalaciones de TI (sala de servidores, edificios, áreas o zonas) en el cargo y las responsabilidades.
> 7. Realizar formación sobre concienciación de la seguridad de la información física de forma regular.

Finalmente, en la misma línea de las buenas prácticas internacionales, el marco de referencia internacional **ISO 27001** de Seguridad de la Información, en el dominio de seguridad **A.11 Seguridad física y ambiental** en el apartado **A.11.1 Áreas seguras** tiene como objetivo la prevención de los ingresos no autorizados a lugares donde se procesen los datos e información de la institución, así como la protección de la misma, en dicho apartado se recomienda establecer dentro de las políticas empresariales y procedimientos institucionales, los siguientes controles:

> **A.11.1.1 Perímetro de seguridad física**
> **Control:** Se deben definir y usar perímetros de seguridad para proteger áreas que contienen información sensible o crítica y recursos de procesamiento de la información.

A.11.1.2 Controles de entrada física
Control: Las áreas seguras deben ser protegidas por medio de controles de entrada apropiados para asegurarse de que el acceso sea permitido solamente a personal autorizado.

A.11.1.3 Aseguramiento de oficinas, salas e instalaciones
Control: La seguridad física para oficinas, salas e instalaciones debe ser diseñada y aplicada.

A.11.1.4 Protección contra amenazas externas y ambientales
Control: La protección física contra desastres naturales, ataques maliciosos o accidentes debe ser diseñada y aplicada.

CAUSA:

El principal motivo que da origen a la omisión de registros en la bitácora es la ausencia de concientización acerca de los procedimientos institucionales y los lineamientos de la organización entorno a los registros en bitácora, estas reglas deben de ser comunicadas e incluso regularmente enviar recordatorios sobre las medidas de control, así como ejercer supervisión y control sobre la ejecución de estas para asegurarse de su cumplimiento.

También, su causa puede referirse a la debilidad o ausencia de regulación específica y clara en las políticas institucionales, es decir, instrucciones directas que sean precisas sobre las obligaciones del personal que ingresa a las áreas restringidas, y que estas sean emitidas o escritas de forma que se pueda entender con exactitud el lineamiento, sin dejar lugar a dudas o la posibilidad de omitir los controles.

EFECTO:

Existe un gran impacto en las actividades de supervisión del control interno que establece estas medidas para poder tener visibilidad de la gestión que se realiza en las áreas restringidas, de tal manera que la información obtenida a través de estos controles no es exacta y puede inducir a errores en la toma de decisiones. También afecta la tarea de análisis de la información, ya que, si estos controles son analizados

para dar seguimiento y por la razón anteriormente explicada, es probable que los datos resultantes de ese análisis estén sesgados.

Lo anteriormente mencionado puede generar que en caso de investigar algún evento o revisar cierta información relacionada con la gestión ejecutada en estas áreas restringidas mediante la bitácora de ingresos, no se cuente con la misma, afectando uno de los pilares de la seguridad de la información que es la disponibilidad, o también, que esta no sea correcta, afectando un segundo pilar de la seguridad de la información que es la integridad de los datos, lo cual se traduce nuevamente en una afectación directa a la información empresarial que se requiere controlar y que a la postre sirve para la toma de decisiones anteriormente mencionada ***(Ver conclusión 02, recomendación 02, oportunidad de mejora 01 y 02)***.

3.2 SEGUIMIENTO DE RECOMENDACIÓN Y REVISIÓN DEL SISTEMA DE GRABACIÓN O VIDEOVIGILANCIA (CCTV)

En el marco de la revisión técnica y operativa realizada por la Auditoría Interna al CEAAM Huetar Caribe, se hizo un seguimiento de recomendaciones de informes anteriores relacionados con el sistema de cámaras y también, se revisó el funcionamiento del sistema de videovigilancia (CCTV) **(*Ver conclusión 03*)**, con el propósito de verificar su integridad, disponibilidad y capacidad para responder adecuadamente a las necesidades de seguridad institucional.

Esta evaluación permitió identificar debilidades técnicas, operativas y de mantenimiento que podrían comprometer la eficacia de los sistemas. A continuación, se detalla el hallazgo identificado el cual evidencia una serie de deficiencias críticas que podrían comprometer la continuidad operativa, la seguridad física y la protección de los activos institucionales.

3.2.1 HALLAZGO 3: SEGUIMIENTO DE RECOMENDACIÓN A HALLAZGO RELACIONADO CON LAS DE DEFICIENCIAS EN EL FUNCIONAMIENTO DEL SISTEMA DE MONITOREO DEL CEAAM HUETAR CARIBE. (*Ver conclusión 03*)

Nivel de exposición de riesgo vinculado al hallazgo

Crítico	Alto	Medio	Bajo	Informativo
				

CONDICIÓN:

La Auditoría Interna mediante el estudio **INAMU-JD-AI-In-007-2024 Informe de Control Interno relacionado con la gestión administrativa afín a los registros de ingresos y egresos de personas usuarias y sus expedientes, además de la planificación de actividades en el CEAAM-HC entre otros, para el periodo 2023**, solicitó a la Presidencia del INAMU mediante una recomendación con fecha de emisión del 14/6/2024 y con una plazo máximo para cumplir la recomendación de 29/7/2024, el solicitarle a la Comisión de Tecnologías de la Información, un diagnóstico general (obsolescencia, software, registro y almacenamiento de datos, riesgos de seguridad y ciberseguridad) de los sistemas de monitoreo instalados en todas y cada una de las oficinas del INAMU, pero la misma se encuentra pendiente con plazo vencido.

Adicional al seguimiento de recomendación anteriormente mencionado, y con el fin de validar si las deficiencias relacionadas al sistema de videovigilancia expuestas en dicho informe se mantienen igual o han variado, la Auditoría Interna realiza la inspección del Sistema de Video de Vigilancia (CCTV) del CEAAM Huetar Caribe.

Una vez en sitio se ubica dicho sistema el cual se encuentra instalado, es monitoreado y operado desde una computadora ubicada en la caseta del guarda de seguridad de este centro **(*Ver imagen en anexo 10*)**.

Mediante indagación, la persona oficial de seguridad, así como la Jefatura del Centro de atención la Sra. Monge Torres no tienen claridad si el sistema de cámaras esté almacenando o grabando los videos, por lo cual consideran que el sistema de vigilancia por video funciona únicamente en tiempo real. Así mismo, argumentan desconocer el procedimiento para solicitar un video en caso de requerirlo, incluso a la persona que deben recurrir para hacer solicitud de un video de este sistema de grabación.

Sobre el video en tiempo real, cuando se está monitoreando la cámara del portón principal, que es la que está por defecto en la computadora del oficial de seguridad, el video presenta un retraso en la imagen, aproximadamente de un minuto, es decir, los eventos se visualizan retrasados.

En la revisión se comprueba que, con solo mover el ratón o “mouse” del equipo de cómputo, la aplicación no responde, se bloquea por varios minutos y aparecen múltiples ventanas de error de sistema, la pantalla muestra solamente 24 errores, pero existen más **(*Ver imagen en anexo 11)***.

Al seleccionar uno de los errores para poder visualizar el mensaje que muestra, se debe esperar a que el sistema reaccione ya que se paraliza por un buen tiempo y luego muestra el detalle con un texto en idioma inglés que dice “The service is already started” que en español significa “El servicio ya se ha iniciado” **(Ver imágenes en anexo 12 y 13)**.

Al querer visualizar el video de las otras cámaras existentes en el CEAAM Huetar Caribe desde la aplicación, el sistema dura bastante en realizar la petición y no muestra los videos en tiempo real de las cámaras de diferentes localidades, solamente pantallas negras en cada uno de los 4 cuadrantes de visualización **(Ver imagen en anexo 14)**.

Después de algún tiempo uno de los cuadrantes lo que hace es mostrar un error en idioma inglés que dice “Playback failed. No record file found.”, que en idioma español significa “Error en la reproducción. No se encontró ningún archivo de grabación.” **(Ver imagen en anexo 15 y 16)**.

Finalmente, y sobre la revisión en sitio, existe tanta lentitud y saturación en el procesamiento de órdenes que el sistema en ocasiones trata de mostrar un mensaje o error y se queda congelado en proceso sin mostrar detalle alguno **(Ver imagen en anexo 17)**.

Lo que generó no poder validar ningún otro aspecto adicional del sistema, como parametrización, almacenamiento de video, calidad de imagen, conexión y funcionamiento de todo el circuito, funcionalidades, entre otros. Ya que las órdenes no se procesaban o tardaban mucho tiempo mostrando error, no la petición solicitada, generando más errores en el equipo.

CRITERIO:

Al validar los registros de Auditoría Interna y el seguimiento de recomendaciones se puede constatar que la recomendación indicada anteriormente, producto del estudio **INAMU-JD-AI-In-007-2024 Informe de Control Interno relacionado con la gestión administrativa afín a los registros de ingresos y egresos de personas usuarias y sus expedientes, además de la planificación de actividades en el CEAAM-HC entre otros, para el periodo 2023.,** a la fecha de emisión de este informe se mantiene en un estado de pendiente de cumplir con el plazo otorgado vencido, además es importante mencionar que, durante un estudio nuevo, adicional a lo evidenciado en el informe anterior se logran identificar nuevas debilidades y deficiencias tanto técnicas como de operación.

En el **Capítulo II: El sistema de control interno** de la **Ley 8292 de Control Interno** se incluye un artículo que indica lo siguiente respecto las actividades que conforman el control interno institucional:

> ***Artículo 10.-Responsabilidad por el sistema de control interno.*** *Serán responsabilidad del jerarca y del titular subordinado establecer, mantener,*

perfeccionar y evaluar el sistema de control interno institucional. Asimismo, será responsabilidad de la administración activa realizar las acciones necesarias para garantizar su efectivo funcionamiento.

Al mismo tiempo, la **Ley 8292 de Control Interno** en el **Capítulo III: La Administración Activa** dispone de un artículo que indica lo siguiente sobre los sistemas de información:

> ***Artículo 16.-Sistemas de información****. Deberá contarse con sistemas de información que permitan a la administración activa tener una gestión documental institucional, (…) con el fin de prevenir cualquier desvío en los objetivos trazados. Dicha gestión documental deberá estar estrechamente relacionada con la gestión de la información, en la que deberán contemplarse las bases de datos corporativas y las demás aplicaciones informáticas, las cuales se constituyen en importantes fuentes de la información registrada.*
>
> *En cuanto a la información y comunicación, serán deberes del jerarca y de los titulares subordinados, como responsables del buen funcionamiento del sistema de información, entre otros, los siguientes:*
>
> *[…]*
> *b) Armonizar los sistemas de información con los objetivos institucionales y verificar que sean adecuados para el cuido y manejo eficiente de los recursos públicos.*

Las buenas prácticas internacionales en materia de gestión y gobierno de las tecnologías de la información como el marco de referencia **COBIT 2019** cuenta con un proceso de gestión llamado **BAI (Construir, Adquirir e Implementar)** y su objetivo de gestión **BAI04 – Gestionar la disponibilidad y la capacidad** describe:

> ***BAI04.01 Evaluar la disponibilidad, rendimiento y capacidad actuales, y crear una línea de referencia:*** *Evaluar la disponibilidad, rendimiento y capacidad de los servicios y recursos para asegurar que la capacidad y el rendimiento con un coste justificable están disponibles para apoyar las necesidades y entregables del negocio contra los acuerdos de nivel de servicio (SLA).*

Dentro de las actividades para cumplir con la práctica anterior menciona lo siguiente:

> *[…]*
> *3. Monitorizar el uso real de la capacidad y el rendimiento frente a umbrales definidos y con el soporte, cuando sea necesario, de software automatizado.*
> *4. Evaluar regularmente los niveles actuales de rendimiento para todos los niveles de procesamiento (demanda del negocio, capacidad de servicios y capacidad de recursos).*

La práctica **BAI04.05 Investigar y resolver los problemas de disponibilidad, rendimiento y capacidad** que tiene como propósito abordar los errores mediante la investigación y resolución de los errores identificados sobre la disponibilidad, el rendimiento y la capacidad de los servicios y recursos, incluye dentro de sus actividades las siguientes acciones:

[…]

> *3. Identificar las brechas de rendimiento y capacidad con base en la monitorización del rendimiento actual y estimado. Usar especificaciones conocidas de disponibilidad, continuidad y recuperación para clasificar los recursos y permitir su priorización.*
>
> *4. Definir acciones correctivas (p. ej., cambios en la carga de trabajo, priorizar tareas o añadir recursos cuando se identifiquen problemas de rendimiento y capacidad).*

El objetivo llamado **BAI09 Gestionar los activos** que trata sobre gestionar los activos de TI a través del ciclo de vida, la generación de valor de estos, que operan según su propósito, que brindan confiabilidad y están disponibles, incluye la práctica BAI09.01 Identificar y registrar los activos actuales la cual indica:

> *[…]*
> *3. Comprobar que los activos son adecuados para su propósito (es decir, que se puedan usar).*
>
> *[…]*
> *6. Determinar regularmente si cada activo continúa proporcionando valor. De ser así, estimar la vida útil esperada durante la que proporcionará valor.*

Mientras que la práctica BAI09.02 menciona sobre los activos críticos o que se consideran así, garantizar la capacidad de prestación del servicio. Con esto maximicen su confiabilidad y la disponibilidad que brindan para soportar las necesidades de negocio. Dentro de sus actividades de gestión dice que:

> […]
> *5. Mantener la resiliencia de los activos críticos aplicando un mantenimiento preventivo regular. Monitorizar el rendimiento y, de ser necesario, proporcionar activos alternativos y/o adicionales para minimizar la probabilidad de fallo.*
>
> *6. Establecer un plan de mantenimiento preventivo para todo el hardware considerando un análisis de coste beneficio, las recomendaciones de los proveedores, el riesgo de suspensión del servicio, el personal calificado y otros factores relevantes.*

Finalmente, continuando en la línea de las buenas prácticas internacionales, el marco de referencia de seguridad de la información **ISO**, en la familia de estándares 27000 cuenta con una política llamada **INTE/ISO/IEC 27002:2016**. **Técnicas de Seguridad. Código de Buenas Prácticas para Controles de Seguridad de la Información**, el cual incluye un Dominio de Seguridad de la Información llamado **Seguridad Física y Ambiental** donde incorpora el objetivo de control Equipo y controles de seguridad que dicen:

> ***11.2.2 Servicios de soporte***
>
> ***Control.***
> *El equipo debería ser protegido contra fallas de energía u otras interrupciones causadas por fallas en los servicios de soporte.*
>
> ***Guía de implementación.***
> *Los servicios de soporte (por ejemplo, la electricidad, las telecomunicaciones, el agua potable, el gas, el alcantarillado, la ventilación y el aire acondicionado) deberían:*
>
> *[…]*
> *b) ser evaluados regularmente en su capacidad para cumplir con el crecimiento del negocio y las interacciones con otros servicios de soporte;*

c) ser inspeccionados y probados regularmente para asegurar su buen funcionamiento;

CAUSA:

La principal causa es la falta de mantenimiento, revisión y monitoreo de la funcionalidad, rendimiento y capacidad del sistema de videovigilancia CCTV, así como del equipo informático que lo soporta para garantizar su óptima condición y operación, sumado a lo anterior, debe existir una comunicación clara y precisa, que retroalimente a las partes interesadas en todas las direcciones, sobre los errores identificados y las necesidades del negocio para el cumplimiento de los objetivos en temas de protección, seguridad, operación, entre otros, ya que el identificar un error no es suficiente para solucionarlo, debe existir acciones y solicitudes o requerimientos para para la prevención, detección y corrección de incidentes.

Es importante mencionar que las causas de los errores de rendimiento de las aplicaciones pueden ser amplias, y se requieren las acciones descritas anteriormente para poder dar con un diagnóstico certero pero sobre todo con su solución, acá se mencionan algunas causas que pueden generar un bajo rendimiento, lentitud e incidentes en los aplicativos: saturación del almacenamiento disponible, capacidad de almacenamiento muy baja, actualizaciones pendientes en el equipo o la aplicación, poca memoria RAM, errores de hardware o software, entre otros.

EFECTO:

Impacto importante en la funcionalidad del sistema de videovigilancia afectando su correcto funcionamiento y utilidad, limitando y/o bloqueando la posibilidad de su utilización en diversas tareas para las que está diseñada la aplicación.

Extrema lentitud del sistema y la computadora, imposibilitando las diferentes validaciones como la versión, actualización, parametrización, configuración, calidad de imagen o programación de la grabación.

Se satura tanto la aplicación que no es posible validar aspectos de conexión como la alimentación de electricidad de las cámaras, que todas enciendan, graben y

reproduzcan sin problemas, la señal de todas para detectar daños o desconexiones, la integridad de las grabaciones, que se almacenen correctamente y sean accesibles, el espacio disponible o puntos ciegos.
No es posible moverse entre cámaras para visualizar otras áreas, lo que provoca que a nivel de monitor sólo está la imagen de la cámara del portón principal, ya que el sistema con sólo mover el ratón se pega y hace imposible que se reciba alguna orden, lo que compromete, limita y atrasa el trabajo de seguridad y puede provocar un problema mayor. (***Ver conclusión 03).***

4 CONCLUSIONES.

Las conclusiones que se detallan a continuación surgen de la inspección en sitio del cuarto de TI y la revisión del sistema de grabación o videovigilancia del CEAAM Huetar Caribe, también, del análisis de la información recopilada durante el proceso de auditoría, los cuales permitieron identificar aspectos relevantes sobre aspectos del control interno, funcionamiento, procedimientos o la gestión operativa, entre otros.

4.1 CONCLUSIÓN

Las áreas de acceso restringido deben mantenerse en esa línea, evitando el ingreso no autorizado a los equipos que ahí dentro se manejan, salvo pocas situaciones como es la limpieza, siendo esta, una actividad que de igual manera debe ser regulada para evitar riesgos o posibles incidentes por la importancia de los activos o la información que resguarda en este tipo de lugares, además, es necesario que las salas que deben de mantener condiciones específicas de humedad y/o temperatura se logren conservar respetando dichos parámetros la mayor parte del tiempo, evitar las situaciones que puedan alterar el medio ambiente salvo las actividades necesarias, pero erradicar y prevenir aquellas que puedan controlarse para cumplir con las especificaciones necesarias para el buen funcionamiento y protección de los activos. además, es necesario proporcionar la mayor cantidad de barreras de seguridad física y ambiental, así como los procedimientos respectivos que garanticen el cumplimiento de la protección de estas salas y activos que se albergan en estos sitios. ***(Ver recomendación 01)***

4.2 CONCLUSIÓN

El establecimiento de procedimientos formales que sean comunicados y seguidos por todo el personal de la institución garantiza al INAMU cumplir con los objetivos estratégicos, pero sobre todo con la protección de los activos, aplicando las medidas de seguridad robustas que dictan las buenas prácticas internacionales en materia de seguridad de la información, se vuelve más valioso asegurar que estas se cumplan mediante lineamientos claros y específicos, así como diferentes controles de comprobación, en procura de proteger y otorgar seguridad de la información considerada valiosa o crítica en la continuidad de las operaciones del INAMU, lo anterior garantiza que se respeten los pilares fundamentales de la información, específicamente el de la disponibilidad e integridad, necesarios para la correcta toma de decisiones y actividades de control interno. ***(Ver recomendación 02)***

4.3 CONCLUSIÓN

Los sistemas de video vigilancia son elementos esenciales para la seguridad física y también de la información, son mecanismos importantes que ayudan en las actividades de prevención, detección y hasta corrección de errores en incidentes que puedan materializarse durante las operaciones y fuera de ésta, también son medidas de control eficaces en temas de protección, es necesario que estos sistemas se encuentren funcionando a la perfección en tiempo y forma para garantizar la oportuna acción ante posibles eventos, permitiendo a las personas encargadas de monitorear las actividades mediante estos servicios el poder validar de manera íntegra y con una alta disponibilidad todas las funcionalidades que permiten estos dispositivos de seguridad.

---

5 RECOMENDACIONES

Como resultado de los hallazgos identificados durante la auditoría realizada en el CEAAM Huetar Caribe, se presentan las siguientes recomendaciones orientadas a fortalecer los mecanismos y procedimientos de control, así como la ejecución en las operaciones del Centro.

Estas sugerencias buscan corregir las deficiencias detectadas, brindar protección de los recursos tecnológicos y seguridad tanto física como de los activos que procesan información, ayudan en la toma de decisiones y forman parte del sistema de control interno de este centro, así asegurar el cumplimiento de la normativa vigente, contribuyendo a una gestión más eficaz en beneficio de la institución, de las personas usuarias y sus familias también.

5.1 RECOMENDACIÓN

AL DEPARTAMENTO DE SERVICIOS GENERALES Y TRANSPORTES

En un plazo no mayor a (30) días, realizar un diagnóstico del sistema de prevención de incendio del CEAAM Huetar Caribe, con el objetivo de determinar la causa raíz que provoca su constante activación, y eliminar razonablemente las inconsistencias determinadas en el presente informe.

Esta recomendación se emite a raíz de la inspección realizada de esta sala, el análisis de la bitácora de acceso al cuarto de TI la cual se adjunta en la sección de anexos, la observación de los eventos y procedimientos ejecutados y finalmente, producto de las indagaciones realizadas con el personal del CEAAM Huetar Caribe.

El objetivo de esta recomendación es regular y minimizar los accesos a esta área restringida, evitar daños de los equipos o afectación a la continuidad de las operaciones, la alteración de las condiciones ambientales del cuarto y mitigar el riesgo por manipulación indebida de los dispositivos.

5.2 RECOMENDACIÓN

A LA UNIDAD DE INFORMATICA:

En un plazo no mayor a treinta (30) días y en línea con la "Política para la gestión operativa de Tecnologías de Información del INAMU", establecer las acciones en apego al numeral 16.- punto 16.3.1- Acceso Físico, para que los controles establecidos para el "Centro de Datos" se implementen en las Unidades Regionales, Albergues y cualquier otro lugar de trabajo fuera del SIGMA, con el propósito de que los ingresos que se realicen a los "Cuartos de TI" se den en estricto apego a la política supra citada.

Esta recomendación se genera con la inspección de la bitácora del cuarto de TI, anudado al análisis y comparación de los datos ahí registrados, además, con la información obtenida de la visita mediante la observación e indagación, finalmente surge también de la revisión de las políticas de la Unidad de Informática, donde el lineamiento acerca del acceso físico no está claro.

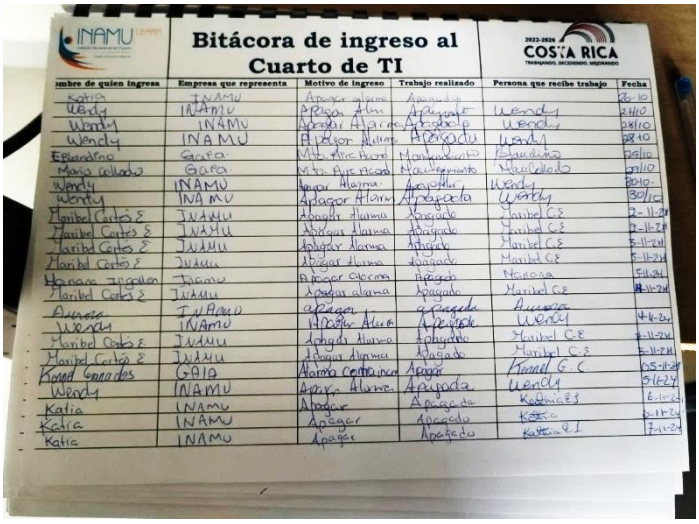
El objetivo de esta recomendación es definir claramente mediante las políticas de la Unidad de informática la regulación y obligaciones específicas a la hora de ingresar áreas sensibles de TI, que esto quede documentado de manera explícita y que sea comunicado a las personas responsables de supervisar estas acciones.

6 ANEXOS

A continuación, se presentan los documentos de respaldo que completan información contenida en el presente informe. Estos anexos contienen evidencia relacionada con los procedimientos realizados durante el proceso de auditoría.

6.1 ANEXO

Figura 1. Bitácora de Ingreso al Cuarto de TI del 26/10/2024 al 07/11/2024.



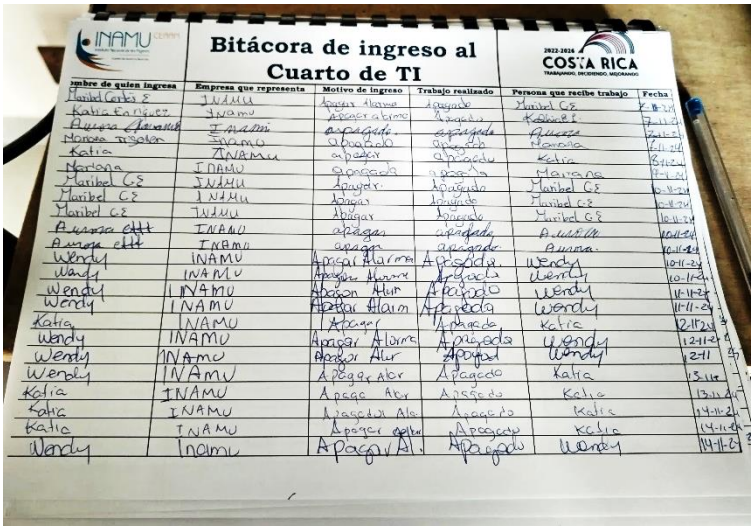
Bitácora de ingreso al Cuarto de TI

Nombre de quien ingresa	Empresa que representa	Motivo de ingreso	Trabajo realizado	Persona que recibe trabajo	Fecha
Katia	INAMU	Apagar alarma	Apagado		26-10
Wendy	INAMU	Apagar Alarma	Apagado	Wendy	24/10
Wendy	INAMU	Apagar Alarma	Apagado	Wendy	28/10
Wendy	INAMU	Apagar Alarma	Apagado	Wendy	28/10
Eduardo	Gaia	Mtto. Aire Acond.	Mantenimiento	Eduardo	29/10
Mario Collado	Gaia	Mtto. Aire Acond.	Mantenimiento	Mario Collado	29/10
Wendy	INAMU	Apagar Alarma	Apagado	Wendy	30-10
Wendy	INAMU	Apagar Alarma	Apagado	Wendy	30/10
Maribel Cortés E	INAMU	Apagar Alarma	Apagado	Maribel C E	2-11-24
Maribel Cortés E	INAMU	Apagar Alarma	Apagado	Maribel C E	2-11-24
Maribel Cortés E	INAMU	Apagar Alarma	Apagado	Maribel C E	5-11-24
Maribel Cortés E	INAMU	Apagar Alarma	Apagado	Maribel C E	5-11-24
Maribel Cortés E	INAMU	Apagar alarma	Apagado	Maribel C E	5-11-24
Aurora	INAMU	Apagar	Apagado	Aurora	4-11-24
Wendy	INAMU	Apagar Alarma	Apagado	Wendy	4-11-24
Maribel Cortés E	INAMU	Apagar Alarma	Apagado	Maribel C E	5-11-24
Maribel Cortés E	INAMU	Apagar Alarma	Apagado	Maribel C E	5-11-24
Ronald Granados	GAIA	Alarma Contra Incen	Apagar	Ronald G C	05-11-24
Wendy	INAMU	Apagar Alarma	Apagado	Wendy	5-11-24
Katia	INAMU	Apagar	Apagado	Katia G S	6-11-24
Katia	INAMU	Apagar	Apagado	Katia	6-11-24
Katia	INAMU	Apagar	Apagado	Katia G S	7-11-24

Fuente: Fotografía tomada en el CEAAM Huetar Caribe por la Auditoría Interna el 30-04-2025.

6.2 ANEXO

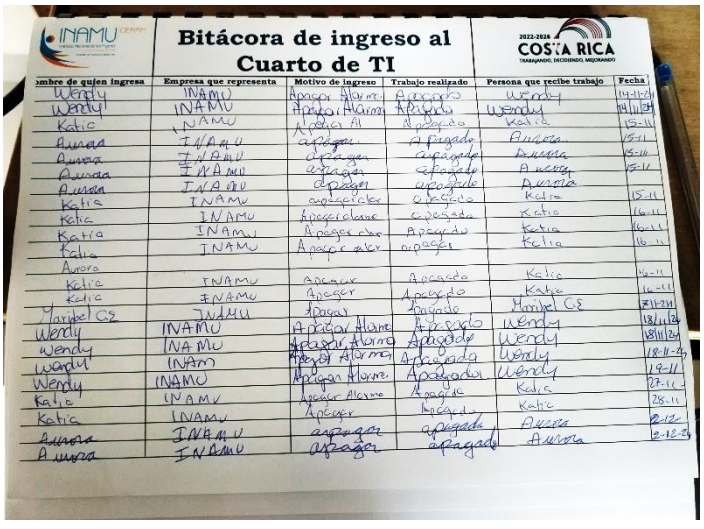
Figura 2. Bitácora de Ingreso al Cuarto de TI del 7/11/2024 al 14/11/2024.



Fuente: Fotografía tomada en el CEAAM Huetar Caribe por la Auditoría Interna el 30-04-2025.

6.3 ANEXO

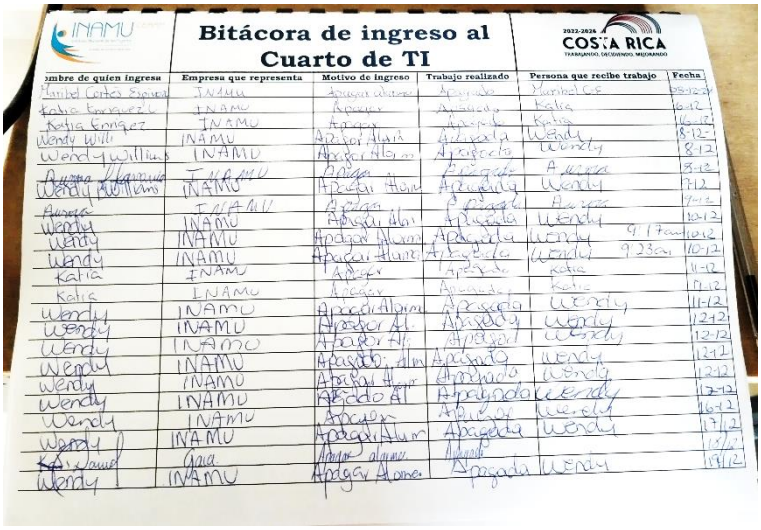
Figura 3. Bitácora de Ingreso al Cuarto de TI del 14/11/2024 al 02/12/2024.



Fuente: Fotografía tomada en el CEAAM Huetar Caribe por la Auditoría Interna el 30-04-2025.

6.4 ANEXO

Figura 4. Bitácora de Ingreso al Cuarto de TI del 05/12/2024 al 19/12/2024.



Fuente: Fotografía tomada en el CEAAM Huetar Caribe por la Auditoría Interna el 30-04-2025.

6.5 ANEXO

Figura 5. Bitácora de Ingreso al Cuarto de TI del 20/12/2024 al 30/12/2024.

Fuente: Fotografía tomada en el CEAAM Huetar Caribe por la Auditoría Interna el 30-04-2025.

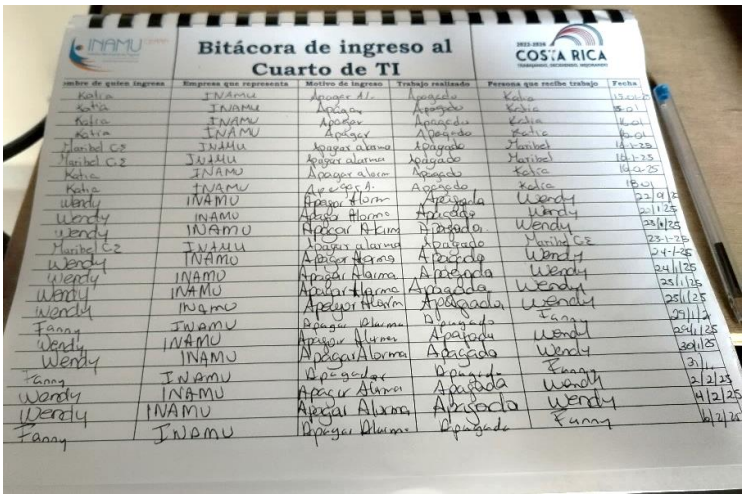
6.6 ANEXO

Figura 6. Bitácora de Ingreso al Cuarto de TI del 30/12/2024 al 15/01/2025.

Fuente: Fotografía tomada en el CEAAM Huetar Caribe por la Auditoría Interna el 30-04-2025.

6.7 ANEXO

Figura 7. Bitácora de Ingreso al Cuarto de TI del 15/01/2025 al 06/02/2025.



Fuente: Fotografía tomada en el CEAAM Huetar Caribe por la Auditoría Interna el 30-04-2025.

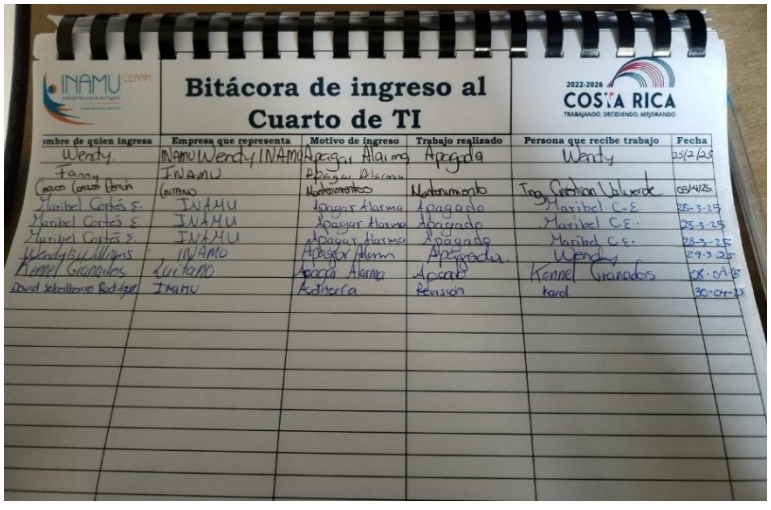
6.8 ANEXO

Figura 8. Bitácora de Ingreso al Cuarto de TI del 07/02/2025 al 25/02/2025.

Fuente: Fotografía tomada en el CEAAM Huetar Caribe por la Auditoría Interna el 30-04-2025.

6.9 ANEXO

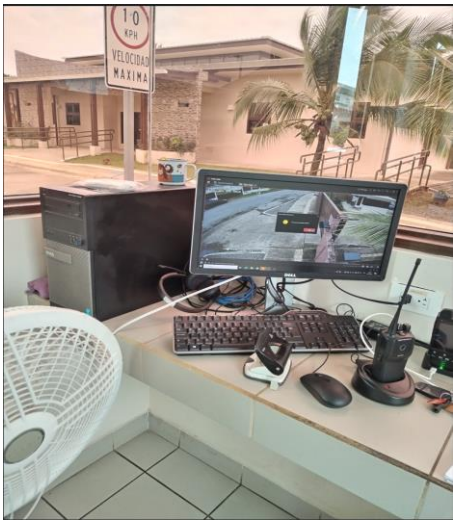
Figura 9. Bitácora de Ingreso al Cuarto de TI del 25/02/2025 al 30/04/2025.



Fuente: Fotografía tomada en el CEAAM Huetar Caribe por la Auditoría Interna el 30-04-2025.

6.10 ANEXO

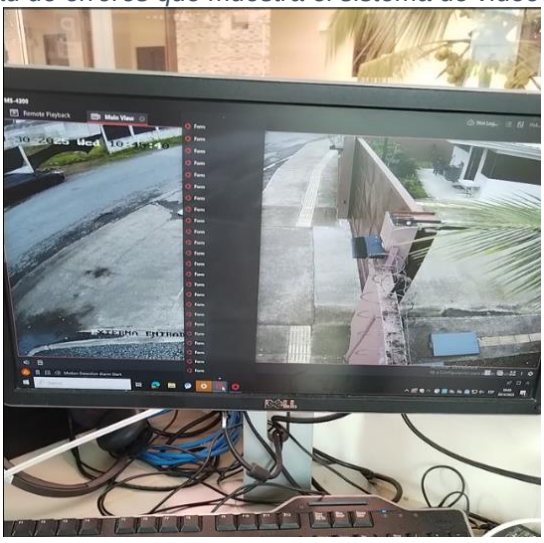
Figura 10. Computadora para monitoreo del sistema de videovigilancia (CCTV).



Fuente: Fotografía tomada en el CEAAM Huetar Caribe, Limón, Costa Rica el 30 de abril de 2025.

6.11 ANEXO

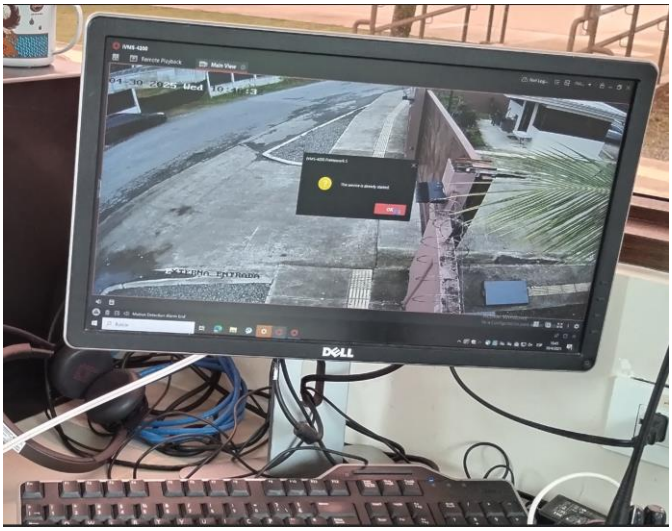
Figura 11. Cantidad de errores que muestra el sistema de videovigilancia (CCTV).



Fuente: Fotografía tomada en el CEAAM Huetar Caribe, Limón, Costa Rica el 30 de abril de 2025.

6.12 ANEXO

Figura 12. Mensaje de error que muestra el sistema de videovigilancia (CCTV).



Fuente: Fotografía tomada en el CEAAM Huetar Caribe, Limón, Costa Rica el 30 de abril de 2025.

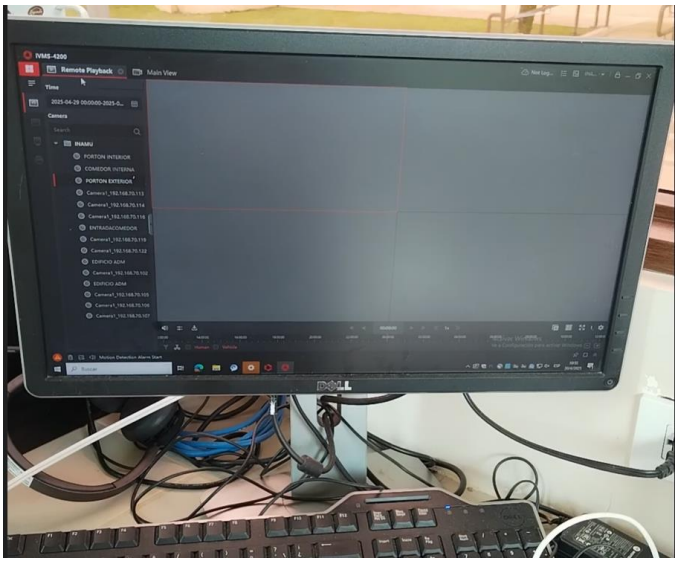
6.13 ANEXO

Figura 13. Acercamiento al mensaje de error del sistema de videovigilancia (CCTV).

Fuente: Fotografía tomada en el CEAAM Huetar Caribe, Limón, Costa Rica el 30 de abril de 2025.

6.14 ANEXO

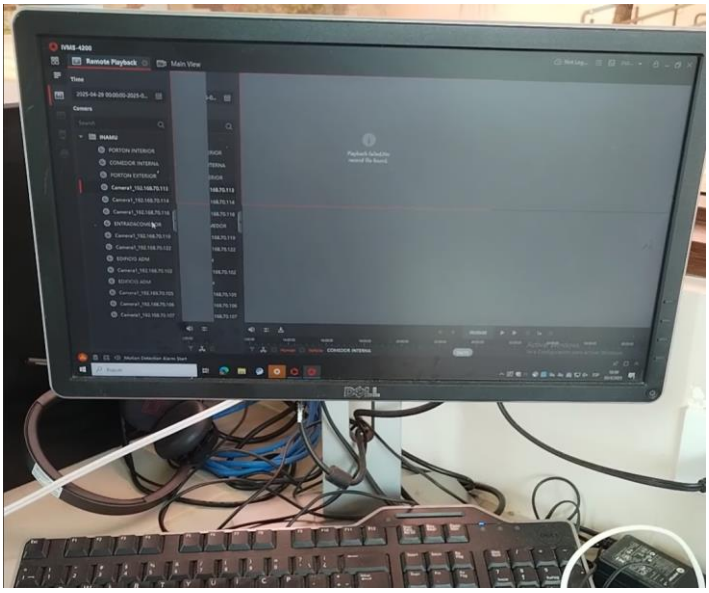
Figura 14. Vista de cámaras (cuatro cuadros) el sistema de videovigilancia (CCTV).



Fuente: Fotografía tomada en el CEAAM Huetar Caribe, Limón, Costa Rica el 30 de abril de 2025.

6.15 ANEXO

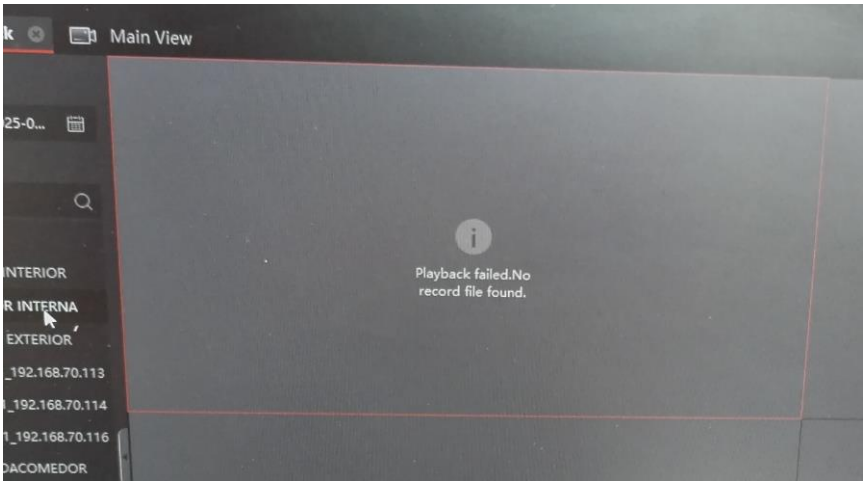
Figura 15. Error de uno de los cuadrantes del sistema de videovigilancia (CCTV).



Fuente: Fotografía tomada en el CEAAM Huetar Caribe, Limón, Costa Rica el 30 de abril de 2025.

6.16 ANEXO

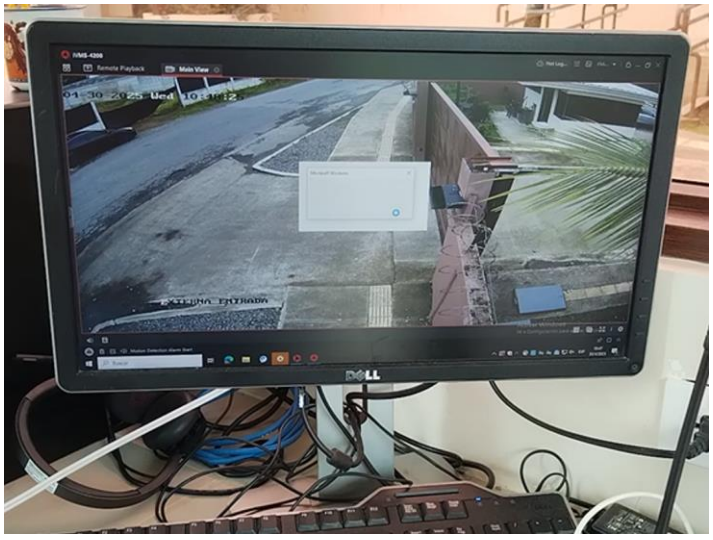
Figura 16. Detalle de error de uno de los cuadrantes del sistema de videovigilancia (CCTV)



Fuente: Fotografía tomada en el CEAAM Huetar Caribe, Limón, Costa Rica el 30 de abril de 2025.

6.17 ANEXO

Figura 17. Saturación en mensajes del sistema de videovigilancia (CCTV).



Fuente: Fotografía tomada en el CEAAM Huetar Caribe, Limón, Costa Rica el 30 de abril de 2025.

Cc. Sra. Yerlin Zuñiga Céspedes, presidenta ejecutiva, Presidencia Ejecutiva
Sra. Kattia Calvo Cruz, jefatura, Despacho de la Presidencia Ejecutiva.
Sra. Alexandra Gómez Ruiz, asesora, Despacho de la Presidencia Ejecutiva.
Sra. Zaida Barboza Hernández, directora a.i., Dirección Administrativa Financiera.
Sra. Adina Castro García, coordinadora, Departamento de Violencia de Género.
Sra. Ingrid Trejos Marín, jefatura, Unidad de Informática.
Sr. Abdenago López Chacón, coordinador, Departamento de Servicios Generales y Transportes.
Sr. Cristian Valverde Loaiza, profesional especialista, Dirección Administrativa Financiera.
Archivo.