CONTROLES DE SEGURIDAD PARA LA PREVENCIÓN DE FUGA DE INFORMACIÓN (DLP) POR PARTE DE USUARIOS INTERNOS EN SISTEMAS HOSPITALARIOS DE LA CCSS EN COSTA RICA

I. Sáenz Córdoba
Escuela de Ciencias Exactas y Naturales, Universidad Estatal a Distancia, isaenzc@uned.ac.cr

ABSTRACT

Information security management in critical hospital infrastructures, such as the Costa Rican Social Security Fund (CCSS), faces unprecedented challenges following the cyberattacks suffered in 2022. This paper analyzes the implementation of Data Loss Prevention (DLP) controls aimed at mitigating risks originating from internal users, who, whether through negligence, the use of "Shadow IT," or a lack of digital culture, represent the primary vector for sensitive data exposure. The study examines the need for a defense-in-depth strategy that integrates compliance with Law No. 8968 on the Protection of the Person Regarding the Processing of Personal Data with technical controls across data in use, in transit, and at rest. Finally, a hybrid model combining Identity and Access Management (IAM), activity monitoring, and administrative controls is proposed, concluding that technology alone is insufficient without a transformation in the organizational security culture.

Keywords: CCSS, DLP, Hospital Security, Insider Threat, Law 8968, Shadow IT, Data Protection, Cybersecurity.

RESUMEN

La gestión de la seguridad de la información en infraestructuras hospitalarias críticas costarricenses, como la de la Caja Costarricense de Seguro Social (CCSS), enfrenta desafíos sin precedentes tras los ciberataques sufridos en 2022. Por lo que este artículo analiza la implementación de controles de prevención de fuga de datos (DLP) orientados a mitigar los riesgos provenientes de usuarios internos; quienes, ya sea por negligencia, uso de Shadow IT o falta de cultura digital, representan el principal vector de exposición de datos sensibles. Además, se examina la necesidad de una estrategia de defensa en profundidad que integre el cumplimiento de la Ley N.º 8968 de Protección de la Persona frente al Tratamiento de sus Datos Personales con controles técnicos en los estados de uso, tránsito y reposo de la información. Finalmente, se propone un modelo híbrido que combina la segmentación de identidades (IAM), el monitoreo de actividad y controles administrativos, y se concluye que la tecnología por sí sola es insuficiente sin una transformación en la cultura organizacional de seguridad.

Palabras clave: CCSS, DLP, seguridad hospitalaria, amenaza interna, Ley 8968, Shadow IT, protección de datos, ciberseguridad.

INTRODUCCIÓN

El uso profesional y ético de las herramientas tecnológicas y sistemas informáticos facilitados por la organización en el entorno hospitalario implica que tanto el usuario directo (médicos, enfermeras, administrativos) como el usuario indirecto (pacientes del sistema de salud público costarricense) representen el mayor vector de riesgo para la fuga de información; no necesariamente por malicia, sino por negligencia o Shadow IT (uso de herramientas no autorizadas para agilizar el trabajo, tales como smartphones, tablets o equipos tecnológicos personales), o bien por hacer uso de redes ajenas facilitadas por la institución.

Estas acciones, si bien es cierto son parte de la cotidianidad del personal médico y administrativo, aunque parezcan bien intencionadas, pueden derivar en la fuga accidental de información sensible, especialmente en sistemas donde convergen datos clínicos, diagnósticos, enfermedades, historiales y resultados médicos altamente sensibles de los pacientes de la CCSS. Por lo cual, surge la importancia de la implementación de controles DLP adaptados al comportamiento interno con los mejores estándares de seguridad informática.

ISSN: 2015-5392

Tras el ciberataque sufrido en Costa Rica en mayo del 2022 al seguro social del país se deduce que la CCSS ha incrementado sus medidas de ciberseguridad y hoy por hoy concentra sus esfuerzos en el control de los usuarios internos, ya que este aspecto resulta clave para reducir el riesgo de fuga de información tanto de colaboradores como de los usuarios de la Caja, sin embargo el crear una cultura de seguridad que combine tecnología y responsabilidad individual para proteger la información crítica de la institución tiene muchos aspectos por mejorar.

En los pasillos hospitalarios, áreas de salud, sucursales y otras oficinas adyacentes, coexisten decenas de colaboradores, desde médicos y enfermeras hasta personal administrativo; quienes, de alguna u otra manera, cuentan con un perfil tecnológico único. Es un entorno donde interactúan diariamente usuarios capaces de gestionar complejos sistemas clínicos con información altamente sensible de pacientes e inclusive otros usuarios del seguro social costarricense que aún enfrentan barreras básicas en la interacción digital, falta de recursos, capacitaciones, problemas en la red y otros factores adversos que permiten el filtrado de los datos.

Esta profunda brecha de habilidades transforma al personal interno en un elemento crítico de la ecuación de riesgo y la falta de conciencia digital sobre las graves consecuencias de una eventual fuga de información involuntaria y desconocimiento de la Ley 8968, Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales.

En perspectiva, la Auditoría Interna de la CCSS indica que aún existen cuentas con asignación excesiva de roles, duplicidad de funciones y perfiles sin descripción, lo que refleja un manejo ineficiente de privilegios dentro de varios de los sistemas institucionales a lo largo y ancho del país [1].

Por su parte, la implementación de controles DLP repercute de manera confrontativa en infraestructuras críticas de la institución que, debido a su antigüedad, representan desafíos significativos vinculados a la infraestructura tecnológica y a la dinámica operativa del personal. Así mismo, impide la adopción de agentes modernos de DLP, por lo que la estrategia debe apoyarse en controles perimetrales de red como medida complementaria para incrementar los niveles de seguridad informática en los nosocomios y algunas áreas de salud.

La resistencia al cambio y la fricción operativa constituyen barreras críticas, exacerbadas por la alta presión y los esquemas de rotación continua (24/7) del personal médico. Estas condiciones laborales propician la adopción de Shadow IT como mecanismo para agilizar procesos; por consiguiente, la implementación de controles de seguridad debe ser gradual, priorizando fases de monitoreo y alerta antes de habilitar bloqueos restrictivos.

Adicionalmente, las limitaciones de conectividad en zonas rurales exigen el despliegue de agentes de endpoint ligeros y autónomos (offline). La inestabilidad de la red en estas áreas fomenta prácticas de alto riesgo, como el uso compartido de cuentas genéricas y el traslado de datos sensibles de pacientes mediante dispositivos de almacenamiento extraíble (USB), lo cual compromete la integridad y confidencialidad de la información.

La Caja Costarricense de Seguro Social (CCSS) presenta una infraestructura tecnológica caracterizada por sistemas críticos obsoletos, equipos con actualizaciones y parches atrasados, así como una carencia de segmentación robusta en sus redes. Además, se evidencian limitaciones en los procesos de continuidad de negocio y una calidad del servicio informático deficiente en determinadas regiones del país; factores que incrementan significativamente la superficie de ataque.

Tras el incidente de ransomware dirigido inicialmente al Ministerio de Hacienda de Costa Rica y, después, a la CCSS, el grupo Hive logró comprometer los sistemas institucionales, cifrar información sensible, paralizar servicios esenciales y generar un impacto de alcance nacional [2]. En respuesta, la CCSS activó planes de contingencia, inició un proceso gradual de restauración de sistemas y fortaleció sus capacidades de ciberseguridad. Este fortalecimiento se vio potenciado por la intervención de los Estados Unidos con un presupuesto inicial de $25 millones y la implementación de políticas públicas orientadas a mejorar la postura de seguridad nacional, aunque con resultados limitados en términos de resiliencia tecnológica y primeros pasos en ciberseguridad [3]

ISSN: 2015-5392

I. CONTEXTO NORMATIVO BASADO EN LA NORMA DE COSTA RICA

La implementación de controles de seguridad orientados a prevenir la fuga de información en los sistemas hospitalarios de la Caja Costarricense de Seguro Social (CCSS) debe fundamentarse en el marco normativo vigente en Costa Rica y en la clasificación institucional de datos críticos. Dicho marco establece los criterios para determinar qué información requiere protección, bajo qué principios regulatorios y con qué responsabilidades legales y operativas. En este contexto, entidades nacionales como la Agencia de Protección de Datos de los Habitantes (PRODHAB), el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), entre otras organizaciones, constituyen referentes normativos y técnicos para el tratamiento de la información personal y la gestión de la seguridad de los datos.

La Ley N.º 8968 constituye el marco normativo fundamental en Costa Rica en materia de privacidad y protección de datos personales. Esta legislación clasifica explícitamente la información clínica, expedientes médicos, diagnósticos y datos biomédicos como datos sensibles; los cuales requieren la implementación de salvaguardas técnicas, administrativas y organizativas de nivel superior, con el fin de limitar su divulgación.

Asimismo, la Ley 8968 se reconoce como un referente pionero en la regulación costarricense sobre el tratamiento y la usabilidad de la información personal. Un principio central de esta normativa es el consentimiento informado, establecido como requisito para el tratamiento o transferencia de datos sensibles, salvo en casos de excepción definidos por la misma ley.

La normativa también estipula que la divulgación indebida o el manejo inadecuado de dichos datos acarrea sanciones administrativas y económicas, aplicables tanto a las instituciones como a los colaboradores responsables. Dicho consentimiento debe ser formalizado mediante la firma y aprobación del usuario final, garantizando así la legitimidad del uso de su información privada [4].

Complementariamente al marco legal principal, la gestión de la información en el sector salud se rige por lineamientos de la PRODHAB que exigen controles reforzados para evitar fugas o accesos no autorizados, dependiente de la mala manipulación de los datos y, en caso de que se demuestre inconsistencias, las sanciones varían según la gravedad de la falta; además, pueden incluir multas basados en salarios bases, eliminación de datos y, en otros casos más estrictos, se podría incluir órdenes administrativas y sanciones más graves que van de 5 a 20 salarios base.

Por otra parte, la normativa interna de la Caja Costarricense de Seguro Social (CCSS), la cual regula estrictamente la seguridad y el control de acceso a sistemas institucionales críticos, como EDUS, ARCA y SICERE [5], [6], procura alinearse con los pilares de la ciberseguridad y, sobre todo, con la confidencialidad obligatoria estipulada en la Ley General de Salud y la Ley de Delitos Informáticos (Ley N.º 9048); la cual sanciona el acceso indebido, la sustracción, alteración o destrucción de información protegida [7], [8].

II. ESTRATEGIA DE CONTROLES TÉCNICOS DE DLP

Para mitigar el riesgo asociado a usuarios internos, ya sea por negligencia, malicia, debilidad o pésimos controles en los sistemas informáticos, es imperativo implementar controles de prevención de pérdida de datos (DLP) que abarquen los tres estados fundamentales de la información. En primer lugar de esta lista, se mencionan por su origen en inglés endpoint (datos en uso), donde las medidas deben centrarse en la restricción de periféricos no autorizados, el control del portapapeles y la implementación de impresión segura con autenticación. En segundo lugar, se menciona que la protección de datos en movimiento requiere la inspección profunda de tráfico cifrado (SSL/TLS), que hace posible el bloqueo de almacenamiento en nubes personales externas y el filtrado de correo saliente basado en contenido sensible.

Por último, para salvaguardar los datos en reposo, es crucial el despliegue de herramientas de descubrimiento y clasificación automatizada en servidores de archivos, junto con el monitoreo de actividad en bases de datos (DAM) para alertar sobre consultas masivas o comportamientos anómalos de usuarios con altos privilegios [9]. Para poner en perspectiva lo indicado anteriormente, se resumen los tres estados del dato (Figura 1).

ISSN: 2015-5392

Figura 1. Los tres estados del dato: en reposo, en tránsito y en uso [10].

III. CONTROLES DE IDENTIDAD Y ACCESO (IAM)

Es importante mencionar que, en el mayor de los casos, la incidencia de fugas de información suele correlacionarse directamente con la asignación de privilegios excesivos a los usuarios de las plataformas tecnológicas; lo que hace ineludible adoptar prácticas de Principio de Mínimo Privilegio (PoLP) y Control de Acceso Basado en Roles (RBAC). El Principio del Mínimo Privilegio (PoLP) es el mecanismo de seguridad que establece que cualquier entidad (como un usuario, aplicación o sistema) debe operar con la menor cantidad de permisos necesarios para realizar su tarea específica; es decir, el médico del EBAIS u hospital deberá únicamente visualizar la información del área de salud competente a la que están adscritos los pacientes, o bien a nivel general, si se trata del ámbito hospitalario. Por otra parte, el Control de Acceso Basado en Roles (RBAC) implementa un mecanismo o modelo de autorización en el que únicamente se deben agrupar los permisos en roles definidos (por ejemplo, “Lector,” “Escritor,” “Administrador”), es decir, si es un médico administrativo o un operativo, claramente debería contar con los roles de usuarios según sus responsabilidades laborales y no “mezclar” en qué se debería tener acceso y qué no.

En entornos hospitalarios complejos como el de la CCSS, esta segmentación dentro de plataformas como el EDUS debe ser granular, garantizando que el personal administrativo (mayormente departamentos de registros de estadística) acceda únicamente a datos logísticos y de agenda; mientras que perfiles clínicos, como farmacéuticos, visualicen exclusivamente prescripciones sin acceso a diagnósticos psiquiátricos o quirúrgicos detallados. Para blindar estas restricciones lógicas, es necesario habilitar mecanismos de Autenticación Multifactor (MFA) en todos los módulos críticos de la red interna y mitigar las vulnerabilidades de seguridad física mediante políticas de gestión de sesiones que fuercen el cierre automático (time-out) tras periodos breves de inactividad, impidiendo así el acceso oportunista a terminales desatendidas en áreas de alta rotación como emergencias, farmacia, laboratorio y rayos x; además, que pueda darse la posibilidad de que un tercero tenga acceso a información clasificada sin el permiso adecuado de manera intencional o accidental [9], [11].

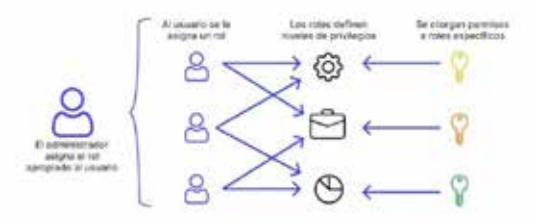

Figura 2. El control de acceso basado en roles [12].

IV. CONTROLES ADMINISTRATIVOS Y PROCESOS INTERNOS

La eficacia de la infraestructura tecnológica de seguridad se ve severamente comprometida, si no se acompaña de una cultura organizacional robusta, dado que el factor humano persiste como el vector de ataque más crítico en la cadena de eliminación de seguridad cibernética Cyber Kill Chain en inglés. Por consiguiente, es necesario establecer controles administrativos más robustos de los existentes que trasciendan la tecnología, comenzando por la formalización de Acuerdos de Confidencialidad (NDA) vinculantes que integren cláusulas explícitas sobre las responsabilidades derivadas de la Ley N.º 8968, aplicables no solo al personal de planta regular, sino extendiéndose obligatoriamente a practicantes o pasantes, proveedores y contratistas externos que, de alguna u otra forma, cuentan con acceso a las plataformas institucionales por la naturaleza de sus puestos de trabajo.

Simultáneamente, para mitigar la susceptibilidad ante ataques de ingeniería social, se deben implementar programas de concienciación continuos y simulacros de phishing que permitan evaluar y corregir el comportamiento de los usuarios frente a amenazas dirigidas. Finalmente, en el plano físico, la seguridad de la información debe reforzarse mediante una política estricta de “escritorio limpio”, erradicando prácticas de riesgo como la exposición de contraseñas en notas adhesivas o el abandono de expedientes clínicos en áreas de libre tránsito como las estaciones de enfermería, previniendo así la fuga de datos por observación directa o descuido que, lamentablemente, por experiencia del autor como paciente en distintos servicios de salud, se observan siempre en las impresoras direcciones IP y, en el peor de los casos, se observan pequeños papeles en blanco con anotaciones a mano como usuarios o claves a los distintos sistemas y a la red [13], [14].

ISSN: 2015-5392

Figura 3. Tomada de Facebook CCSS con posibles usuarios y claves debajo del monitor [15].

V. REFLEXIÓN FINAL

Se concluye que una estrategia efectiva de prevención de fuga de información (Data Loss Prevention, DLP) no puede limitarse exclusivamente a la implementación de controles tecnológicos. Por el contrario, requiere un enfoque integral que incorpore auditorías de seguridad física y programas de concienciación dirigidos a los usuarios. Este enfoque holístico permite mitigar el factor humano, identificado como el vector de riesgo más crítico y recurrente en la protección de datos sensibles. En este sentido, los usuarios finales constituyen el eslabón más vulnerable de la cadena de seguridad, dado que, de manera consciente o inconsciente, pueden facilitar el acceso no autorizado a plataformas tecnológicas que gestionan información altamente sensible. [16]

REFERENCIAS

A. Segura, «CCSS gasta más de $1.4 millones en licencias de sistema informático que no se utilizan», CR Hoy. Accedido: 21 de enero de 2026. [En línea]. Disponible en: https://crhoy.com/nacionales/ccss-gasta-mas-de-1-4-millones-en-licencias-de-sistema-informatico-que-no-se-utilizan/

Caja Costarricense de Seguro Social (CCSS), «Oficio de Advertencia sobre la exposición reciente a ataques cibernéticos a la CCSS.» Costa Rica, 31 de mayo de 2022. [En línea]. Disponible en: https://www.ccss.sa.cr/arc/auditoria/informes/AD-ATIC-067-2022.pdf

T. Gómez, «EE.UU. y Costa Rica firman plan de $25 millones para ciberseguridad», El Observador CR. Accedido: 21 de enero de 2026. [En línea]. Disponible en: https://observador.cr/ee-uu-y-costa-rica-firman-plan-de-25-millones-para-ciberseguridad/

Asamblea Legislativa de Costa Rica, «Ley 8968: Ley de Protección de la Persona frente al tratamiento de sus datos personales [Diario Oficial La Gaceta N.º 170]», Sistema Costarricense de Información Jurídica. Accedido: 21 de enero de 2026. [En línea]. Disponible en: https://pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=70975&nValor3=85989&strTipM=TC

Agencia de Protección de Datos de los Habitantes (PRODHAB), «Guías y directrices sobre medidas de seguridad para el tratamiento de datos personales». San José, Costa Rica.

Caja Costarricense de Seguro Social (CCSS), «Normativa de Seguridad de la Información y Control de Acceso a Sistemas Institucionales». San José, Costa Rica.

Asamblea Legislativa de Costa Rica, «Ley 5395: Ley General de Salud», Sistema Costarricense de Información Jurídica. Accedido: 21 de enero de 2026. [En línea]. Disponible en: https://pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=6581

Asamblea Legislativa de Costa Rica, «Ley 9048: Reforma de la Sección VIII, Delitos Informáticos y Conexos, del Título VII del Código Penal», Sistema Costarricense de Información Jurídica. Accedido: 21 de enero de 2026. [En línea]. Disponible en: https://pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=73583

National Institute of Standards and Technology, «Security and Privacy Controls for Information Systems and Organizations», NIST, Gaithersburg, MD; U.S. Department of Commerce, NIST Special Publication (SP) 800-53 Rev. 5, dic. 2020. doi: 10.6028/NIST.SP.800-53r5.

sealpath, «Protegiendo la información en sus tres estados», Sealpath. Accedido: 21 de enero de 2026. [En línea]. Disponible en: https://www.sealpath.com/es/blog/tres_estados_info/

D. F. Ferraiolo y D. R. Kuhn, «Role-Based Access Controls», presentado en 15th National Computer Security Conference, Baltimore, USA, 1992, pp. 554-563. [En línea]. Disponible en: https://csrc.nist.gov/files/pubs/conference/1992/10/13/rolebased-access-controls/final/docs/ferraiolo-kuhn-92.pdf

I. Novikov, «¿Qué es RBAC (control de acceso basado en roles)?», Wallarm. Accedido: 21 de enero de 2026. [En línea]. Disponible en: https://lab.wallarm.com/what/que-es-rbac-control-de-acceso-basado-en-roles/?lang=es

International Organization for Standardization (ISO), «ISO/IEC 27002:2022 - nformation security, cybersecurity and privacy protection — Information security controls». Ginebra, Suiza. Accedido: 21 de enero de 2026. [En línea]. Disponible en: https://www.iso.org/standard/75652.html

ISSN: 2015-5392