1. OBJETIVO

Establecer los parámetros tendientes a garantizar el manejo seguro de la información y los recursos tecnológicos del Instituto Cardiovascular del Cesar S.A., previniendo pérdidas de información, accesos no autorizados y posibles amenazas cibernéticas. Esta política establece procedimientos y controles necesarios para la protección de los datos sensibles de pacientes, colaboradores y terceros, así como de la infraestructura tecnológica de la institución.

2. ALCANCE

Esta política aplica a todas las personas que, dentro del Instituto Cardiovascular del Cesar S.A., gestionan información en cualquiera de sus formas, incluyendo las áreas operativas, administrativas, asistenciales y tecnológicas. Comprende la recolección, procesamiento, validación, almacenamiento, transmisión y disposición de la información utilizada para la toma de decisiones relacionadas con los procesos y sistemas de la institución.

3. DECLARACIÓN

El Instituto Cardiovascular del Cesar reconoce que la información es un activo critico que debe ser adecuadamente protegido y que su exposición a los diferentes riesgos internos y externos deliberados o accidentales pueden impactar negativamente en la seguridad de los pacientes. Por lo anterior provee los mecanismos necesarios para administrar efectivamente la información, mitigando los efectos nocivos de los riesgos asociados y conservando la prestaron del servicio continuamente.

Disposiciones generales:

El instituto Cardiovascular del Cesar adopta los siguientes principios de Seguridad de la Información:

Confidencialidad de la Información: El Instituto Cardiovascular del Cesar se compromete a proteger la confidencialidad de la información sensible de los pacientes, garantizando que los datos sólo sean accesibles a aquellos usuarios con autorización expresa, de acuerdo con sus roles y responsabilidades.

Integridad de la Información: Todos los sistemas de la institución deben asegurar la integridad de los datos. Esto implica que los datos no deben ser modificados sin autorización, y cualquier cambio debe ser registrado y auditable. Se deben utilizar mecanismos de validación y controles de acceso para garantizar que la información se mantenga precisa y completa en todo momento.

Disponibilidad de la Información: Se implementan medidas tecnológicas para garantizar la disponibilidad continua de la información crítica, asegurando que los sistemas de la institución permanezcan operativos incluso en situaciones de contingencia. Esto incluirá la implementación de sistemas de respaldo (backups) periódicos, planes de recuperación ante desastres (DRP).

Protección de Datos Personales: Cumplimiento estricto con la legislación vigente en materia de protección de datos personales, como la Ley 1581 de 2012 en Colombia, asegurando que la información personal de los pacientes sea tratada de manera adecuada, respetando sus derechos y garantizando que no sea utilizada para fines no autorizados.

Ciberseguridad: Se adoptan las mejores prácticas y tecnologías en ciberseguridad para proteger los sistemas contra amenazas cibernéticas, como virus, ransomware, malware y ataques de denegación de servicio (DoS). Esto incluye el uso de firewalls, antivirus y otras herramientas de seguridad informática.

Control de Accesos: Todos los accesos a los sistemas informáticos son gestionados mediante un control de acceso riguroso. Esto incluye la autenticación de usuarios a través de contraseñas seguras y el monitoreo continuo de los accesos a los sistemas. Los accesos son verificados periódicamente para asegurar que se mantengan dentro de los parámetros establecidos.

Responsabilidades del Personal: Cada miembro del personal es responsable de sus acciones y de los errores que puedan cometer relacionados con el manejo y protección de la información. Esto incluye el compromiso de aplicar los conocimientos adquiridos durante las capacitaciones y de actuar en conformidad con las políticas establecidas. La responsabilidad individual es fundamental para garantizar un entorno seguro y la protección de los datos de la institución y de los pacientes.

Cumplimiento de Normativas: La institución se compromete a cumplir con todas las normativas legales y regulaciones relacionadas con la protección de datos personales y la seguridad de la información.

Otras disposiciones:

- Los funcionarios tienen asignado un correo electrónico institucional exclusivamente para uso profesional, el cual no debe ser cerrado del equipo. La pérdida de información asociada al correo será responsabilidad del funcionario. Además, está completamente prohibido el envío de correos indebidos, como mensajes de contenido personal, inapropiado o que comprometan la seguridad y reputación del Instituto. Cualquier incumplimiento será tratado como una falta grave.

- Se prohíbe el uso de correos electrónicos personales en los equipos de cómputo del instituto, si se detecta uno de estos será inmediatamente cerrado del equipo por el Área de Sistemas y reportado ante su jefe inmediato.

- A cada funcionario que aplique se le asignará un usuario único para acceder a los sistemas y herramientas tecnológicas necesarias para el desarrollo de sus funciones. Este usuario único es personal e intransferible, por lo que no puede ser compartido ni utilizado desde equipos diferentes al asignado, ya que esto podría comprometer la seguridad de la información institucional.

- Para la creación de usuarios, el jefe inmediato debe enviar una solicitud formal a la Dirección Administrativa para validar la vinculación y funciones del funcionario; una vez aprobada, se autoriza al proceso de Tecnologías de la Información y Comunicaciones (TIC) a proceder con la gestión, para asegurar el control de accesos a los sistemas.

- Los equipos tendrán deshabilitados los accesos a puertos USB, discos ópticos y otros dispositivos externos para:
  - Prevenir ataques de malware.
  - Evitar extracciones no autorizadas de información.
  - Restringir la carga de archivos no relacionados con las actividades laborales.

- Los funcionarios tienen perfiles de conectividad a internet ajustados a sus necesidades laborales, con monitoreo basado en direcciones IP para garantizar un uso eficiente y adecuado.

- Las contraseñas son personales e intransferibles; compartirlas constituye una falta grave. El funcionario es plenamente responsable del uso correcto de sus credenciales, y cualquier inconveniente o perjuicio derivado de un manejo indebido recaerá bajo su exclusiva responsabilidad.

- Se da capacitación a cada funcionario nuevo, adaptada al área en la que ingresará, con el objetivo de ofrecer una explicación clara sobre el manejo de la información en las plataformas institucionales. Esta capacitación incluye el uso de los softwares específicos requeridos para el desempeño de sus funciones, garantizando un adecuado manejo de las herramientas tecnológicas y el cumplimiento de los protocolos de seguridad de la información.

- El escritorio de cada computador debe permanecer organizado, con accesos directos únicamente a carpetas institucionales, programas básicos necesarios para el desarrollo de las actividades del área, correo y la papelera de reciclaje.

Esto permite mantener un entorno ordenado y prevenir la pérdida de información o problemas relacionados con el manejo de archivos. Cualquier archivo adicional será trasladado con el acompañamiento del proceso de TIC a las carpetas correspondientes, y el usuario será notificado de la acción para garantizar el correcto resguardo de la información.

- Los usuarios deben evitar almacenar información sensible en sus equipos locales y usar únicamente las unidades drive de Backup designadas.

- El compartir carpetas requiere autorización formal del líder o coordinador del área, quien será responsable de la información contenida.

- Está prohibida la instalación de software no autorizado, incluyendo juegos. Cualquier necesidad de software adicional debe justificarse ante el Área de TIC.

- Los equipos de cómputo deben utilizarse exclusivamente para las actividades relacionadas con las funciones del cargo asignado. Está estrictamente prohibido emplearlos para realizar actividades ajenas al Instituto, ya que esto puede comprometer la seguridad de la información, el desempeño de los equipos y el cumplimiento de las responsabilidades laborales.

- Está estrictamente prohibido que personas ajenas a la Institución manipulen los equipos de cómputo asignados, debido a razones de seguridad y confidencialidad de la información. Permitir el acceso de terceros a los equipos puede comprometer datos sensibles, exponer la red a riesgos externos.

- Al ausentarse del puesto de trabajo, el funcionario debe bloquear su equipo (Windows + L) para prevenir accesos no autorizados y evitar el traspaso de datos sensibles. Esta medida garantiza la seguridad de la información institucional, y debido a su importancia, las contraseñas asociadas al equipo y a los sistemas son completamente privadas e intransferibles.

- No está permitido el uso de aplicaciones de mensajería personal en los equipos de cómputo institucionales. Además, queda estrictamente prohibido utilizar estas aplicaciones para compartir información sensible del Instituto, ya que esto representa un riesgo para la seguridad y confidencialidad de los datos.

- Los equipos están configurados con sistemas antivirus que se actualizan automáticamente de manera diaria para garantizar la máxima protección contra amenazas. Estas actualizaciones se realizan sin necesidad de intervención del usuario, y el Área de TIC supervisa su correcto funcionamiento.

- Se debe realizar un respaldo diario de los datos institucionales en los medios seguros designados. Este proceso es ejecutado por el Área de Sistemas para garantizar la integridad y disponibilidad de la información.

4. MONITOREO

- Porcentaje del personal capacitado en seguridad de la información:
  Fórmula: (Número de empleados capacitados / Número total de empleados) * 100
  Objetivo: Capacitar al 100% del personal al menos una vez al año.

- Número de casos reportados de incumplimiento a la seguridad informática.
  Fórmula: (Número total de casos reportados de incumplimiento a la seguridad informática / Total de funcionarios o áreas monitoreadas)
  Objetivo: Tendencia descendente.

5. BITÁCORA DE CAMBIOS

NO.	FECHA DE APROBACIÓN	ITEM ALTERADO	MOTIVO	REALIZADO POR
1	**06-06-2025**	Todos	Versión inicial del documento	**Elaboró:** José Miguel Casadiego **Ingeniero TIC** **Aprobó:** Martha Socarras Cuadrado **Gerente**