Inverclinicas S.A.S

Política Murillo: POLITICA DE SEGURIDAD DIGITAL Y SEGURIDAD DE LA INFORMACIÓN

	Inverclinicas S.A.S **Proceso MUR**: Tecnologia de la informacion **Área emisora MUR**: Sistemas **Política Murillo**: POLITICA DE SEGURIDAD DIGITAL Y SEGURIDAD DE LA INFORMACIÓN	**Código** PL-SIS-001 **Fecha** 2026-09-16 **Versión** 1.0

Estratégico	Misional	Apoyo	Evaluación

Justificación

Clínica Murillo en consecuente con su misión y responsabilidad hacia sus partes interesadas, establece las políticas de seguridad digital y seguridad de la información como un componente estratégico que contribuye al logro de los objetivos y cumplimiento de sus obligaciones.

Esta política establece un lineamiento sobre los aspectos relevantes de ciberseguridad, con el objetivo de proteger la infraestructura tecnológica e información almacenada y gestionadas desde las diferentes fuentes de información que se administran en la institución.

Política

Políticas de Gestión de incidentes de seguridad de la información

Establecer los lineamientos para detectar, reportar, analizar, valorar, contener oportunamente, evaluar el impacto y evitar la recurrencia de los incidentes de seguridad de la información en la Organización.

- Definir el procedimiento de Gestión de Incidentes de Seguridad de la Información para orientar a los colaboradores en la detección, reporte, escalamiento y contención de los incidentes de seguridad de la información; este procedimiento también debe incluir los pasos necesarios para generar un aprendizaje y mejora continua para evitar la recurrencia de los incidentes.
- El responsable final de un incidente de seguridad de la información es el propietario del activo de información afectado, por tanto es quien debe cumplir con la debida diligencia para que se asignen los recursos y prioridad requeridos.
- Los colaboradores tienen la responsabilidad de reportar en forma inmediata los eventos, incidentes o debilidades de seguridad de la información que identifiquen, haciendo uso del Procedimiento de Gestión de Incidentes de Seguridad de la Información.
- Se debe llevar un registro actualizado de los eventos e incidentes de seguridad de la información gestionados, manteniendo disponible toda la información requerida para auditorías, organismos de control y como parte del aprendizaje que la organización deba lograr para evitar su recurrencia.
- Todo incidente de seguridad de la información debe generar una documentación que describa cuál fue el riesgo que se materializó, identificando la o las vulnerabilidades aprovechadas y cuáles fueron las actividades para la contención y la remediación, detallando también las medidas utilizadas para evitar la recurrencia y que conlleven a la organización al aprendizaje correspondiente.
- Se deben reportar los incidentes de seguridad de la información a los líderes de los procesos; también se deben reportar a las autoridades competentes, cuando estos estén relacionados con el incumplimiento del marco legal y regulatorio aplicable en Colombia.
- Un incidente de seguridad de la información obliga al responsable del riesgo correspondiente, a realizar la actualización de la matriz de riesgos del proceso afectado, con la asesoría del Oficial de Seguridad de la Información; lo anterior considerando que debe registrarse la situación a la que queda expuesto la organización mientras se corrigen las vulnerabilidades evidenciadas.
- Se debe realizar capacitación y sensibilización a todos los colaboradores sobre la gestión de incidentes de seguridad de la información, para que desarrollen las capacidades y conocimiento necesarios para la identificación, reporte oportuno y seguimiento de los eventos de seguridad de la información, dejando claro la responsabilidad que cada uno tiene frente a este aspecto.

Políticas de seguridad de las operaciones

Establecer los lineamientos para asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.

- Procesos y procedimientos oficialmente definidos; estos dispositivos incluyen entre otros: access points, piñas, repetidores, equipos para análisis de tráfico.

- Se debe establecer una línea base de software para los computadores asignados a los colaboradores y se debe asegurar su aplicación, de manera que sólo esté instalado el software autorizado, validando que cuente con las herramientas de protección de seguridad definidas por la Dirección de TD&TI

Seguridad en la nube

- El contrato o licencia de alquiler en la nube, sin importar el tipo de plataforma, infraestructura o servicio, debe ser revisado y tener el visto bueno del área Jurídica.
- Toda plataforma, servicio o infraestructura de nube con la que cuente la organización, debe contar con logs de auditoría.
- El proveedor de servicios en la nube debe contar con controles que garanticen la confidencialidad, integridad y disponibilidad de la información.
- Se debe asegurar que todo servicio de computación en la nube se diseñe, implemente y opere conforme a las políticas de seguridad de la información de la organización.
- Se debe hacer un análisis de riesgos de seguridad de la información como prerrequisito para el despliegue de un servicio en la nube.
- En los contratos con los proveedores de servicios en la nube debe quedar estipulado que la organización debe realizar auditorías de seguridad de la información sobre estos servicios.
- La autenticación y autorización de usuarios de los servicios en la nube debe estar delegada en los sistemas de información destinados para tal fin, de esta manera, la organización es la encargada de gobernar el acceso, nunca el proveedor.
- Los controles definidos para los activos de información deben aplicarse indistintamente que estos sean procesados o almacenados de forma local o en la nube.
- En caso de contratar un servicio en la nube con almacenamiento de datos personales en un país diferente a Colombia, se debe garantizar que este país cumpla con los requerimientos exigidos por la ley 1581 de 2012.

Política de Seguridad de la información para las relaciones con terceros

Definir los criterios de seguridad de la información en las relaciones de la organización con terceros (proveedores, clientes, otros), para preservar la confidencialidad, integridad y disponibilidad de la información.

- Previo al establecimiento de un contrato se debe realizar un análisis de riesgos de seguridad de la información; los controles que se definan como resultado, deben ser exigidos al proveedor a través del contrato.
- El responsable del contrato debe realizar la debida diligencia para asegurar el cumplimiento de los requerimientos de seguridad de la información establecidos contractualmente con el proveedor.
- Se deben exigir contractualmente las condiciones de seguridad de la información para el almacenamiento, transmisión y procesamiento de los datos por parte de terceros con los que la organización establezca relaciones.
- Se debe establecer el compromiso con cualquier tercero que tenga relación con la organización, para que reporte y remedie las vulnerabilidades que se identifiquen sobre los sistemas de información que estén bajo su responsabilidad.
- Todo tercero está obligado a cumplir las políticas de seguridad de la información de la organización.
- El uso de sistemas de información de terceros exige el cumplimiento de las políticas de seguridad de la información definidas por la organización, las cuales deben ser previamente aceptadas.
- La información compartida con un tercero pasa a ser de su responsabilidad y exige el cumplimiento de las políticas de seguridad de la organización, asumiendo las consecuencias por cualquier incumplimiento.
- En los contratos con los proveedores, se debe evitar el uso del adjetivo “seguro” como un parámetro de cumplimiento debido a que este no define ningún tipo de responsabilidad; se debe especificar con términos concretos y medibles a qué se refiere esa condición de seguridad.

Políticas de seguridad en las comunicaciones

Definir pautas generales sobre el buen uso de las comunicaciones digitales, las cuales incluyen correo electrónico, mensajería instantánea y redes sociales, con el fin de asegurar la protección de la información de la organización.

- Los servicios de comunicación digital institucionales únicamente son asignados por la Dirección de TI&TD, con la autorización del jefe inmediato del colaborador correspondiente.

- Se debe implementar la trazabilidad de las comunicaciones digitales, garantizando las evidencias necesarias para la gestión de incidentes, auditorías o solicitudes de entes de control.
- Las cuentas de comunicaciones digitales institucionales deben ser suspendidas cuando un colaborador finalice su vínculo laboral o contractual con la organización.
- Todas las cuentas de usuario de comunicaciones digitales deben tener siempre asignado un único responsable; su uso es de carácter personal e intransferible.
- La Dirección de TI&TD debe implementar mecanismos de control para la protección de comunicaciones digitales para prevenir riesgos asociados con malware o ataques informáticos. Todos los mensajes electrónicos deben ser analizados para identificar malware.
- Si se presenta una solicitud a un colaborador para la entrega de información catalogada como confidencial, esta debe remitirse al propietario de la información quien debe tomar la decisión sobre las acciones a tomar.
- Los colaboradores deben abstenerse de abrir o hacer uso y revisión no autorizada de la cuenta de correo electrónico de otros usuarios.
- No está permitido el uso de correo personal y redes sociales en los equipos corporativos de la organización; la única excepción se presenta para los responsables de manejar las redes sociales corporativas.
- Cada colaborador es responsable por todas las actividades realizadas con su usuario en las herramientas definidas por la organización para las comunicaciones digitales, como son correo electrónico y mensajería instantánea, y por tanto, de las acciones que se puedan derivar como consecuencia de un mal uso que comprometa la seguridad de la información de la organización.
- Todo correo que provenga de una fuente no confiable debe ser eliminado.
- No se deben abrir archivos adjuntos o enlaces contenidos en correos electrónicos, a menos que se tenga plena certeza de la confiabilidad de la fuente, de la información de los adjuntos y de los sitios a los que direccionan los links. Ante cualquier duda, se debe consultar el procedimiento Protección Contra Software Malicioso.

Política de adquisición, desarrollo y mantenimiento de sistemas de información

Asegurar que el software desarrollado al interior de la organización o adquirido a terceras partes, cumpla con los requerimientos de seguridad de la información definidos por el proceso de negocio para el cual fue desarrollado o adquirido.

- Se deben establecer y mantener ambientes separados de desarrollo, pruebas y producción, claramente identificados, dentro de la infraestructura de desarrollo de sistemas de información.
- No se deben realizar pruebas, instalaciones o desarrollos de software, directamente sobre el entorno de producción.
- Se debe restringir el acceso a compiladores, editores y otros utilitarios del sistema operativo en el ambiente de producción.
- Se deben implementar los controles necesarios para asegurar que las migraciones entre los ambientes de desarrollo, pruebas y producción cumplen con los requisitos de seguridad de la información definidos por el proceso de negocio para el cual fue desarrollado o adquirido el software.
- Todo el software debe cumplir con la generación de archivos de registro (logs) que entreguen la información suficiente sobre las acciones ejecutadas, especialmente para el seguimiento a las anomalías y los hechos relacionados con incumplimiento de las políticas de seguridad de la información.
- Se debe restringir el acceso a los repositorios de códigos fuente, dejando la trazabilidad de quién consulta, modifica, elimina o adiciona este tipo de archivos. Los archivos de código fuente no pueden ser almacenados en computadores diferentes a los repositorios establecidos formalmente.
- Se debe asegurar que los sistemas de información adquiridos o desarrollados por contratistas cuenten con un acuerdo de licenciamiento, el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual.
- Se debe asegurar que los sistemas de información adquiridos o desarrollados por contratistas cuenten con un contrato de soporte mediante el cual se asegure la gestión de los aspectos relacionados con seguridad de la información, incluyendo la gestión de vulnerabilidades.
- Los desarrolladores de software internos o externos, contratados, deben aplicar las buenas prácticas y lineamientos de desarrollo seguro durante todo el ciclo de vida del desarrollo de software, desde el diseño hasta la puesta en marcha.

- Todos los proyectos bajo la responsabilidad de la organización deben exigir el cumplimiento de esta política para lo concerniente a la adquisición o desarrollo de software.

Clínica Murillo se encuentra comprometida y facilita los espacios y recursos para la implementación integral de esta política y las estrategias que permitan su cumplimiento.

Esta política se le hace seguimiento a través del programa de Seguridad de la información y el Comité de Tecnología de la Información que permiten evaluar el despliegue e instancia de resolución de situaciones de interés y casos de Ciberseguridad, asimismo implementación y mejora continua de los programas asociados.

El proceso de Tecnología de la información es el responsable de la administración de esta política y en esa medida, gestionará con las áreas correspondientes su divulgación a todos los colaboradores y actualización de acuerdo a disposiciones y mejoras.

Actualizaciones

No.	CAMBIO REALIZADO	FECHA DE ACTUALIZACIÓN
1	Emisión del documento bajo estándar ISO 9001.	Septiembre 16 del 2026

ELABORÓ	REVISÓ	APROBÓ
Luis Palma Varela Jefe de Desarrollo y Mejoramiento	Royman Rojas Jefe de Sistema	Karen De La Hoz Tejeda Gerente