PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2026

Contenido

1. MARCO CONCEPTUAL

- **Seguridad de la Información:** Conjunto de principios, políticas y medidas orientadas a proteger la información institucional frente a accesos no autorizados, pérdidas, alteraciones o divulgaciones indebidas, garantizando su uso adecuado dentro de la entidad.
- **Privacidad de la Información:** Protección de los datos personales y sensibles tratados por la entidad, asegurando que su uso se realice conforme a la normativa vigente y únicamente para los fines institucionales autorizados.
- **Confidencialidad:** Principio que garantiza que la información solo sea accesible y conocida por personas, sistemas o procesos debidamente autorizados.
- **Integridad:** Propiedad que asegura que la información se mantiene completa, exacta y sin modificaciones no autorizadas durante su almacenamiento, procesamiento o transmisión.
- **Disponibilidad:** Capacidad de la información y de los sistemas que la soportan para estar accesibles y operativos cuando sean requeridos por los usuarios autorizados.
- **Activo de Información:** Cualquier información, sistema, base de datos, documento, equipo o recurso tecnológico que tiene valor para la entidad y es necesario para el cumplimiento de sus funciones.

- **Tecnologías de la Información y las Comunicaciones (TIC):** Conjunto de recursos tecnológicos utilizados para la captura, procesamiento, almacenamiento y transmisión de la información institucional.

- **Datos Personales:** Información asociada o que pueda asociarse a una persona natural identificada o identificable, tratada por la entidad en el desarrollo de sus funciones.

- **Información Sensible:** Datos personales cuyo uso indebido puede afectar la intimidad del titular o generar discriminación, especialmente relevante en el sector salud.

- **Usuario de la Información:** Servidor público, contratista o tercero autorizado que accede y utiliza la información y los sistemas institucionales para el desarrollo de sus funciones.

- **Gestión de la Información:** Conjunto de actividades orientadas a administrar, proteger y utilizar adecuadamente la información durante todo su ciclo de vida dentro de la entidad.

- **Cultura de Seguridad de la Información:** Conjunto de valores, prácticas y comportamientos adoptados por los funcionarios para garantizar el uso responsable y seguro de la información institucional.

- **Plan de Seguridad y Privacidad de la Información:** Instrumento de planificación que define las acciones, estrategias y actividades orientadas a fortalecer la protección de la información institucional durante una vigencia determinada.

- **Gobernanza de la Información:** Marco de decisiones y responsabilidades que orienta la administración adecuada de la información como activo estratégico de la entidad.

2. INTRODUCCIÓN

La seguridad informática, es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con ésta (incluyendo la información contenida). Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore (activo) y signifique un riesgo si ésta llega a manos de otras personas. Este tipo de información se conoce como información privilegiada o confidencial.

Con la definición de las políticas y estándares de seguridad informática se busca establecer en el interior de la entidad una cultura de calidad operando en una forma confiable.

La seguridad informática, es un proceso donde se deben evaluar y administrar los riesgos apoyados en políticas y estándares que cubran las necesidades del Hospital en materia de seguridad.

Para el desarrollo de este manual se busca estructurarlo en base a ciertos criterios tales como:

- Seguridad Institucional
- Seguridad física y del medio ambiente
- Manejo y control de equipos de Cómputo

- Control de usuarios
- Lineamientos legales

El presente documento corresponde a un Plan, orientado a definir las acciones a ejecutar durante la vigencia para fortalecer la seguridad y privacidad de la información institucional.

3. JUSTIFICACIÓN

La formulación del presente Plan de Seguridad y Privacidad de la Información se justifica en la necesidad de garantizar la protección de la información institucional, clínica, administrativa y financiera del Hospital Departamental San Antonio de Padua, frente a riesgos asociados al uso de tecnologías de la información.

Así mismo, el plan permite establecer lineamientos claros para el uso adecuado de los recursos tecnológicos, fortalecer la cultura de seguridad de la información y asegurar la continuidad de los procesos institucionales, en concordancia con los objetivos estratégicos de la entidad.

4. OBJETIVO

Fortalecer la seguridad y privacidad de la información del Hospital Departamental San Antonio de Padua, mediante la implementación de acciones orientadas a proteger los activos de información, garantizar su confidencialidad, integridad y disponibilidad, y promover el uso responsable de las tecnologías de la información.

5. METAS

- Garantizar el cumplimiento de las políticas de seguridad y privacidad de la información durante la vigencia del plan.
- Fortalecer los controles de acceso lógico y físico a la información institucional.
- Promover buenas prácticas en el uso de los recursos tecnológicos por parte de los funcionarios.
- Asegurar la correcta gestión de copias de respaldo de la información crítica.

6. EVALUACIÓN DE NECESIDADES (DIAGNÓSTICO)

El diagnóstico de seguridad de la información evidencia la necesidad de fortalecer los controles sobre el acceso a la información, el uso adecuado de los equipos de cómputo y la gestión de respaldos, debido al crecimiento en el uso de herramientas tecnológicas y a la criticidad de la información manejada por la entidad.

7. POBLACIÓN OBJETIVO

La población objetivo del presente plan está conformada por los funcionarios, contratistas, personal asistencial, administrativo y de apoyo que interactúan directa o indirectamente con los sistemas de información y activos tecnológicos del Hospital.

8. PRESUPUESTO

El Presupuesto constituye un componente esencial del Plan de Seguridad y Privacidad de la Información, ya que garantiza la viabilidad real de las acciones propuestas y su coherencia con la planeación financiera institucional. La

adecuada asignación de recursos permite asegurar la implementación de controles técnicos y administrativos, la adquisición de herramientas tecnológicas, el mantenimiento de la infraestructura existente y el desarrollo de actividades de fortalecimiento de la seguridad de la información.

Este apartado evidencia que el Plan no es solo una declaración de intenciones, sino un instrumento ejecutable, alineado con la disponibilidad presupuestal de la entidad y con los procesos de gestión financiera, lo cual es fundamental para asegurar su sostenibilidad durante la vigencia.

9. CRONOGRAMA

El Cronograma permite organizar temporalmente la ejecución del Plan, estableciendo de manera clara los periodos en los cuales se desarrollarán las actividades definidas. Este componente facilita el seguimiento y control del avance del Plan, asegurando que las acciones se implementen de manera oportuna y ordenada.

En el contexto del Plan de Seguridad y Privacidad de la Información, el cronograma semestral resulta adecuado para la planificación institucional, ya que permite evaluar avances parciales, realizar ajustes oportunos y garantizar el cumplimiento de las metas establecidas dentro de la vigencia.

10. ESTRUCTURA DEL PLAN O PROGRAMA

La Estructura del Plan describe la forma en que se organizan y articulan los diferentes componentes del Plan de Seguridad y Privacidad de la Información. Este apartado es fundamental para evidenciar que el Plan cuenta con una

metodología clara, lógica y coherente, que integra diagnóstico, objetivos, metas, estrategias, cronograma y evaluación.

Además, la estructura facilita la comprensión del documento como un instrumento de planeación formal, permitiendo a los responsables de su ejecución y seguimiento identificar claramente las relaciones entre sus diferentes secciones.

11. DESARROLLO GENERAL

11.1 Aplicación

Las políticas y estándares de seguridad informática tienen por objeto establecer medidas y patrones técnicos de administración y organización de las Tecnologías de Información y Comunicaciones TIC´s de todo el personal comprometido en el uso de los servicios informáticos proporcionados por la entidad, en cuanto a la mejora y al cumplimiento de los objetivos institucionales.

También se convierte en una herramienta de difusión sobre las políticas y estándares de seguridad informática a todo el personal de la entidad. Facilitando una mayor integridad, confidencialidad y confiabilidad de la información, al manejo de los datos, al uso de los bienes informáticos tanto de hardware como de software disponible, minimizando los riesgos en el uso de las tecnologías de información.

11.2 Evaluación de las Políticas

Las políticas tendrán una revisión periódica se recomienda que sea mínimo cada año, para realizar actualizaciones, modificaciones y ajustes basados en las recomendaciones y sugerencias.

11.3 Beneficios

Las políticas y estándares de seguridad informática establecidas en el presente documento son la base fundamental para la protección de los activos informáticos y de toda la información de las Tecnologías de Información y Comunicaciones (TIC´s) en la entidad.

12. SEGURIDAD INSTITUCIONAL

Política: Toda persona que ingresa como funcionario nuevo al Hospital departamental san Antonio de Padua, para manejar equipos de cómputo y hacer uso de servicios informáticos debe aceptar las condiciones de confidencialidad, de uso adecuado de los bienes informáticos y de la información, así como cumplir y respetar las directrices impartidas en el Manual de Políticas y Estándares de Seguridad Informática.

12.1 Usuarios Nuevos

Todo el personal nuevo de la entidad, que requiera para el desarrollo de sus actividades, asignación de equipo de cómputo, usuario de red, usuarios de aplicativos deberá ser notificado a la persona encargada de sistemas, para asignarle los derechos correspondientes o en caso de retiro del funcionario, anular y cancelar los derechos otorgados como usuario informático, esta solicitud debe ser realizada por el jefe de proceso.

12.2 Obligaciones de los usuarios

Es responsabilidad de los usuarios de bienes y servicios informáticos cumplir las Políticas y Estándares de Seguridad Informática para Usuarios del presente Manual. Al igual cuando se termine el contrato, el usuario avisara a sistemas, donde se le firmara un paz y salvo para salvaguardar la información si hace

parte de los procesos administrativos y posterior inactivación del usuario en Dinámica Gerencial Hospitalaria.

12.3 Capacitación en seguridad informática

Todo servidor o funcionario nuevo en la entidad deberá contar con la inducción sobre las Políticas y Estándares de Seguridad Informática, donde se den a conocer las obligaciones para los usuarios y las sanciones en que pueden incurrir en caso de incumplimiento. La inducción debe ser realizada por el jefe de proceso en acompañamiento del responsable de sistemas.

12.4 Sanciones

Se consideran violaciones graves el robo, daño, divulgación de información reservada o confidencial de esta dependencia, o de que se le declare culpable de un delito informático.

13. SEGURIDAD FÍSICA Y DEL MEDIO AMBIENTE

Política: Para el acceso a los sitios y áreas restringidas se debe notificar al responsable de sistemas para la autorización correspondiente, y así proteger la información y los bienes informáticos.

13.1 Protección de la información y de los bienes informáticos

- El usuario o funcionario deberán reportar de forma inmediata al encargado de sistemas, cuando se detecte riesgo alguno real o potencial sobre equipos de cómputo o de comunicaciones, tales como caídas de agua, choques eléctricos, caídas o golpes o peligro de incendio.

- El usuario o funcionario tienen la obligación de proteger las unidades de almacenamiento que se encuentren bajo su responsabilidad, aun cuando no se utilicen y contengan información confidencial o importante.
- Es responsabilidad del usuario o funcionario evitar en todo momento la fuga de información de la entidad que se encuentre almacenada en los equipos de cómputo personal que tenga asignados.

13.2 Controles de acceso físico

- Cualquier persona que tenga acceso a las instalaciones de la entidad, deberá registrar al momento de su entrada, el equipo de cómputo, equipo de comunicaciones, medios de almacenamiento y herramientas que no sean propiedad de la entidad, en el área de recepción o portería, el cual podrán retirar el mismo día. En caso contrario deberá tramitar la autorización de salida correspondiente.

  Las computadoras portátiles, y cualquier activo de tecnología de información, podrán ser retirado de las instalaciones de la entidad únicamente con la autorización de salida del área de Inventarios, anexando el comunicado de autorización del equipo debidamente firmado por el almacenista.
- Las computadoras personales, serán registrados por el vigilante de cada servicio, al momento de ingreso y egreso

13.3 Seguridad en áreas de trabajo

El área de telecomunicaciones de la entidad son áreas restringidas, por lo que solo el personal autorizado por la persona encargada de sistemas puede acceder a él.

13.4 Protección y ubicación de los equipos

- Los usuarios no deben mover o reubicar los equipos de cómputo o de comunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización del encargado de sistemas, en caso de requerir este servicio deberá solicitarlo.
- El Área de activos fijos será la encargada de generar el resguardo y recabar la firma del usuario informático como responsable de los activos informáticos que se le asignen y de conservarlos en la ubicación autorizada por el.
- El equipo de cómputo asignado deberá ser para uso exclusivo de las funciones de los funcionarios o servidores de la entidad.
- Será responsabilidad del usuario contar con la capacitación necesaria para el manejo de las herramientas informáticas que se utilizan en su equipo, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas.
- Es responsabilidad de los usuarios almacenar su información únicamente en la partición del disco duro diferente destinada para archivos de programas y sistemas operativos, generalmente c:\.
- Mientras se opera el equipo de cómputo, no se deberán consumir alimentos o ingerir líquidos.
- Se debe evitar colocar objetos encima del equipo cómputo o tapar las salidas de ventilación del monitor o de la CPU.
- Se debe mantener el equipo informático en un lugar limpio y sin humedad.
- El usuario debe asegurarse que los cables de conexión no sean pisados al colocar otros objetos encima o contra ellos en caso de que no se cumpla

solicitar una reubicación de cables con el personal de sistemas encargado.

- Cuando se requiera realizar cambios múltiples del equipo de cómputo derivado de reubicación de lugares físicos de trabajo o cambios locativos, éstos deberán ser notificados con cinco días de anticipación a la persona encargada d sistemas a través de

  un plan detallado, así mismo solicitar al almacenista los materiales necesarios para la adecuación del nuevo sitio de trabajo.
- Queda terminantemente prohibido que el usuario o funcionario distinto al personal de sistemas abra o destape los equipos de cómputo.

13.5 Mantenimiento de equipos

Únicamente el personal autorizado por el responsable de sistemas podrá llevar a cabo los servicios y reparaciones al equipo informático.

Los usuarios deberán asegurarse de respaldar en copias de respaldo o backups la información que consideren relevante cuando el equipo sea enviado a reparación y borrar aquella información sensible que se encuentre en el equipo, previendo así la pérdida involuntaria de información, derivada del proceso de reparación.

13.6 Pérdida de Equipo

- El servidor o funcionario que tengan bajo su responsabilidad o asignados algún equipo de cómputo será responsable de su uso y custodia; en consecuencia, responderá por dicho bien de acuerdo a la normatividad vigente en los casos de robo, extravío o pérdida del mismo.

- El servidor o funcionario deberán dar aviso inmediato al almacenista y encargado de sistemas de la desaparición, robo o extravío de equipos de cómputo, periféricos o accesorios bajo su responsabilidad.

13.7 Uso de dispositivos extraíbles

- El responsable de sistemas velará porque todos los usuarios de los sistemas de Información estén registrados en su Base de Datos para la autorización de uso de dispositivos de almacenamiento externo, como PenDrives o Memorias USB, Discos portátiles, Unidades de Cd y DVD Externos, para el manejo y traslado de información o realización de copias de seguridad o Backups.
- Cada Jefe de dependencia debe reportar al encargado de sistemas, el listado de funcionarios a su cargo que manejan estos tipos de dispositivos, especificando clase, tipo y uso determinado.
- El uso de los quemadores externos o grabadores de disco compacto es exclusivo para Backups o copias de seguridad de software y para respaldos de información que por su volumen así lo justifiquen.
- El servidor o funcionario usuario que tengan asignados estos tipos de dispositivos serán responsable del buen uso de ellos.
- Todo funcionario o servidor que use para su trabajo y de carácter personal memoras USB debe responsabilizarse por el buen uso de ellas.

13.8 Daño del equipo

El equipo de cómputo, periférico o accesorio de tecnología de información que sufra algún desperfecto, daño por maltrato, descuido o negligencia por parte del usuario responsable, se le levantara un reporte de incumplimiento de políticas de seguridad.

14. ADMINISTRACIÓN DE OPERACIONES EN LOS EQUIPOS DE CÓMPUTO

- Los usuarios y funcionarios deberán proteger la información utilizada en la infraestructura tecnológica de la entidad. De igual forma, deberán proteger la información reservada o confidencial que por necesidades institucionales deba ser guardada, almacenada o transmitida, ya sea dentro de la red interna institucional a otras dependencias de sedes alternas o redes externas como internet.
- Los usuarios y funcionarios que hagan uso de equipos de cómputos deben conocer y aplicar las medidas para la prevención de código malicioso como pueden ser virus, caballos de Troya o gusanos de red.
- Cuando un funcionario no autorizado o un visitante requieran la necesidad de ingresar a la Sala donde se encuentren los Servidores, debe solicitar mediante comunicado interno debidamente firmada y autorizado por el Jefe inmediato de su sección o dependencia y para un visitante se debe solicitar la visita con anticipación la cual debe traer el visto bueno del jefe del proceso, y donde se especifique tipo de actividad a realizar, y siempre contar con la presencia de un funcionario de sistemas.
- El encargado de sistemas deberá llevar un registro escrito de todas las visitas autorizadas a los Centros de telecomunicaciones restringidos.
- Todo equipo informático ingresado a los Centros de telecomunicaciones restringidos deberá ser registrado en el libro de visitas.
- Cuando se vaya a realizar un mantenimiento en algunos de los equipos del Centro de telecomunicaciones restringido, se debe dar aviso con anticipación a los usuarios para evitar traumatismos.

- El jefe de cada proceso, con apoyo del encargado de sistemas, deberá solicitar al almacenista los equipos de protección para las instalaciones contra incendios, inundaciones, sistema eléctrico de respaldo, UPS.

14.1 Uso de medios de almacenamiento

- Los usuarios y servidores de la entidad deben conservar los registros o la información que se encuentra activa y aquella que ha sido clasificada como reservada o confidencial.
- Las actividades que realicen los usuarios y funcionarios en la infraestructura Tecnología de Información y Comunicaciones (TIC´s) de la entidad, podrán ser registradas y objeto de auditoría.

14.2 Adquisición de software

- Los usuarios y funcionarios que requieran la instalación de software que no sea propiedad de la entidad, ni de los entes de control del estado, deberán justificar su uso y solicitar su autorización por el funcionario de sistemas, con el visto bueno de su Jefe inmediato, indicando el equipo de cómputo donde se instalará el software y el período de tiempo que será usado.
- Se considera una falta grave el que los usuarios o funcionarios instalen cualquier tipo de programa (software) en sus computadoras, estaciones de trabajo, servidores, o cualquier equipo conectado a la red, que no esté autorizado por el responsable de sistemas.
- Es responsabilidad del almacenista o quien haga sus veces, suministrar y custodiar, las licencias de software para instalaciones por parte del responsable de sistemas, en equipos de trabajo y servidores.
- El responsable de sistemas deberá ofrecer mantenimiento preventivo a los equipos de cómputo de la entidad.

- En el proceso de reinstalar un programa el encargado de sistemas debe borrar completamente la versión instalada para luego proceder a instalar la nueva versión que desea, esto siempre y cuando no sea una actualización del mismo.
- Deben mantener un inventario de equipos físicos y de los programas instalados y pueden borrar o instalar programas o software autorizados y legalmente licenciados.
- Cuando se adquieren software para tareas específicas en la entidad, el jefe de proceso de velar porque el proveedor brinde a los funcionarios la capacitación y soporte necesario para el manejo de la misma.

14.3 Licenciamiento de Software

Para el Control de Licenciamiento de Software la entidad, a través del responsable de almacén en adelante, debe garantizar que todos los equipos adquiridos cuenten con sus respectivas licencias de software y los que no sean factibles se implementaran software libre.

14.4 Identificación del incidente

- El usuario o funcionario que detecte o tenga conocimiento de la posible ocurrencia de un incidente de seguridad informática deberá reportarlo al Área de sistemas lo antes posible, indicando claramente los datos por los cuales lo considera un incidente de seguridad informática.
- Cuando exista la sospecha o el conocimiento de que información confidencial o reservada ha sido revelada, modificada, alterada o borrada sin la autorización de las Directivas competentes, el usuario o funcionario deberá notificar al responsable de sistemas.

- Cualquier incidente generado durante la utilización u operación de los activos de tecnología de información de la entidad debe ser reportado al responsable de sistemas.

14.5 Administración de la Red

Los usuarios de las áreas no deben establecer redes de área local, conexiones remotas a redes internas o externas, intercambio de información con otros equipos de cómputo utilizando el protocolo de transferencia de archivos (FTP), u otro tipo de protocolo para la transferencia de información empleando la infraestructura de red de la entidad, sin la autorización de su jefe de proceso y del encargado de sistemas.

14.6 Seguridad para la red

Será considerado como un ataque a la seguridad informática y una falta grave, cualquier actividad no autorizada por el jefe de proceso y de sistemas, en la cual los usuarios o funcionarios realicen la exploración de los recursos informáticos en la red de la entidad, así como de las aplicaciones que sobre dicha red operan, con fines de detectar y explotar una posible vulnerabilidad.

14.7 Uso del Correo electrónico y acceso a páginas web

- Los usuarios y funcionarios no deben usar cuentas de correo electrónico asignadas a otras personas, ni recibir mensajes en cuentas de otros. Si fuera necesario leer el correo de alguien más (mientras esta persona se encuentre fuera o de vacaciones) el usuario ausente debe redireccionar el correo a otra cuenta de correo interno, quedando prohibido hacerlo a una dirección de correo electrónico externa a la entidad.

- Los usuarios y funcionarios deben tratar los mensajes de correo electrónico y archivos adjuntos como información de propiedad del Hospital. Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor.
- Los usuarios podrán enviar información reservada y/o confidencial vía correo electrónico siempre y cuando vaya destinada exclusivamente a personas autorizadas y en el ejercicio estricto de sus funciones y responsabilidades.
- Queda prohibido falsificar, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico.
- Queda prohibido interceptar, revelar o ayudar a terceros a interceptar o revelar las comunicaciones electrónicas.
- Los usuarios deben administrar el espacio en el correo electrónico, de tal forma que siempre dispongan como mínimo de un 20% de espacio libre, para ello deben descargar y guardar la información en carpetas en el disco local.
- Los funcionarios no podrán ingresar a páginas web de redes sociales (Facebook, badoo, Myspace, chats, etc), y juegos, a menos que esta haga parte de sus actividades laborales, lo podrá hacer previa autorización del jefe del proceso.

14.8 Controles contra virus o software malicioso

- El encargado del área de sistemas velara por la instalación y actualización de antivirus en todos los equipos de cómputo de la entidad.
- El almacenista será el responsable de suministrar las respectivas licencias de acuerdo al número de equipos de cómputo disponibles en la entidad.

- Para prevenir infecciones por virus informático, los usuarios no deben hacer uso de software que no haya sido proporcionado y validado por el área de sistemas.
- Los usuarios de los equipos de cómputo deben verificar que la información y los medios de almacenamiento, estén libres de cualquier tipo de código malicioso, para lo cual deben ejecutar el software antivirus instalado en su pc.
- Todos los archivos de computadoras que sean proporcionados por personal externo o interno considerando al menos programas de software, bases de datos, documentos y hojas de cálculo que tengan que ser descomprimidos, el usuario debe verificar que estén libres de virus utilizando el software antivirus autorizado antes de ejecutarse.
- Ningún usuario, empleado o personal externo, podrá bajar descargar software de sistemas, boletines electrónicos, sistemas de correo electrónico, de mensajería instantánea y redes de comunicaciones externas, sin verificar que no contenga virus.
- Cualquier usuario que sospeche de alguna infección por virus de computadora, deberá dejar de usar inmediatamente el equipo y notificar al encargado de sistemas, para la revisión y erradicación del virus.
- Los usuarios no deberán alterar o eliminar, las configuraciones de seguridad para detectar y/o prevenir la propagación de virus que sean implantadas por el área d sistemas en: Antivirus, Outlook, office, Navegadores u otros programas.
- Debido a que algunos virus son extremadamente complejos, ningún usuario o funcionario deberá intentar erradicarlos de las computadoras, solo la persona de sistemas.

14.9 Controles para la Generación y Restauración de Copias de Respaldo (Backups)

Procedimiento de generación y restauración de copias de respaldo para salvaguardar la información crítica de los procesos significativos de la entidad. Se deberán considerar como mínimo los siguientes aspectos:

Establecer como medida de seguridad informática la necesidad de realizar copias de respaldo o backups, en los equipos de cómputo administrativos y servidores de acuerdo al cronograma para tal fin.
Cada funcionario es responsable directo de la generación de los backups o copias de respaldo, asegurándose de validar la copia que saca de su equipo el responsable de sistemas.

El área de sistemas debe conocer y manejar el software utilizado para la generación y/o restauración de copias de respaldo, registrando el contenido y su prioridad. Rotación de las copias de respaldo, debidamente marcadas.
Almacenamiento interno o externo de las copias de respaldo, de acuerdo con el manual de procedimiento.

14.10 Planes de Contingencia

Definición: Se entiende por PLAN DE CONTINGENCIA los procedimientos alternativos a la operación normal en una organización, cuyo objetivo principal es permitir el continuo funcionamiento y desarrollo normal de sus operaciones, preparándose para superar cualquier eventualidad ante accidentes de origen interno o externo, que ocasionen pérdidas importantes de información. Estos deben prepararse de cara a futuros sucesos.

15. ACCESO LÓGICO

Política: Cada usuario y funcionario son responsables de los mecanismos de control de acceso que les sean proporcionado; esto es, de su " I D " login de usuario y contraseña necesarios para acceder a la red, información, correo electrónico, inicio de sesión, aplicativos y a la infraestructura tecnológica de la entidad, por lo que deberá mantener de forma confidencial.

El permiso de acceso a la información que se encuentra en la infraestructura tecnológica de la entidad debe ser proporcionado por el dueño de la información, con base en el principio de "Derechos de Autor" el cual establece que únicamente se deberán otorgar los permisos mínimos necesarios para el desempeño de sus funciones.

15.1 Controles de acceso lógico

- Todos los usuarios de servicios de información son responsables por el de usuario y contraseña que recibe para el uso y acceso de los recursos.
- Todos los usuarios deberán autenticarse por los mecanismos de control de acceso provistos por la entidad antes de poder usarla infraestructura tecnológica.
- Los usuarios no deben proporcionar información a personal externo, de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica, a menos que se tenga el visto bueno del dueño de la información y de su jefe inmediato.
- Cada usuario que acceda a la infraestructura tecnológica de la entidad debe contar con un identificador de usuario (ID) único y personalizado. Por lo cual no está permitido el uso de un mismo ID por varios usuarios.

- Los usuarios y funcionarios son responsables de todas las actividades realizadas con su identificador de usuario (ID). Los usuarios no deben divulgar ni permitir que otros utilicen sus identificadores de usuario, al igual que tiene prohibido utilizar el ID de otros usuarios.

15.2 Administración de privilegios

Cualquier cambio en los roles y responsabilidades en el manejo de información y aplicativos de los usuarios deberán ser notificados al administrador de redes, para el cambio de privilegios.

15.3 Equipo desatendido

- Los usuarios deberán mantener sus equipos de cómputo con controles de acceso como contraseñas y protectores de pantalla (screensaver) previamente instalados por el responsable de sistemas cuando no se encuentren en su lugar de trabajo.
- Cada usuario es responsable de la conservación de la clave de su equipo y está en obligación de divulgarla en el momento de retiro de la entidad.

15.4 Administración y uso de contraseñas

- La asignación de contraseñas debe ser realizada de forma individual, por lo que el uso de contraseñas compartidas está prohibido.
- Cuando un usuario olvide, bloquee o extravíe su contraseña, deberá acudir a área de sistemas para que se le proporcione una nueva contraseña.
- Está prohibido que las contraseñas se encuentren de forma legible en cualquier medio impreso y dejarlos en un lugar donde personas no autorizadas puedan descubrirlos.

- Sin importar las circunstancias, las contraseñas nunca se deben compartir o revelar. Hacer esto responsabiliza al usuario que prestó su contraseña de todas las acciones que se realicen con el mismo.
- Todo usuario que tenga la sospecha de que su contraseña es conocido por otra persona, deberá cambiarlo inmediatamente.
- Los usuarios no deben almacenar las contraseñas en ningún programa o sistema que proporcione esta facilidad.

15.5 Controles para Otorgar, Modificar y Retirar Accesos a Usuarios

- Todo usuario debe quedar registrado en la Base de Datos Usuarios y Roles, disponible para tal fin en los aplicativos que usa la entidad.
- La creación de un nuevo usuario y/o solicitud para la asignación de otros roles dentro del sistema, deberá de venir acompañado del reporte debidamente firmado por el jefe del proceso, para trámite ante el proveedor del software o quien haga sus veces.

15.6 Control de accesos remotos

La administración remota de equipos conectados a Internet no está permitida, salvo que se cuente con el visto bueno y con un mecanismo de control de acceso seguro autorizado por el dueño de la información.

16. CUMPLIMIENTO DE SEGURIDAD INFORMÁTICA

Política: El jefe del proceso de Gestión en sistemas, junto con los jefes cada uno de los procesos de la entidad, o quien haga sus veces, tiene la responsabilidad de proponer y revisar el cumplimiento de normas y políticas de seguridad, que garanticen acciones preventivas y correctivas para la salvaguarda de equipos

e instalaciones de cómputo, así como de bancos de datos de información automatizada en general.

17. DERECHOS DE PROPIEDAD INTELECTUAL

Los sistemas desarrollados por personal interno o externo para actividades propias de la entidad son propiedad intelectual del hospital Departamental san Antonio de Padua.

18. CUMPLIMIENTO DE LA POLITICA DE SEGURIDAD

- Los jefes de procesos o responsable de proceso de inducción en la entidad, será responsable de la socialización de las políticas de seguridad y aplicación de estas.
- El área de sistemas realizará acciones de verificación del cumplimiento del Manual de Políticas y Estándares de Seguridad Informática.
- El área de sistemas podrá implantar mecanismos de control que permitan identificar tendencias en el uso de recursos informáticos del personal interno o externo, para revisar la actividad de procesos que ejecuta y la estructura de los archivos que se procesan. El mal uso de los recursos informáticos que sea detectado será reportado conforme a lo indicado en la política de Seguridad de Personal.
- Los jefes y responsables de los procesos establecidos deben apoyar las revisiones del cumplimiento de los sistemas con las políticas y estándares de seguridad informática apropiadas y cualquier otro requerimiento de seguridad.

19. VIOLACIONES DE SEGURIDAD INFORMÁTICA

- Está prohibido el uso de herramientas de hardware o software para violar los controles de seguridad informática. A menos que se autorice por el área de sistemas.
- Ningún usuario o funcionario, debe probar o intentar probar fallas de la Seguridad Informática conocidas, a menos que estas pruebas sean controladas y aprobadas por el área de sistemas.
- No se debe intencionalmente escribir, generar, compilar, copiar, coleccionar, propagar, ejecutar o intentar introducir cualquier tipo de código (programa) conocidos como virus, gusanos o caballos de Troya, diseñado para auto replicarse, dañar o afectar el desempeño o acceso a las computadoras, redes o información de la entidad.

20. EQUIPOS DE TODAS LAS DEPENDENCIAS

La Alta Dirección deberá poner a disposición del área de sistemas, la información contractual de los equipos informáticos de Cómputo Escritorio, Portátil y periférica, así como de los servicios de soporte y mantenimiento.

- El área de sistemas será quien valide el cumplimiento de las Condiciones Técnicas de los equipos informáticos de Cómputo Escritorio, Portátiles y Periféricos adquiridos por la entidad.
- El almacenista o quien haga sus veces, tendrá bajo su resguardo las licencias de software, CD de software y un juego de manuales originales, así como un CD de respaldo para su instalación, mismos que serán entregados por la Alta dirección o el área usuaria de la licencia, para llevar el control de software instalado, para los equipos informáticos de cómputo Escritorio, Portátiles y periféricos al momento de la recepción de

los mismos, los cuales serán facilitados al responsable de sistemas en situaciones donde se requiera.

- Los requerimientos de Equipos Informáticos de Cómputo Escritorio, Portátiles y periféricos se llevarán a cabo mediante la solicitud y justificación por escrito, firmada por el Jefe del Área solicitante, lo cuales serán evaluados por el área de sistemas e inclusión en el Plan Anual de compras.
- La alta dirección y jefes de proceso, con apoyo del personal de sistemas, son encargados de tramitar las asignaciones, reasignaciones, bajas, etc. de equipos informáticos de cómputo Escritorio, Portátiles y periféricos ante el área encargada del Inventario para su ejecución, con base a las solicitudes realizadas al respecto y las revisiones de aprovechamiento de los mismos.
- El grupo de apoyo de sistemas elaborará y registrará en cada asignación o movimiento de equipos informáticos de cómputo Escritorio, Portátiles y periféricos, el documento denominado Hoja de vida de equipo, el cual contiene los datos generales del usuario y de los bienes informáticos entregados, así mismo, contendrá los datos de software instalado autorizado y configuración del equipo.
- Queda prohibido a los usuarios mover los equipos informáticos de cómputo Escritorio, Portátiles y periféricos por su propia cuenta, el usuario deberá solicitar al área de sistemas, el movimiento, así como informar la razón del cambio y en su caso, requerir la reasignación del equipo.
- Si algún equipo informático de cómputo Escritorio, Portátiles o periférico es trasladado por el usuario a oficinas distintas al lugar asignado, oficinas externas o foráneas para realizar sus labores, dicho bien estará bajo resguardo del responsable que retira el equipo y el pase de salida

quedará a consideración del jefe de proceso para su autorización y visto bueno.

- Las diferentes Áreas serán encargadas de proporcionar al área de sistemas, la relación de bienes y equipos que entrarán al proceso de baja, según corresponda. El área de sistemas realizará la evaluación técnica del equipo y definirá la reasignación o baja definitiva del bien que será informada al almacén para control de Inventarios de Activos por medio del procedimiento definido por el mismo.
- Queda prohibida la baja de equipo de cómputo que no cuente con evaluación técnica por parte del área de sistemas.
- El área de sistemas no es responsable de proporcionar asesoría técnica, mantenimiento preventivo o correctivo a equipo de cómputo de propiedad privada del usuario.
- El usuario que ingrese equipos de su propiedad a las instalaciones de la entidad es responsable de la información almacenada en el mismo, y deberá mantener la privacidad, integridad y respaldos de la misma sin ser esto responsabilidad del área de sistemas.
- Queda prohibido instalar software no autorizado o que no cuente con licencia, el responsable de sistemas deberá realizar las instalaciones de acuerdo con los estándares aquí establecidos.
- Es responsabilidad del usuario a quien esté asignado el equipo de escritorio o portátil, la información contenida en la misma.
- Cuando un usuario cambie de área, el equipo asignado a éste deberá permanecer dentro del área designada originalmente. Será responsabilidad de la nueva área en la que habrá de laborar el usuario, el proporcionarle equipo de cómputo para el desarrollo de sus funciones.

- En el caso de reinstalaciones de equipo, el usuario será el responsable de verificar que toda la información y archivos de trabajo estén contenidos en el equipo asignado, el usuario deberá firmar la Solicitud o Asignación del servicio proporcionado por el técnico o ingeniero asignado firmando de conformidad.
- El área de sistemas no es responsable de la configuración de dispositivos personales tales como Palms, IPOD y teléfonos celulares propiedad del usuario.
- El usuario que requiera la instalación de Software de su propiedad deberá solicitar por escrito al jefe del proceso, anexando copia de la licencia que compruebe su propiedad o en el caso de software libre el documento probatorio.

21. EVALUACIÓN

La Evaluación del Plan permite verificar el grado de cumplimiento de las acciones y metas definidas, así como analizar la efectividad de las medidas implementadas en materia de seguridad y privacidad de la información. Este componente es clave para la mejora continua, ya que facilita la identificación de oportunidades de ajuste y fortalecimiento del Plan.

La evaluación proporciona insumos para la toma de decisiones por parte de la alta dirección y contribuye a garantizar que el Plan se mantenga actualizado y alineado con las necesidades institucionales.

La estrategia del Plan de Seguridad y Privacidad de la Información se basa en la aplicación permanente de políticas, controles y buenas prácticas de seguridad informática, acompañadas de actividades de seguimiento, sensibilización y control, que permitan asegurar la protección de la información institucional.

11.1 ACTIVIDADES DEL PLAN

Actividad 1

- Monitorear y revisar periódicamente el cumplimiento de las políticas de seguridad de la información.

Actividad 2

- Gestionar y fortalecer los controles de acceso lógico y físico a la información institucional.

La medición de las actividades del Plan de Seguridad y Privacidad de la Información se realiza mediante indicadores de cumplimiento, debido a que corresponden a actividades permanentes de gestión y control, ejecutadas de manera continua por el área responsable.

La calificación se establece con base en el porcentaje de cumplimiento de las revisiones realizadas y la correcta gestión de los controles de acceso, lo cual permite evaluar de forma objetiva la aplicación de las políticas de seguridad de la información, garantizando la confidencialidad, integridad y disponibilidad de los activos de información de la entidad.

Actividad	Medición	Calificación
Monitoreo de políticas	% de revisiones realizadas	100%
Controles de acceso	% de accesos gestionados conforme a política	100%

22. BENEFICIOS

Permite identificar y comunicar los resultados positivos esperados derivados de la implementación del Plan de Seguridad y Privacidad de la Información. Estos beneficios no solo se reflejan en la protección de los activos de información, sino también en el fortalecimiento de la gestión institucional, la continuidad de los servicios y la confianza de los usuarios internos y externos.

Este componente evidencia el valor agregado del Plan para la entidad, demostrando su contribución al cumplimiento de los objetivos institucionales y a la mejora de los procesos administrativos y asistenciales.

23. MARCO NORMATIVO

El Plan de Seguridad y Privacidad de la Información se formula y ejecuta en cumplimiento del marco normativo vigente que regula la protección de la información, los datos personales, la seguridad digital y la gestión de las tecnologías de la información en las entidades públicas del sector salud. Este marco normativo establece los principios, lineamientos y obligaciones que orientan la adopción de medidas administrativas, técnicas y organizacionales para garantizar la confidencialidad, integridad, disponibilidad y privacidad de la información institucional.

El presente Plan se fundamenta en las disposiciones constitucionales, legales y reglamentarias que reconocen la información como un activo estratégico de la entidad y establecen la responsabilidad institucional frente a su adecuada gestión, protección y uso. Asimismo, el marco normativo asegura la alineación del Plan con los lineamientos de gobierno digital, control interno, gestión

documental y protección de datos personales, garantizando su coherencia con el Modelo Integrado de Planeación y Gestión (MIPG).

La observancia de este marco legal permite a la entidad fortalecer la confianza de los usuarios, prevenir incidentes de seguridad de la información, dar cumplimiento a los principios de legalidad y transparencia, y asegurar la continuidad de los servicios institucionales, especialmente aquellos relacionados con la atención en salud y la administración de información sensible.

24. NORMOGRAMA

El Normograma del Plan de Seguridad y Privacidad de la Información constituye una herramienta de apoyo que permite identificar, organizar y sistematizar las normas que regulan la seguridad, privacidad y protección de la información en la entidad. Su finalidad es facilitar la consulta normativa, asegurar la trazabilidad legal del Plan y evidenciar el cumplimiento de las disposiciones vigentes aplicables.

A través del normograma se establece la relación directa entre el Plan y las normas que lo soportan, permitiendo a los responsables de su implementación conocer las obligaciones legales asociadas a la gestión de la información, así como los lineamientos que orientan la adopción de controles y medidas de seguridad. Este instrumento contribuye a la adecuada gestión del riesgo legal y fortalece los procesos de auditoría, seguimiento y control institucional.

El normograma se estructura considerando el ámbito constitucional, legal, reglamentario y técnico, incorporando las normas que regulan la protección de datos personales, la seguridad digital, la gestión de tecnologías de la

información, el control interno y la gestión documental, con especial énfasis en las disposiciones aplicables al sector salud.

Tipo de Norma	Número / Año	Nombre de la Norma	Relación con el Plan
Constitución Política	1991	Constitución Política de Colombia – Art. 15	Reconoce el derecho fundamental al habeas data y a la protección de la información personal
Ley	1581 de 2012	Ley de Protección de Datos Personales	Establece principios y obligaciones para el tratamiento de datos personales
Decreto	1377 de 2013	Decreto reglamentario de la Ley 1581	Define responsabilidades y procedimientos para el tratamiento de datos
Ley	1712 de 2014	Ley de Transparencia y Acceso a la Información Pública	Regula el acceso, protección y reserva de la información
Decreto	1074 de 2015	Decreto Único Reglamentario del Sector Comercio	Compila normas sobre protección de datos personales
Decreto	1078 de 2015	Decreto Único Reglamentario TIC	Establece lineamientos sobre seguridad digital y gestión de TI
CONPES	3854 de 2016	Política Nacional de Seguridad Digital	Orienta la gestión de la seguridad digital en entidades públicas
Resolución	0256 de 2016	Ministerio de Salud y Protección Social	Regula el manejo de la información en el sector salud
Ley	1955 de 2019	Plan Nacional de Desarrollo	Incorpora lineamientos de gobierno digital y seguridad de la información
Modelo	MIPG	Modelo Integrado de Planeación y Gestión	Integra la seguridad de la información a la gestión institucional
Norma Técnica	ISO/IEC 27001	Sistema de Gestión de Seguridad de la Información	Referente técnico para la implementación de controles de seguridad

25. CONTROL DE REVISIONES

VERSIÓN	FECHA	COMENTARIO
01		Actualización

Elaborado por: **Nombre: EDWIN FABIAN CASTRO QUINTERO** **Cargo:** Ingeniero de Sistemas Agremiado **Firma:**	**Fecha:**
Revisado por **Nombre: JOHN DAVID VILLA** **Cargo:** Apoyo Dinámica Gerencial **Firma**	**Fecha:**
Revisado por **Nombre: DIEGO FERNANDO MOMPOTES** **Cargo:** Profesional Planeacion Agremiado **Firma**	**Fecha:**
Aprobado por: **Nombre: JOSÉ ANTONIO MUÑOZ PAZ** **Cargo:** Gerente **Firma**	**Fecha:**