






HOSPITAL REGIONAL DE II NIVEL DE SAN MARCOS ESE	Versión 1	Documento Controlado	Página 1 de 12
Plan de Seguridad y Privacidad de la Información	Fecha vigencia 31/12/2020	Código PL-GIC-01	

TABLA DE CONTENIDO

INTRODUCCION	2
OBJETIVO.....	2
OBJETIVOS ESPECIFICOS	2
ALCANCE	2
DIAGNOSTICO	5
PLANEACIÓN	5
IMPLEMENTACION	6
EVALUACION DE DESEMPEÑO	6
MEJORA CONTINUA.....	7
COMPROMISO DE LA ALTA DIRECCIÓN.....	8
ASIGNACIÓN DE RESPONSABILIDAD	8
ENFOQUE DEL MODELOS MSPI	8
PLAN DE COMUNICACIONES.....	9
ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	9
• USO DE Y DISPOSITIVOS MÓVILES.....	9
• Gestión de Activos de Información	9
• Acceso y Uso de la Información	10
• Manejo y Disposición de Información, Medios y Equipos	10
• Uso y protección de equipos de Cómputo	10
• Uso de Correo Electrónico.....	11
• Uso de Impresora y servicio de Impresión.....	11
• Uso de Internet	11
DEFINICIONES.....	3
BIBLIOGRAFIA	12
CRONOGRAMA.....	12
CONTROL DE LOS CAMBIOS	12

ELABORACIÓN	REVISIÓN	APROBACIÓN
 MIGUEL ANGEL RODRIGUEZ HERAZO Cargo	 LIDIA CENAIDA PEREZ CISNEROS Asesora para el proceso Financiero	 DUVER DICSON VARGAS ROJAS Agente Especial Interventor
Fecha: 31/12/2020	Fecha: 31/12/2020	Fecha: 31/12/2020



HOSPITAL REGIONAL DE II NIVEL DE SAN MARCOS ESE	Versión 1	Documento Controlado	Página 2 de 12
Plan de Seguridad y Privacidad de la Información	Fecha vigencia 31/12/2020	Código PL-GIC-01	

INTRODUCCION

El HOSPITAL REGIONAL DE II NIVEL DE SAN MARCOS viene realizando cambios significativos en la protección, seguridad e integridad de la información ya que este es el activo más importante para el desarrollo de las actividades diarias de la parte administrativa y asistencial, por lo busca establecer buenas políticas basadas en las normas establecidas por MINTIC y así brindar confianza a los usuarios del sistema de información de la institución los usuarios.

El presente documento identifica y recopila buenas prácticas para la gestión del ciclo de operación del modelo de seguridad y privacidad de la información, a partir de una evaluación de diagnóstico, planeación, implementación, gestión y mejora continua del mismo.

OBJETIVO

Presentar el plan de seguridad y privacidad de la información y los elementos que lo conforman, como marco de referencia para la entidad y regulación de lineamientos y medidas que permitan el aseguramiento de la protección y uso adecuado de la información y activos de información bajo la normatividad vigente de MinTic.

OBJETIVOS ESPECIFICOS

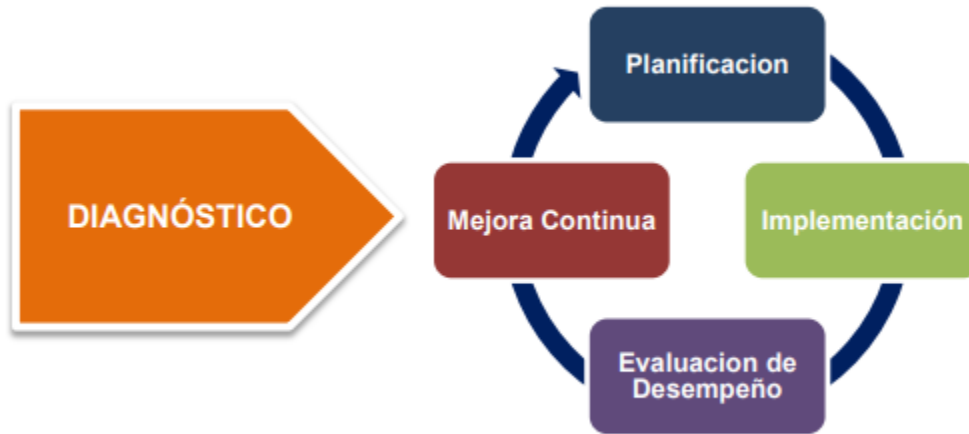
- Optimizar la gestión de la seguridad de la información al interior de la entidad
- Promover el uso de mejores prácticas de seguridad de la información, para ser la base de aplicación del concepto de Seguridad Digital.
- Definir políticas de seguridad el plan de seguridad de la información de la entidad.
- Proponer soluciones para minimizar los riesgos a lo que está expuesto cada activo
- Evaluar y comparar el nivel de riesgo actual, con el impacto generado después de implementado el plan de gestión y seguridad de la información.

ALCANCE

El presente documento identifica e incluye las orientaciones para la gestión del ciclo de operación del modelo de seguridad y privacidad de la información, el cual debe ser aplicado sobre todos los procesos de la Administración y de cumplimiento por parte de todos los servidores públicos con relación contractual.



HOSPITAL REGIONAL DE II NIVEL DE SAN MARCOS ESE	Versión 1	Documento Controlado	Página 3 de 12
Plan de Seguridad y Privacidad de la Información	Fecha vigencia 31/12/2020	Código PL-GIC-01	



Ciclo de operación Modelo de Seguridad y Privacidad de la Información

Tomado de: <http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html>

DEFINICIONES

Acceso a la Información Pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización. (ISO/IEC 27000).

Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)



HOSPITAL REGIONAL DE II NIVEL DE SAN MARCOS ESE	Versión 1	Documento Controlado	Página 4 de 12
Plan de Seguridad y Privacidad de la Información	Fecha vigencia 31/12/2020	Código PL-GIC-01	

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).

Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)

Bases de Datos Personales: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)

Información Pública Reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Datos Abiertos: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6)

Datos Personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

Datos Personales Públicos: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar



HOSPITAL REGIONAL DE II NIVEL DE SAN MARCOS ESE	Versión 1	Documento Controlado	Página 5 de 12
Plan de Seguridad y Privacidad de la Información	Fecha vigencia 31/12/2020	Código PL-GIC-01	

contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)

Datos Personales Privados: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)

Datos Personales Mixtos: Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

Datos Personales Sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)

SGSI: Siglas del Sistema de Gestión de Seguridad de la Información

MSPI: Modelo De Seguridad Y Privacidad De La Información

DIAGNOSTICO

En esta fase y mediante el uso de herramientas de diagnóstico, se desarrollan actividades de reconocimiento y valoración de gestión, cumplimiento de requisitos y lineamientos de seguridad de la información basado con el Modelo de Seguridad y Privacidad de Información de la estrategia de Gobierno Digital del Gobierno Nacional (u otros modelos de seguridad de la información aplicables y reconocidos), y de la implementación de controles de seguridad de la información con visión de mitigar riesgo asociado que pudiese generar un gran impacto indeseado en el hospital. El resultado de la evaluación de diagnóstico permitirá establecer el nivel de madurez del ciclo de operación del modelo de seguridad y privacidad de la información

PLANEACIÓN

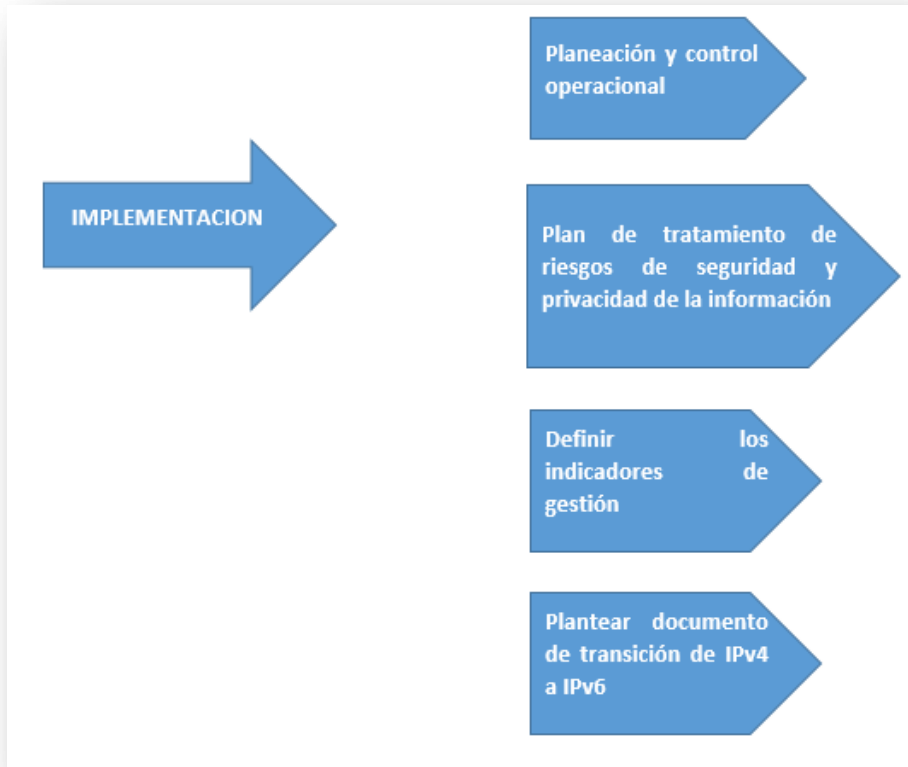
Para el desarrollo de esta fase y basado con el resultado de la evaluación de diagnóstico, se identificarán los aspectos claves que definan y orienten las actividades para los propósitos de seguridad y privacidad de la información, entre ellos, la justificación, el alcance, la política y los objetivos del Modelo de Seguridad y Privacidad de la Información (MSPI).



HOSPITAL REGIONAL DE II NIVEL DE SAN MARCOS ESE	Versión 1	Documento Controlado	Página 6 de 12
Plan de Seguridad y Privacidad de la Información	Fecha vigencia 31/12/2020	Código PL-GIC-01	

IMPLEMENTACION

En esta fase se busca la implementación de la fase de planificación del SGSI, teniendo en cuenta para esto los aspectos más relevantes en los procesos de implementación del Sistema de Gestión de Seguridad de la Información de la entidad.

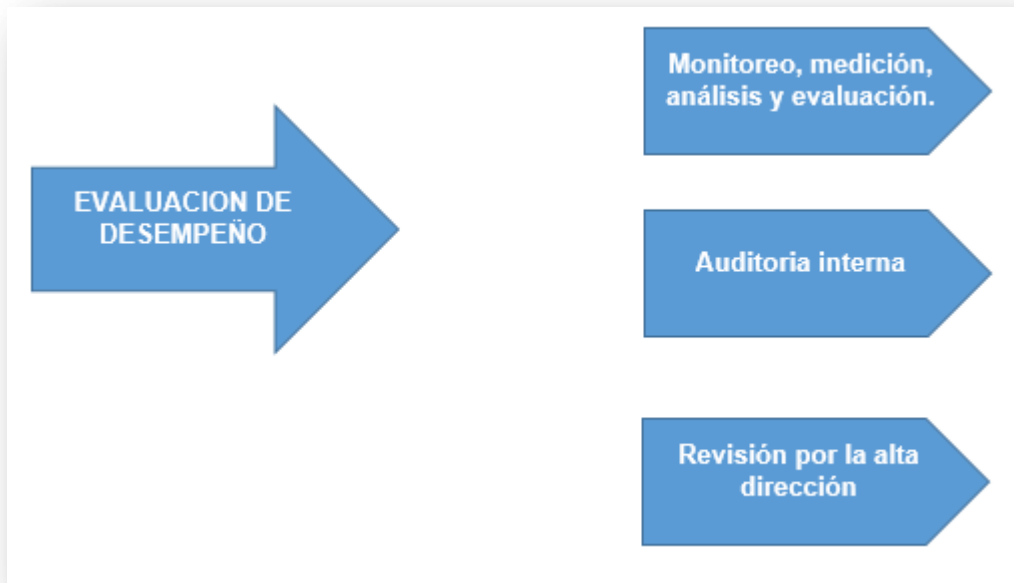


EVALUACION DE DESEMPEÑO

En esta fase se realizará seguimiento y monitoreo para evaluar el desempeño y la eficacia del SGSI, a través de instrumentos que permita determinar la efectividad de la implantación del SGSI para verificación de la efectividad, la eficiencia y la eficacia de las acciones implementadas.



HOSPITAL REGIONAL DE II NIVEL DE SAN MARCOS ESE	Versión 1	Documento Controlado	Página 7 de 12
Plan de Seguridad y Privacidad de la Información	Fecha vigencia 31/12/2020	Código PL-GIC-01	



MEJORA CONTINUA

En esta última fase la entidad debe buscar y consolidar los resultados obtenidos del componente de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, que permita realizar el plan de implementación de las acciones correctivas identificadas para el SGSI.



El plan de seguridad y privacidad de la información y lineamientos asociados, será de aplicabilidad e implementación para todos los procesos y aspectos administrativos y asistenciales, y de cumplimiento por parte de todos aquellos servidores públicos y terceros que presten sus servicios o tengan algún tipo de relación con el hospital. El alcance del MSPI permitirá definir los límites sobre los cuales se implementará la seguridad y privacidad de la información, por tanto, deberá tener en cuenta, los procesos que impactan directamente, procesos,



HOSPITAL REGIONAL DE II NIVEL DE SAN MARCOS ESE	Versión 1	Documento Controlado	Página 8 de 12
Plan de Seguridad y Privacidad de la Información	Fecha vigencia 31/12/2020	Código PL-GIC-01	

servicios, sistemas de información, ubicaciones físicas, terceros relacionados e interrelaciones del MSPI con otros procesos.

COMPROMISO DE LA ALTA DIRECCIÓN

El gerente debe aprobarla actualización de la política general de seguridad de la información como muestra de su compromiso y apoyo a las actividades de diseño, implementación, mantenimiento y mejora continua de políticas y lineamientos orientados a la guardar la confidencialidad, integridad y disponibilidad de la información de la Entidad. Este compromiso se verá reflejado a través de:

- La revisión y aprobación de políticas y lineamientos de seguridad de la información.
- La promoción de una cultura de seguridad y protección de la información.
- El apoyo para la divulgación de los propósitos y lineamientos de seguridad de la información a todo el personal que labora o que de una u otra manera tiene relación con el hospital.
- La asignación de los recursos necesarios para la implementación y mantenimiento del sistema de gestión de seguridad de la información.
- La realización de actividades de verificación y evaluación del desempeño del sistema de gestión de seguridad de la información de manera periódica.

ASIGNACIÓN DE RESPONSABILIDAD

La gerencia definirá una estructura de roles y asignará de manera formal la responsabilidad de la seguridad y privacidad de la información en diferentes niveles del hospital para permitir la adecuada y oportuna toma de decisiones enfocados al cumplimiento de los objetivos de seguridad y privacidad de la información (MSPI).

ENFOQUE DEL MODELOS MSPI

Este modelo va enfocado a todos los líderes de áreas y de procesos, los cuales deberán prestar su apoyo y responsabilidad para su aplicación. Grupos Internos de Trabajo, tales como Control Interno, Talento Humano, Jurídica, Planeación y demás áreas operativas y asistenciales, para promover y aplicar las políticas y demás lineamientos de las políticas de seguridad de la información, terceros, tales como entidades descentralizadas, auditores externos y entidades de regulación, quienes requieren de consultar nuestro sistema de información, en beneficio del cumplimiento de las obligaciones legales, contractuales y demás aplicables. Todos los funcionarios, contratistas, o partes interesadas, que presten sus servicios o tengan algún tipo de relación con el hospital, quienes deben ser informados de las responsabilidades de seguridad a través de los términos y condiciones o contratos laborales, procedimientos de seguridad y guías.



HOSPITAL REGIONAL DE II NIVEL DE SAN MARCOS ESE	Versión 1	Documento Controlado	Página 9 de 12
Plan de Seguridad y Privacidad de la Información	Fecha vigencia 31/12/2020	Código PL-GIC-01	

PLAN DE COMUNICACIONES

El hospital aplicará un plan de comunicaciones, de sensibilización y de capacitación que promueva estrategias para crear, incentivar y mantener una cultura de protección de la información en todos los niveles de la Entidad. El plan de comunicaciones de seguridad y privacidad de la información, y especialmente con respecto a actividades de socialización y sensibilización dirigida a los servidores públicos será ejecutado en conjunto con el apoyo del responsable de la oficina de Sistemas.

ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Se establecerá y liderará la gestión de seguridad de la información a través de la identificación de una estructura de roles y responsabilidades, que involucren las actividades de direccionamiento, implementación y control operacional en beneficio del cumplimiento de los propósitos de protección de la información y su mantenimiento eficaz a través del tiempo, así como de la conformación y asignación de responsabilidades pertinentes al sistema de gestión de seguridad de la información de la Entidad.

- **USO DE Y DISPOSITIVOS MÓVILES**

Teniendo en cuenta el alto grado riesgo que representa la información y los datos través del acceso y uso de dispositivos móviles de propiedad de terceros (teléfonos móviles, tabletas, portátiles, medios de almacenamiento USB); El Hospital autoriza el uso de dispositivos móviles para el acceso y uso a la información y datos de la Entidad, siempre y cuando, exista una relación contractual entre las partes y éstos sean utilizados para el apoyo al cumplimiento de sus responsabilidades y de los objetivos contractuales. Los usuarios de dispositivos móviles no estarán autorizados a cambiar la configuración de los equipos, a desinstalar software, formatear o restaurar configuraciones de fábrica; únicamente se deberá aceptar y aplicar actualizaciones.

- **Gestión de Activos de Información**

Todos aquellos activos de información del hospital incluida la información que sean sensibles para cumplimiento de la misión de la entidad, deberán contar con la asignación de protección de su confidencialidad, integridad y disponibilidad en concordancia con los resultados de una evaluación de riesgos y el nivel de exposición identificado. Activos de información de los procesos deberán ser identificados y administrados dentro de un inventario, al igual que valorados con respecto a su sensibilidad frente a impactos de afectación sobre la confidencialidad, integridad y disponibilidad de estos.



HOSPITAL REGIONAL DE II NIVEL DE SAN MARCOS ESE	Versión 1	Documento Controlado	Página 10 de 12
Plan de Seguridad y Privacidad de la Información	Fecha vigencia 31/12/2020	Código PL-GIC-01	

- **Acceso y Uso de la Información**

Todo trabajador o tercero del hospital entenderá y asumirá su responsabilidad de protección de la información a través de su acceso y uso apropiados.

Todo trabajador o tercero del hospital previo a recibir su usuario de acceso a los sistemas de información del hospital, deberá firmar y aceptar una declaración de responsabilidad sobre el uso y acciones realizadas con dichas cuentas.

Los usuarios no deberán almacenar información en discos duros de los equipos de cómputo o virtuales disponibles, archivos de video, música, fotos o cualquier tipo de archivo que no sea de carácter institucional.

- **Manejo y Disposición de Información, Medios y Equipos**

Se establecerán controles para evitar la divulgación, modificación, el retiro o la destrucción no autorizada de información almacenada en los medios proporcionados, velando por la disponibilidad y confidencialidad de la información. Los medios y equipos donde se almacena la información deberán mantenerse con las medidas de protección físicas y lógicas aplicables, se deberán generar planes de mantenimiento preventivo y correctivo que se requieran.

Para el retiro de equipos de cómputo por su estado de obsolescencia y/o daño, se deberá garantizar la aplicación del procedimiento de saneamiento, es decir llevar a cabo buenas prácticas para la eliminación y/o destrucción de la información con herramientas automáticas que aseguren que la misma no pueda en ningún caso ser recuperada.

Toda aquella información que por su obsolescencia se encuentre en medio físico papel y ésta no sea confidencial, deberá ser eliminada mediante la técnica de rasgado o picado mediante el uso de equipo especializado.

- **Uso y protección de equipos de Cómputo**

En equipo de cómputo de propiedad de los usuarios únicamente se podrá instalar y utilizar software o programas, sistemas de información, herramientas de software en equipos de cómputo de propiedad del hospital que sean licenciados y autorizados por el hospital.

Los equipos de cómputo no podrán ser utilizados para actividades de divulgación, propagación o almacenamiento de contenido personal o comercial de publicidad, promociones, ofertas, programas destructivos (virus), propaganda política, material religioso, o cualquier otro uso que no esté autorizado.



HOSPITAL REGIONAL DE II NIVEL DE SAN MARCOS ESE	Versión 1	Documento Controlado	Página 11 de 12
Plan de Seguridad y Privacidad de la Información	Fecha vigencia 31/12/2020	Código PL-GIC-01	

- **Uso de Correo Electrónico**

El hospital tendrá el derecho a realizar monitoreo o seguimiento del uso del correo electrónico a todos funcionarios y/o contratistas a quienes se les conceda una cuenta de correo corporativa.

No se podrá hacer uso de lenguaje ofensivo, inapropiado o con declaraciones de blasfemia, obscenidad, ilegales, incitadores a infringir la ley, hostigamiento basado en sexo, raza, nacionalidad, contenido despectivo o difamatorio en cualquier mensaje electrónico para con sus compañeros, clientes, proveedores u otros; su uso inadecuado, se considerará fuera del alcance y responsabilidad del hospital y por lo tanto, los daños y perjuicios que pueda llegar a causar, serán de completa responsabilidad de la propietario de la cuenta de correo electrónico que la haya generado.

Está prohibido utilizar el correo electrónico para el intercambio de información o de software que violen las leyes de derechos de autor.

Es responsabilidad de los usuarios de correo electrónico hacer mantenimiento a su buzón de correo: eliminar mensajes de la bandeja de entrada, archivar mensajes, Eliminar definitivamente los mensajes de la bandeja Elementos Eliminados.

- **Uso de Impresora y servicio de Impresión**

Los documentos que se impriman en las impresoras de hospital deberán ser de carácter institucional.

Las labores de reparación o mantenimiento de las impresoras son exclusivas de ejecución por parte del personal de sistemas y ningún funcionario o persona podrá realizar dicha actividad.

- **Uso de Internet**

El hospital se reserva el derecho de realizar monitoreo o seguimiento de los accesos a sitios en internet realizados por parte de los funcionarios públicos. Se permitirá el acceso a servicios de internet, con lineamientos que garanticen la navegación y uso controlados de componentes del servicio.

Se restringirá toda posibilidad de descarga de software no autorizado o código malicioso en los equipos de cómputo a través de internet, así mismo, el acceso y uso del servicio de internet se concederá solo para propósitos laborales o fines particulares definidos y aprobados por el hospital.

Se restringirá el acceso a sitios web dedicados a compartir material audiovisual fotos, videos, streaming tales como Facebook, Youtube.



HOSPITAL REGIONAL DE II NIVEL DE SAN MARCOS ESE	Versión 1	Documento Controlado	Página 12 de 12
Plan de Seguridad y Privacidad de la Información	Fecha vigencia 31/12/2020	Código PL-GIC-01	

No se permitirá el acceso a sitios web con contenidos que están en contra de la ley, principios de ética moral tales como, pornografía, terrorismo, contenidos obscenos, discriminación racial o similar.

BIBLIOGRAFIA

- <http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html>
- <https://www.mintic.gov.co/gestionti/615/articles>
- https://www.mintic.gov.co/gestionti/615/articles82_Modelo_de_Seguridad_Privacidad.pdf

CRONOGRAMA

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN																																																				
FASES	ENERO				FEBRERO				MARZO				ABRIL				MAYO				JUNIO				JULIO				AGOSTO				SEPTIEMBRE				OCTUBRE				NOVIEMBRE				DICIEMBRE							
I. FASE DIAGNOSTICO	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
II. FASE PLANIFICACION																																																				
III. FASE DE IMPLEMENTACION																																																				
IV. FASE DE EVALUACION DE DESEMPEÑO																																																				
V. MEJORA CONTINUA																																																				
VI. SEGUIMIENTO Y CONTROL																																																				

CONTROL DE LOS CAMBIOS

FECHA	VERSIÓN	DESCRIPCIÓN DEL CAMBIO