



HOSPITAL REGIONAL DE II NIVEL DE SAN MARCOS ESE	Versión 1	Documento Controlado	Página 1 de 9
Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información	Fecha vigencia 31/12/2020	Código PL-GIC-02	

TABLA DE CONTENIDO

OBJETIVO..... 2

OBJETIVOS ESPECIFICOS 2

ALCANCE 2

DEFINICIONES..... 2

ROLES Y RESPONSABLES..... 4

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN..... 5

MEDICIÓN DE RIESGO 6

PROPUESTA DE SEGURIDAD..... 6

PLAN SEGURO PARA EL ACOPIO DE COPIAS DE SEGURIDAD..... 7




MARCO LEGAL 7

REQUISITOS TÉCNICOS..... 8

SEGUIMIENTO Y EVALUACIÓN..... 8

CRONOGRAMA..... 9

CONTROL DE LOS CAMBIOS 9

ELABORACIÓN	REVISIÓN	APROBACIÓN
 MIGUEL ANGEL RODRIGUEZ HERAZO Ingeniero de Sistemas	 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 9
Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información	Fecha vigencia 31/12/2020	Código PL-GIC-02	

OBJETIVO

Desarrollar un plan de gestión de seguridad y privacidad que permita minimizar los riesgos de pérdida de activos de la información

OBJETIVOS ESPECIFICOS

Identificar las potenciales amenazas o vulnerabilidades asociadas a los activos de información.

Concientizar a todos los colaboradores, áreas, procesos, proveedores, externos en general sobre la necesidad e importancia de gestionar de manera adecuada, los riesgos inherentes a la gestión.

Proteger los activos de información para disminuir los impactos generados ante posibles amenazas.

Definir estrategias de seguridad que establezca planes para la clasificación de los activos de información.

Realizar acciones de mejora para los activos clasificados como altamente críticos. Mejorar el nivel de exposición de los activos de información para eliminar o minimizar el riesgo dentro de la institución.

Evaluar y comparar el nivel de riesgo actual con el impacto generado después de implementar el plan de gestión de seguridad de la información.

Involucrar y comprometer a todos en la formulación e implementación de controles y acciones encaminadas a prevenir y administrar los riesgos.

ALCANCE

Capacitar al personal del Hospital Regional De II Nivel de San Marcos en el proceso de plan de gestión del riesgo de la seguridad de la información y la ciudadanía en general que tengan acceso a la información de la institución

DEFINICIONES

Para la administración del riesgo, se tendrán en cuenta los siguientes términos y definiciones:

- **Activos de información:** Los activos de información son los recursos que utiliza un Sistema de Gestión de Seguridad de la Información para que las organizaciones **funcionen y consigan los objetivos** que se han propuesto por la alta dirección.
- **Alcance del SGSI:** ámbito de la organización que queda sometido al SGSI, incluyendo una identificación clara de las dependencias, relaciones y límites que existen entre el alcance y aquellas partes que no hayan sido



HOSPITAL REGIONAL DE II NIVEL DE SAN MARCOS ESE	Versión 1	Documento Controlado	Página 3 de 9
Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información	Fecha vigencia 31/12/2020	Código PL-GIC-02	

consideradas (en aquellos casos en los que el ámbito de influencia del SGSI considere un subconjunto de la organización como delegaciones, divisiones, áreas, procesos, sistemas o tareas concretas).

- **Análisis del riesgo:** Uso sistemático de la información para identificar las fuentes y estimar el riesgo. (Guía ISO/IEC 73:2002)
- **Confidencialidad:** propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados. (NTC 5411-1:2006)
- **Evaluación de riesgos:** Proceso de comparar el riesgo estimado contra el criterio de riesgo dado con el objeto de determinar la importancia del riesgo. (ISO/IEC Guía 73:2002)
- **Evento de seguridad de la información:** presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad. (ISO/IEC TR 18044:2004)
- **Enfoque de evaluación de riesgos:** descripción de la metodología a emplear (cómo se realizará la evaluación de las amenazas, vulnerabilidades, probabilidades de ocurrencia e impactos en relación a los activos de información contenidos dentro del alcance seleccionado), desarrollo de criterios de aceptación de riesgo y fijación de niveles de riesgo aceptables. (www.ISO27000.es)
- **Gestión del riesgo:** actividades coordinadas para dirigir y controlar una organización en relación con el riesgo. (Guía ISO/IEC 73:2002)
- **Incidente de seguridad de la información:** Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información. (ISO/IEC TR 18044:2004)
- **Informe de evaluación de riesgos:** estudio resultante de aplicar la metodología de evaluación anteriormente mencionada a los activos de información de la organización. (www.ISO27000.es)
- **Integridad propiedad:** Salvaguardar la exactitud y estado completo de los activos. (NTC 5411-1:2006)



HOSPITAL REGIONAL DE II NIVEL DE SAN MARCOS ESE	Versión 1	Documento Controlado	Página 4 de 9
Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información	Fecha vigencia 31/12/2020	Código PL-GIC-02	

- **ISO/IEC 27001:** ISO/IEC 27001 es un reconocido marco internacional de las mejores prácticas para un sistema de gestión de seguridad de la información. Le ayuda a identificar los riesgos para su información importante y pone en su lugar los controles apropiados para ayudarlo a reducir el riesgo. (ISO/IEC 27001)
- **Manual de seguridad:** por analogía con el manual de calidad, aunque el término se usa también en otros ámbitos. Sería el documento que inspira y dirige todo el sistema, el que expone y determina las intenciones, alcance, objetivos, responsabilidades, políticas y directrices principales, etc., del SGSI. (www.ISO27000.es)
- **Procedimientos:** documentos en el nivel operativo, que aseguran que se realicen de forma eficaz la planificación, operación y control de los procesos de seguridad de la información. . (www.ISO27000.es)
- **Riesgo residual:** nivel restante de riesgo después del tratamiento del riesgo. [Guía ISO/IEC 73:2002]
- **Seguridad de la información:** Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad (Accountability), no repudio y fiabilidad. (NTC-ISO/IEC 17799:2006)
- **SGSI:** Es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Information Security Management System. (WWW.ISO27000.ES)
- **Tratamiento del riesgo:** proceso de selección e implementación de medidas para modificar el riesgo. (Guía ISO/IEC 73:2002)

ROLES Y RESPONSABLES

El éxito de la administración del riesgo depende de la decidida participación de los directivos, servidores públicos y contratistas; por esto, es preciso identificar los actores que intervienen:

- **Alta Dirección:** aprueban las directrices para la administración del riesgo en la Entidad. La Alta Dirección es la responsable del fortalecimiento de la política de administración del riesgo.



HOSPITAL REGIONAL DE II NIVEL DE SAN MARCOS ESE	Versión 1	Documento Controlado	Página 5 de 9
Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información	Fecha vigencia 31/12/2020	Código PL-GIC-02	

• **Proceso Administración del Sistema Integrado de Gestión:** Genera la metodología para la administración del riesgo de la Entidad, coordina, lidera, capacita y asesora en su aplicación.

• **Responsables de los procesos:** Identifican, analizan, evalúan y valoran los riesgos de la entidad (por procesos e institucionales) al menos una vez al año. Si bien los Líderes SIG apoyan la ejecución de las etapas de gestión del riesgo a nivel de los procesos, esto no quiere decir que el proceso de administración de riesgos este solo bajo su responsabilidad. Al contrario, cada responsable de proceso se encarga de garantizar que en el proceso a su cargo se definan los riesgos que le competen, se establezcan las estrategias y responsabilidades para tratarlos y, sobre todo, que se llegue a cada funcionario que trabaja en dicho proceso.

• **Servidores públicos y contratistas:** ejecutar los controles y acciones definidas para la administración de los riesgos definidos, aportar en la identificación de posibles riesgos que puedan afectar la gestión de los procesos y/o de la entidad.

• **Control Interno:** debe realizar evaluación y seguimiento a la política, los procedimientos y los controles propios de la administración de riesgos

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Hospital Regional de II Nivel de San Marcos, mediante el plan de tratamiento de riesgos de seguridad y privacidad de la información buscará identificar y evaluar los riesgos e incidentes que puedan afectar a la institución. Aunque la protección de la información digital se ve amenazada frecuentemente por errores cometidos por los usuarios, en la ESE Hospital Regional de II Nivel de San Marcos se encontraron otras amenazas e impactos como los siguientes:

- Los puntos de red ubicados en cada oficina no son suficientes y se debe realizar estudio de necesidad para mejorar. No existe una estructura o protocolo fijo y establecido para la infraestructura física del hospital.
- Algunos cables de energía están sueltos, no están cerca a los escritorios o no son suficientes para la cantidad de equipos que tiene cada oficina, existe riesgo de pérdida de información en el caso que sean desconectados por accidente.
- Bebidas y alimentos cerca a los equipos de cómputo, poniendo en riesgo todos los equipos y sufrir un corto circuito.
- Existe un riesgo de pérdida de información por falta de equipos en algunas áreas.



HOSPITAL REGIONAL DE II NIVEL DE SAN MARCOS ESE	Versión 1	Documento Controlado	Página 6 de 9
Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información	Fecha vigencia 31/12/2020	Código PL-GIC-02	

- La información es llevada en memorias o discos duros portátiles personales, por ende, la información sale de la entidad corriendo riesgo de pérdida de información.
- Los documentos físicos que se manejan en la entidad no se han digitalizado por lo tanto están expuestos a pérdidas y daños físicos debido a que los sitios de almacenamiento en las oficinas no son los adecuados.

MEDICIÓN DE RIESGO

Según la siguiente escala se busca hacer la medición de los riesgos

Escala para calificar la probabilidad del riesgo		
Nivel	Concepto	Frecuencia
Raro	El evento puede ocurrir solo en circunstancias excepcionales.	No se ha presentado en los últimos 5 años.
Improbable	El evento puede ocurrir en algún momento.	Al menos de 1 vez en los últimos 5 años.
Moderado	El evento podría ocurrir en algún momento.	Al menos de 1 vez en los últimos 2 años.
Probable	El evento probablemente ocurrirá en la mayoría de las circunstancias.	Al menos de 1 vez en el último año.
Casi certeza	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.

PROPUESTA DE SEGURIDAD

- Revisar, organizar y ubicar las conexiones de electricidad según las necesidades propias de las oficinas.
- Establecer políticas de seguridad y privacidad de la información como también las políticas de seguridad informática.
- Implementar y socializar las políticas de seguridad y privacidad de la información con el personal del hospital.
- Implementar el sistema de documentación digital en el hospital para reducir riesgos de pérdida de información física.
- Habilitar el software para digitalización de documentos y gestión documental en los próximos meses.



HOSPITAL REGIONAL DE II NIVEL DE SAN MARCOS ESE	Versión 1	Documento Controlado	Página 7 de 9
Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información	Fecha vigencia 31/12/2020	Código PL-GIC-02	

PLAN SEGURO PARA EL ACOPIO DE COPIAS DE SEGURIDAD

Realizar diario Back-up del sistema de información para mitigar el riesgo de pérdida de información, ante un daño de software o hardware.

Guardar en un equipo periférico los Back-up.

Dejar en custodia equipo periférico donde se almacena el Back-up.

Almacenar un Back-up por lo menos una vez en la semana en una nube.

Contar con un plan alternativo que asegure la continuidad de la actividad del negocio en caso que ocurran incidentes graves.

MARCO LEGAL

Decreto 612 de 4 abril de 2018, “Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las Entidades del Estado”.

Decreto 1008 de 14 de junio de 2018, “Por el cual se establecen los lineamientos generales de la política de Gobierno Digital”.

Ley 594 de 14 de julio 2000, “Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones”.

Decreto 1078 del 26 de mayo 2015, “Por medio del cual se expide el Decreto único reglamentario del sector de tecnologías de la información y las comunicaciones”.

Acuerdo 003 del 17 de febrero de 2015, “Por el cual se establecen lineamientos generales para las entidades del Estado en cuanto a la gestión de documentos electrónicos generados como resultado del uso de medios electrónicos de conformidad con lo establecido en el capítulo IV de la Ley 1437 de 2011, se reglamenta el artículo 21 de la Ley 594 de 2000 y el capítulo IV del Decreto 2609 de 2012”.

Decreto 1083 del 26 de mayo 2015, “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública”.



HOSPITAL REGIONAL DE II NIVEL DE SAN MARCOS ESE	Versión 1	Documento Controlado	Página 8 de 9
Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información	Fecha vigencia 31/12/2020	Código PL-GIC-02	

Ley 1474 del 12 de julio de 2011, “Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.”

REQUISITOS TÉCNICOS

Norma técnica colombiana NTC-ISO/IEC 27000 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. (SGSI). Visión General y Vocabulario

Norma técnica colombiana NTC-ISO/IEC 27001 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la seguridad de la información (SGSI). Requisitos

Guía 7 gestión de riesgos. Modelo de seguridad y privacidad de la información. Ministerio de Tecnologías de la información y las Comunicaciones, estrategias de Gobierno en Línea.

Guía 8 controles de seguridad y privacidad de la información. Modelo de seguridad y privacidad de la información. Ministerio de Tecnologías de la información y las Comunicaciones, estrategias de Gobierno en Línea.

Guía para la administración de riesgos en seguridad de la información. DNP. Departamento Nacional de Planeación.

SEGUIMIENTO Y EVALUACIÓN

Periódicamente deben revisarse los activos, impactos, amenazas, vulnerabilidades, cambios, que exijan valoración de los riesgos de seguridad de la información.

Es necesaria una supervisión activa que permita detectar nuevas amenazas, nuevas vulnerabilidades, nuevos impactos, mediante esquemas de seguimiento y medición al sistema de gestión y seguridad de la información.

