***LA VERSIÓN DIGITAL Y ORIGINAL DE ESTE DOCUMENTO SE ENCUENTRA BAJO CUSTODIA DE LA OFICINA ASESORA DE PLANEACIÓN Y CALIDAD, LA LEGALIZACION DE ESTE DOCUMENTO SE REALIZA MEDIANTE LA IMPRESIÓN Y FIRMA DE LA PRIMERA HOJA DE DICHA VERSION; LA PRESENTE ES UNA COPIA IDÉNTICA DE LA ORIGINAL Y ES UN DOCUMENTO COPIA CONTROLADA DE CONSULTA.***

***LA OFICINA DE PLANEACIÓN Y CALIDAD ES RESPONSABLE DE PUBLICAR LAS ACTUALIZACIONES REALIZADAS POR EL PROCESO.***



*ESTA APROBACION SE REALIZA CONFORME SE DESCRIBE EN EL DOCUMENTO: "PC-PR-007 PROCEDIMIENTO PARA LA ELABORACIÓN Y CONTROL DE LOS DOCUMENTOS DEL MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN".*

## TABLA DE CONTENIDO

## INTRODUCCION

Nos encontramos inmersos en la denominada revolución digital, en donde se reconoce el protagonismo de la información en los procesos del Hospital, por tanto, la importancia de tener la información adecuadamente identificada y protegida, ya que es uno de los activos más importantes.

La información de las entidades públicas es vital dentro de la política pública y su relación con el ciudadano.

La seguridad de la información tiene como objetivo proteger los activos ante el conjunto de amenazas que se puedan presentar relacionadas con confidencialidad, integridad y disponibilidad. Esto se realiza implementando medidas de control que permitan gestionar y reducir los riesgos a los cuales está expuesta la institución.

Debemos generar una cultura de prevención contra los riesgos a los que día a día se pueden ver sometidos los activos de información.

Dentro del Marco de Seguridad y Privacidad de la Información un tema decisivo es la gestión de riesgos, considerando la Guía de Riesgos de la función pública.

## 1. OBJETIVOS

### 1.1 Objetivo General

Controlar y minimizar los riesgos asociados a los procesos del Hospital, con el fin de proteger los activos de información.

### 1.2 Objetivos Específicos

Realizar un plan de trabajo de acuerdo a los recursos con que se cuentan actualmente para la elaboración del Plan de tratamiento de riesgos de seguridad y privacidad de la información

Administrar los riesgos y minimizar su impacto de los riesgos mediante acciones que permitan controlarlos.

Proteger los activos de información mediante implementación de acciones adecuadas acordes al entorno del Hospital.

## 2. AMBITO DE APLICACIÓN

El ámbito de aplicación del Plan de Tratamiento de Riesgos de SPI cubre las necesidades que en materia de seguridad de la información tienen las dependencias del Hospital sobre cada uno de sus procesos, entregando valor a través de las soluciones y servicios correspondientes.

## 3. RESPONSABLE

El responsable de este documento es el coordinador de Tecnologías de la Información o quien haga sus veces.

## 4. DEFINICIONES

**Activo de información:** Los activos son los recursos del Sistema de Seguridad de la Información ISO 27001, necesarios para que la empresa funciones y consiga los objetivos que se ha propuesto la alta dirección. (SGSI, 2017)

**Administración del Riesgo:** La administración de riesgos se puede definir entonces como el proceso de identificación, medida y administración de los riesgos que

amenazan la existencia, los activos, las ganancias o al personal de una organización, o los servicios que ésta provee. (Auditool, 2016)

**Análisis de Riesgos:** Estudio que debe hacerse, con el fin de identificar los activos críticos de los sistemas de información que dan soporte a los procesos de negocio de nuestra organización y las amenazas que puede comprometer su disponibilidad, integridad o confidencialidad. (Openwebinar, 2020)

**Amenaza:** Una amenaza se refiere a un incidente nuevo o recién descubierto que tiene el potencial de dañar un sistema o empresa en general. (Hostdime, 2020)

**Confidencialidad:** Por confidencialidad entendemos la cualidad de la información para no ser divulgada a personas o sistemas no autorizados. Se trata básicamente de la propiedad por la que esa información solo resultará accesible con la debida y comprobada autorización. (Firma-e, 2014)

**INTEGRIDAD:** Hace referencia a la cualidad de la información para ser correcta y no haber sido modificada, manteniendo sus datos exactamente tal cual fueron generados, sin manipulaciones ni alteraciones por parte de terceros. Esta integridad se pierde cuando la información se modifica o cuando parte de ella se elimina, y una gran garantía para mantenerla intacta es, como hemos mencionado en anteriores ocasiones, la firma digital. (Firma-e, 2014)

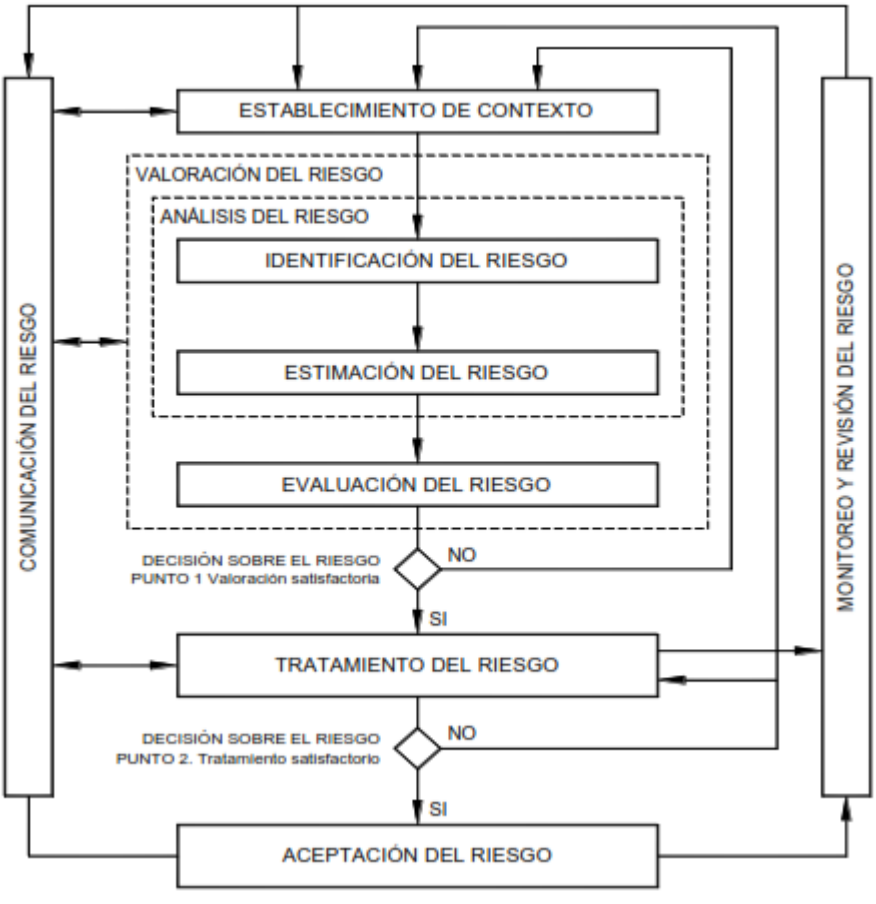
**DISPONIBILIDAD:** Pilar de la Seguridad de la Información. Por disponible entendemos aquella información a la que podemos acceder cuando la necesitamos a través de los canales adecuados siguiendo los procesos correctos. (Firma-e, 2014)

**Riesgo:** El riesgo es la probabilidad de que una amenaza se convierta en un desastre. La vulnerabilidad o las amenazas, por separado, no representan un peligro. Pero si se juntan, se convierten en un riesgo, o sea, en la probabilidad de que ocurra un desastre. (Unisdr, 2015)

## 5. NORMAS

La seguridad Informática y la seguridad de la información son métodos y técnicas físicas y documentales empleadas para mantener siempre la confidencialidad, integridad y disponibilidad de la información. La Norma ISO 27001 describe cómo implementar el sistema de gestión de seguridad de la información de una empresa y es la Normas sobre la cual el Hospital se basará para el manejo de los riesgos de seguridad y que junto con la Norma ISO 27005 se apoya para la gestión de los riesgos de la seguridad de la información


## 6. VISION GENERAL DEL PROCESO DE GESTION DE RIESGOS



El proceso de gestión del riesgo en la seguridad de la información puede ser iterativo para las actividades de valoración del riesgo y/o el tratamiento de este.

### 6.1. Establecimiento de contexto de riesgos

Se define el contexto a través de la identificación de las fuentes que pueden dar origen a los riesgos en los procesos y las amenazas asociadas, su valoración, su probabilidad de ocurrencia. Involucra a todos los procesos del Hospital.

Deben manejarse criterios de evaluación del riesgo, criterios de impacto, y criterios de aceptación del riesgo.

### 6.2. Criterios de Evaluación del riesgo

- Se enfoca en el valor estratégico de la información del Hospital.
- La criticidad de los activos de información involucrados
- Los requisitos legales y reglamentarios
- La importancia de la disponibilidad, confidencialidad e integridad de la información para las operaciones del Hospital.
- Las expectativas y percepciones de las partes interesadas y las consecuencias negativas para el buen nombre y reputación de la entidad.

### 6.3. Criterios de Impacto

Se especifican en términos de grado, daño, costos del Hospital, causados por un evento de seguridad de la información. Se consideran los siguientes aspectos:

- Nivel de clasificación de los activos de información de los procesos
- Brechas en la seguridad de la información (ejemplo: perdidas de confidencialidad, integridad y disponibilidad de la información)
- Operaciones deterioradas
- Perdida del negocio y del valor financiero
- Alteración de planes y fechas limites
- Daños para la reputación
- Incumplimiento de los requisitos legales reglamentarios o contractuales.

### 6.4. Criterios de Aceptación del Riesgo

Estos criterios dependen con frecuencia de las políticas, metas, objetivos de la organización y de las partes interesadas.

Las escalas de aceptación de los riesgos de seguridad pueden tomarse del manual de administración del riesgo y el diseño de controles.

## 7. Metodología PHVA

Las actividades de gestión del riesgo en la seguridad de la información para las cuatro fases del proceso de Modelo de seguridad y privacidad de la información, toma como base la metodología PHVA y los lineamientos emitidos por Mintic.

| ETAPAS DEL MSPI | PROCESO DE GESTION DEL RIESGO EN LA SEGURIDADDE LA INFORMACION |
|---|---|
| **Planear** | Establecer Contexto<br>Valoración del Riesgo<br>Planificación del Tratamiento del Riesgo<br>Aceptación del Riesgo |
| **Implementar** | Implementación del Plan de Tratamiento de Riesgo |
| **Gestionar** | Monitoreo y Revisión Continuo de los Riesgos |
| **Mejora Continua** | Mantener y Mejorar el Proceso de Gestión del Riesgo en la Seguridad de la Información. |

## 8. Valoración de los riesgos de seguridad de la información

### 8.1. Identificación del Riesgo

Se identifican los inventarios de activos de información de los procesos, como base del enfoque de valoración de los riesgos de seguridad de la información.

| | |
|---|---|
| **Hardware** | Equipos físicos de cómputo y de comunicaciones como, servidores, biométricos que por su criticidad son considerados activos de información |
| **Servicios** | Servicio brindado por parte de la entidad para el apoyo de las actividades de los procesos, tales como: Servicios WEB, intranet, CRM, ERP, Portales organizacionales, Aplicaciones entre otros (Pueden estar compuestos por hardware y software) |
| **Intangibles** | Se consideran intangibles aquellos activos inmateriales que otorgan a la entidad una ventaja competitiva relevante, uno de ellos es la imagen corporativa, reputación o el good will, entre otros |
| **Componentes de red** | Medios necesarios para realizar la conexión de los elementos de hardware y software en una red, por ejemplo, el cableado estructurado y tarjetas de red, routers, switches, entre otros |
| **Personas** | Aquellos roles que, por su conocimiento, experiencia y criticidad para el proceso, son considerados activos de información, por ejemplo: personal con experiencia y capacitado para realizar una tarea específica en la ejecución de las actividades |
| **Instalaciones** | Espacio o área asignada para alojar y salvaguardar los datos considerados como activos críticos para la empresa |

**Fuente:** Ministerio de Tecnologías de la Información y las Comunicaciones

**Tabla 4.** Tipología de Activos:

| Tipo de activo | Descripción |
|---|---|
| **Información** | Información almacenada en formatos físicos (papel, carpetas, CD, DVD) o en formatos digitales o electrónicos (ficheros en bases de datos, correos electrónicos, archivos o servidores), teniendo en cuenta lo anterior, se puede distinguir como información: Contratos, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, registros contables, estados financieros, archivos ofimáticos, documentos y registros del sistema integrado de gestión, bases de datos con información personal o con información relevante para algún proceso (bases de datos de nóminas, estados financieros) entre otros. |
| **Software** | Activo informático lógico como programas, herramientas ofimáticas o sistemas lógicos para la ejecución de las actividades |

Se identifican las amenazas que pueden causar daños en la información

## 8.2. Análisis del Riesgo

Se identifican las causas y las consecuencias que podrían afectar la confidencialidad, integridad, y disponibilidad de la información.

La estimación del riesgo con su valoración

| PROBABILIDAD DE OCURRENCIA | |
|---|---|
| Casi seguro | 5 |
| Probable | 4 |
| Posible | 3 |
| Improbable | 2 |
| Rara vez | 1 |

Este análisis debe realizarse para cada uno de los procesos de acuerdo a la experiencia para que puedan determinar el impacto y la probabilidad del riesgo.

El impacto del riesgo hace referencia a las consecuencias que pueden ocasionar al Hospital la materialización del riesgo, o magnitud de sus efectos.

| IMPACTO | |
|---|---|
| Catastrofico | 5 |
| Mayor | 4 |
| Moderado | 3 |
| Menor | 2 |
| Insignificante | 1 |

## 8.3. Valoración

Se definen los controles existentes, la solidez del control, el análisis del riesgo determinado por su probabilidad e impacto, y el nivel de riesgo residual

**SOLIDEZ DEL CONTROL**

| |
|---|
| FUERTE |
| MODERADO |
| DEBIL |

El nivel de riesgo inherente, que permite analizar de manera global los riesgos que deben priorizarse según la zona en que queden ubicados:

**NIVEL DE RIESGO**

| |
|---|
| EXTREMA |
| ALTA |
| MODERADA |
| BAJA |

## 8.4. Manejo

Los riesgos son dinámicos y pueden cambiar sin previo aviso Se tiene una lista con el nivel de evaluación de los riesgos y mirar cual es el manejo que se le va a dar a cada uno de ellos:

**OPCIONES DE MANEJO**
Aceptar el Riesgo
Reducir el Riesgo
Evitar el Riesgo
Compartir el Riesgo

Deben definirse las actividades dependiendo de la opción de manejo que se defina, cuál va a ser el soporte o evidencia para su manejo el responsable y el plazo de ejecución.

Durante esta vigencia se evaluará el nivel de impacto vs. Probabilidad y los controles existentes para calcular el nivel de riesgo para el Hospital

## 8.5. Riesgos identificados en el Hospital

A continuación, se especifican algunos riesgos identificados que pueden llegar afectar la confidencialidad, integridad y disponibilidad de la información en el Hospital.

La identificación de los riegos se ha realizado con observación directa, ingeniería social y con el análisis a los equipos de seguridad perimetral:

| RIESGOS INFORMÁTICOS | CAUSAS | EFECTO |
|---|---|---|
| **Perdida de Información** | -Fallas en el proceso de copia de respaldo o de restauración de la información, o pérdida de esta.<br><br>-Fallas en los análisis y socialización de las vulnerabilidades de la infraestructura de IT<br><br>-Ingreso a la red y acceso a los activos de TI por parte de PCs ajenos al Hospital.<br><br>-Habilitación de puertos USB en modo lectura y escritura para medios de almacenamiento<br><br>-Ataques cibernéticos internos o externos<br><br>-No cerrar sesión cuando se retira del puesto.<br><br>-Acceso no autorizado a las dependencias.<br><br>-Conectar dispositivos externos a los equipos. | -Afectación parcial o total de la continuidad de las operaciones de los servicios<br><br>-Mala imagen, multas, sanciones y pérdidas económicas<br><br>-Generación de consultas, funcionalidades o reportes con información sensible de los clientes<br><br>-Pérdida o fuga de información |

| | | |
|---|---|---|
| | -Falta de implementación de la política escritorio limpio | |
| **Correos electrónicos de extraña procedencia** | - No generar una Cultura de Seguridad de la Información<br>- Falta de Filtros en el Servidor de Correo | -Monitoreo de las actividades realizadas en el equipo.<br><br>-Ataque remoto mediante un troyano o gusano.<br>Robo de contraseñas. |
| **Daño en los equipos tecnológicos** | Manejo inadecuado de los equipos<br><br>Falta de mantenimiento o mala conexión de estos en las instalaciones.<br><br>Falta de equipos de energía regulada | -Perdida de información<br><br>-Perdidas de los equipos informáticos<br><br>- Indisponibilidad del Servicio |

| | | |
|---|---|---|
| | Fallas por obsolescencia tecnológica<br><br>Derrame de líquido<br><br>Falta de ambiente adecuado para los equipos<br><br>Falta Educación a los usuarios en el manejo de los equipos de computo | - Traumatismos en los procesos |
| **Perdida de Conectividad** | -Daño externo del ISP (Internet service provider)<br><br>-Ataque DDoS o DOS (Denegación de servicios distribuidos o Denegación de servicios) | |

| | | |
|---|---|---|
| **Ataques Informáticos** | -Estimulo o Reto personal<br>-Rebelión<br>-Ánimo de lucro<br>-Espionaje | -Daño en los equipos tecnológicos<br>-incidente en la confidencialidad, integridad y disponibilidad de la información<br>-Denegación de servicios<br>-Secuestro de la información<br>-Divulgación ilegal de la información<br>-Suplantación de identidad<br>-Destrucción de la información |

## 8.6 Amenazas

| AMENAZA | TIPO |
|---|---|
| Polvo, Corrosión | Evento Naturales |
| Pandemia | Evento Naturales |
| Incendios | Evento Naturales |
| Fenómenos Sísmicos | Evento Naturales |
| Fenómenos Térmicos | Evento Naturales y Daños físicos |
| Perdida en el suministro de energía | Daño Físico |
| Ingeniería Social | Acciones no autorizadas |
| Intrusión | Acciones no autorizadas |
| Accesos forzados al sistema | Acciones no autorizadas |
| Manipulación del Hardware | Acciones no autorizadas |
| Manipulación con Software | Acciones no autorizadas |
| Fallas del equipo | Fallas técnicas |
| Saturación del sistema de información | Fallas técnicas |

## 8.7. Vulnerabilidades

| VULNERABILIDADES | DESCRIPCIÓN |
|---|---|
| **Fácil acceso a las dependencias** | No existe un control para el acceso de las personas no autorizadas adecuado |
| **Falta de dispositivos de seguridad biométrica para acceso** | El dispositivo de seguridad biométrica reduce el riesgo de robo de información o equipos electrónicos por fácil acceso. |
| **Falta de Aplicación de la Política de escritorio Limpio.** | La política de escritorio limpio, debe |

| | |
|---|---|
| | implementarse para que los funcionarios no dejen expuestos: documentos, equipos electrónicos u objetos de valor, sobre los escritorios, que pueden ser robados fácilmente. |
| **Falta de Capacitación de los funcionarios en temas de seguridad Informática.** | El eslabón más débil en términos de seguridad informática en una organización son los funcionarios, dado que no tienen conocimiento sobre las amenazas y riesgos que enfrentan y como poder mitigarlos. |

## 8.8 identificación de Controles existentes

La identificación de los controles existentes permite realizar la evaluación de riesgos. Lo controles garantizan que al momento de la materialización de un riesgo se reduzcan o mitiguen los riesgos informáticos y la organización funcionen correctamente. Pero se debe tener en cuenta que nunca se va a estar 100% seguros.

El Hospital se cuenta con controles actualmente en el área de Tecnología de la Información y su infraestructura, los cuales no se especifican en este documento para no exponerlos.

## 8.9. Evaluación del riesgo

La evaluación de riesgo se realiza especificando la probabilidad de ocurrencia y el impacto que genera el riesgo en los activos de información, dado por la matriz de calificación, evaluación y respuestas a los riesgos.

## 8.10. Monitoreo y Seguimiento

Mínimo una vez al año 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, la cual deben realizar cada uno de los líderes de las áreas funcionales del Hospital.

## 9. MATRIZ DE RIESGOS DE SEGURIDAD DIGITAL

Para realizar el análisis de los riesgos de cada uno de los procesos se tiene consolidado el formato de matriz de riegos de seguridad digital “PC-FR-020” de todas las áreas del Hospital, las cuales a comienzo de año deben reunirse, apoyados por el área de Planeación para el diligenciamiento de la Matriz.

## 10. IMPLEMENTACION

Para su implementación se realizan las siguientes actividades

-Definir alcance
-Identificación de activos
-Identificación de riesgos
-Identificación de amenazas
-Identificación de controles
-Evaluación de riesgos
-Valoración de riesgos

Esta implementación va de la mano con la Política de Seguridad y los aspectos relacionados con la seguridad de la información.

## 11. CRONOGRAMA

Se especifica el cronograma de las actividades de los proyectos a realizar en el 2021 en el archivo DI-FR-004 PLAN DE TRATAMIENTO DE RIESGOS SPI 2021

## 12. BIBLIOGRAFIA

www.mintic.gov.co G.ES.07 Guía de gestión de riesgos - MinTIC

## 13. CONTROL DE REGISTROS

| Identificación | | Almacenamiento | | Clasificación | Tiempo de retención en archivo de Gestión | Disposición Final |
|---|---|---|---|---|---|---|
| Código Formato | Nombre | Lugar de Archivo | Medio de Archivo | | | |
| DI-FR-004 | Plan de Trabajo | Oficina de TI | Electrónico | Por fecha | 5 años | Archivo de obsoletos |

## 14. CONTROL DE CAMBIOS

| FECHA DEL CAMBIO | VERSIÓN | DESCRIPCIÓN DEL CAMBIO | RESPONSABLES |
|---|---|---|---|
| 29/01/2020 | 1 | Creación del documento | Profesional Universitario Tecnologías de la Información |
| 29/01/2021 | 2 | Actualización del documento | Profesional Universitario Tecnologías de la Información |