Plan de Tratamiento de Riesgos de la

Seguridad y Privacidad de la Información

ENERO 2021

TABLA DE CONTENIDOS

INTRODUCCIÓN

Teniendo en cuenta que la actual revolución digital genera nuevos riesgos y amenazas para garantizar la confidencialidad, integridad y disponibilidad de la información generada por los procesos de la E.S.E Hospital San Juan de Dios de Pamplona, se hace necesaria la implementación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, que garantice la protección de la información ante la ocurrencia de eventos que pongan en peligro su integridad.

Para la realización de este Plan, La E.S.E acogió la Matriz del Mapa de Riesgos de Seguridad Digital proporcionada por el Ministerio de las Tics, realizando la identificación de los activos de información junto con sus posibles amenazas, vulnerabilidades, proporcionando controles para el manejo de los mismos, basados en el impacto de la probabilidad de ocurrencia.

1. OBJETIVOS

1.1. OBJETIVO GENERAL

Desarrollar el Plan de gestión de Seguridad y Privacidad de la Información que permita minimizar los riesgos de perdida de activos de la información en la E.S.E Hospital San Juan de Dios de Pamplona

1.2. OBJETIVOS ESPECIFICOS

- Cumplir con los requisitos legales y reglamentarios pertinentes a la legislación colombiana en materia de seguridad de la información.
- Priorizar los riesgos según los criterios establecidos en el Mapa de Riesgos de Seguridad Digital.
- Realizar la identificación de los principales Activos de Información presentes en la E.S.E.
- Identificar las principales amenazas que afectan a los activos.

- Definir el impacto de la ocurrencia de las amenazas.

- Establecer controles, responsables y periodos de ejecución des las acciones de mitigación de las amenazas de los activos de la información.

- Medir a través de indicadores, el manejo de los riesgos establecidos.

2. ALCANCES Y LIMITACIONES

2.1 ALCANCES

La E.S.E Hospital San Juan de Dios, con el propósito de realizar una eficiente gestión de riesgos de Seguridad y Privacidad de la Información, debe lograr el compromiso para emprender la implementación de este plan en todos los procesos institucionales que se generen, mediante el uso de buenas prácticas y lineamientos nacionales, y locales, con el propósito que ello contribuya a la toma de decisiones y prevenir incidentes que puedan comprometer los activos de información, designando roles de liderazgo que apoyen y asesoren la implementación del Plan, capacitando al personal de la Entidad para su correcta ejecución.

2.2 LIMITACIONES

Crear el rubro de presupuesto necesario para apoyar la implementación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información en la E.S.E Hospital San Juan de Dios de Pamplona.

3.EJECUCIÓN DEL PLAN

3.1 IMPORTANCIA DE LA GESTIÓN DE RIESGOS

La evolución en el manejo de la información, agudizado por el surgimiento de la pandemia del COVID-19, ocasionó la transformación de muchos procesos que anteriormente no involucraban el manejo de recursos digitales, se hace prioritario salvar, proteger y custodiar los activos de la información de la E.S.E Hospital San Juan de Dios de Pamplona.

Siguiendo los lineamientos trazados por el Gobierno Nacional en cumplimiento de la ley de transparencia 1712 del 2014 y Gobierno en Línea, que vienen impulsando actividades dentro de las entidades públicas para que se ajusten a modelos y estándares que permitan brindar seguridad a la información, con

iniciativas como el concurso Máxima Velocidad, creado por el Ministerio de las TICS, la E.S.E da cumplimiento al Decreto 1078 de 2015, por medio del cual “Se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones ”.

Para la realización del plan de tratamiento de riesgos de seguridad y privacidad de la información se utilizó la Guía 7 Gestión de riesgos y la Guía 8 Controles de seguridad de la información.

3.2 DEFINICIÓN GESTIÓN DEL RIESGO

Según la Organización Internacional de Normalización (ISO), la gestión del riesgo se define como: “Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. (NTC ISO 31000:2011)”. Según la Cartilla de Administración de Riesgos del DAFP, la administración del riesgo se divide en los siguientes procesos:

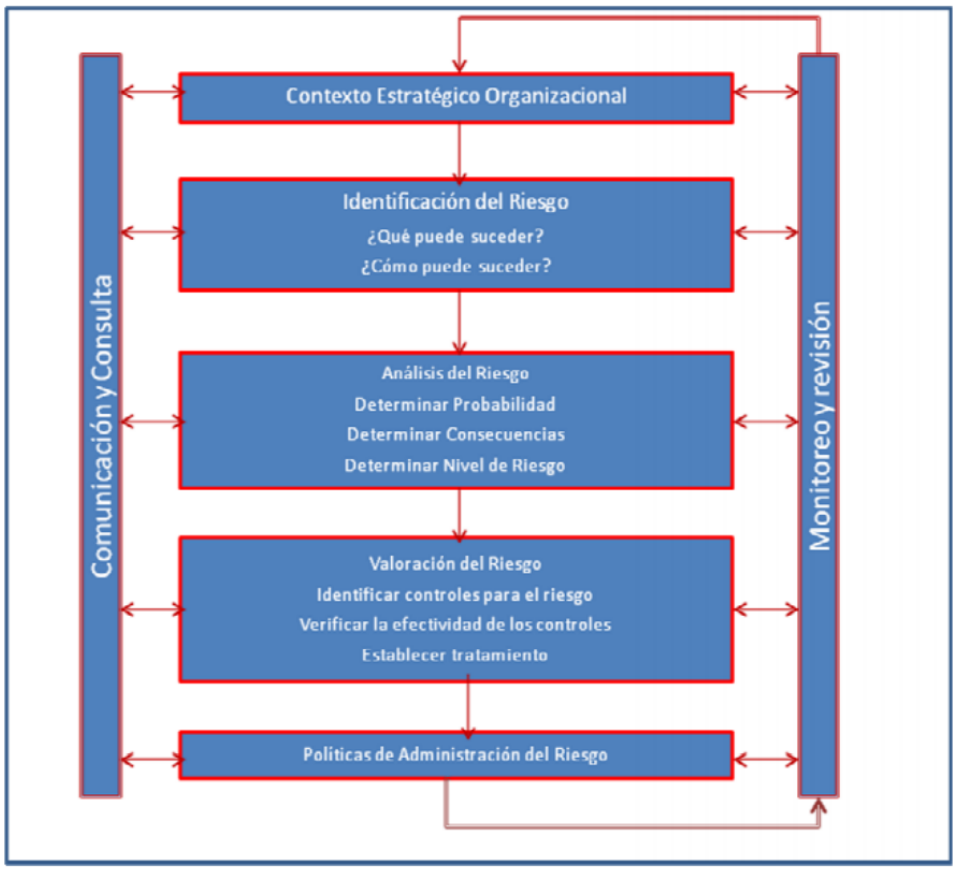

Figura 1. Proceso de Administración del Riesgo

3.3 IDENTIFICACIÓN DEL RIESGO

Para la identificación de los riesgos, el Ministerio de las TIC, en su guía número 7 de Seguridad y Privacidad de la Información, establece la siguiente lista de clasificación de riesgos:

Riesgo Estratégico: Se asocia con la forma en que se administra la Entidad. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta Gerencia.

Riesgos de Imagen: Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.

Riesgos Operativos: Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la entidad y de la articulación entre dependencias.

Riesgos financieros: Se relacionan con el manejo de los recursos de la entidad que incluyen: la ejecución presupuestal, la elaboración de estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.

Riesgos de Cumplimiento: Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad de acuerdo a su misión.

Riesgos de Tecnología: Están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.

3.3 IDENTIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN

El Mapa de Riesgos de Seguridad Digital, proporcionado por el Ministerio de Las TIC, define los siguientes tipos de Activo de Información:

Información y Datos de la Entidad: Datos e información almacenada o procesada física o electrónicamente, tales como: Bases y archivos de datos, contratos, documentación del sistema, investigaciones, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos sobre retiro y pruebas de auditoría, entre otros.

Sistemas de información y aplicaciones de software: Software de aplicación, interfaces, software del sistema, herramientas de desarrollo y otras utilidades relacionadas.

Dispositivos de tecnologías de información-hardware: Equipos de Computo que por su criticidad son considerados activos de información, no solo activos fijos.

Soporte para el saneamiento de información: Equipo para almacenamiento de información como: USB, Discos Duros, CDs, SAND, NAS.

Servicios: Servicios de computación y comunicaciones, tales como Internet, páginas de consulta, directorios compartidos e intranet.

Teniendo en cuenta los criterios mencionados, se identifican los siguientes activos de información.

Tipo de Activo de Información	Activo de Información
Servicios	Canal de datos
Información y datos de la entidad	Políticas de Seguridad Digital
Sistemas de Información y aplicaciones de software	Directorio Activo
Información y datos de la entidad	Copias de Respaldo
Información y datos de la entidad	Información Personal

Tabla 1. Identificación de activos de información

3.4 IDENTIFICACIÓN DE LAS AMENAZAS

Una amenaza tiene el potencial de causar daños a la información, los procesos y los sistemas y, por lo tanto, a la E.S.E Hospital San Juan de Dios. Las amenazas pueden ser de origen natural o humano y podrían ser accidentales o deliberadas es recomendable identificar todos los orígenes de las amenazas accidentales como deliberadas. Las amenazas se deberían identificar genéricamente y por tipo (ej. Acciones no autorizadas, daño físico, fallas técnicas). A continuación, se describen las amenazas identificadas:

Activo de Información	Propiedad que afecta el Riesgo	Amenazas
Canal de datos	Perdida de disponibilidad	Falla del equipo de telecomunicaciones
Políticas de Seguridad Digital	Perdida de integridad	Fallas humanas
Directorio Activo	Perdida de confidencialidad	Abusos de los derechos
Copias de Respaldo	Perdida de disponibilidad	Uso no autorizado de la información

Información Personal	Perdida de confidencialidad	Hurto de la Información

Tabla 2. Identificación de Amenazas

3.5 IDENTIFICACIÓN DE LAS VULNERABILIDADES

A continuación, se presentan las vulnerabilidades que podrían causar la materialización de las amenazas para cada activo de información:

Activo de Información	Amenazas	Vulnerabilidades
Canal de datos	Falla del equipo de telecomunicaciones	Gestión inadecuada de la red (Tolerancia a fallas en el enrutamiento)
Políticas de Seguridad Digital	Fallas humanas	Desconocimiento o no aplicación de las políticas de seguridad y privacidad de la información
Directorio Activo	Abusos de los derechos	Asignación errada de los derechos de acceso
Copias de Respaldo	Uso no autorizado de la información	Uso Inadecuado o descuido del control de acceso físico a las edificaciones y los recintos
Información Personal	Hurto de la Información	Ausencia de políticas de control de acceso

Tabla 3. Identificación de Vulnerabilidades

3.6 ANÁLISIS DEL RIESGO INHERENTE

Para cuantificar y clasificar el riesgo inherente, se toma como base: La tabla de probabilidad, la tabla de impacto y la matriz de calificación:

Tabla de Probabilidad: La probabilidad es la medida para estimar la ocurrencia del riesgo y se mide con criterios de frecuencia.

TABLA DE PROBABILIDAD			
NIVEL	**DESCRIPTOR**	**DESCRIPCIÓN (FACTIBILIDAD)**	**FRECUENCIA**
1	RARO	El evento puede ocurrir solo en circunstancias excepcionales	No se ha presentado en los últimos 5 años.
2	IMPROBABLE	El evento puede ocurrir en algún momento.	Al menos de 1 vez en los últimos 5 años.
3	POSIBLE	El evento podría ocurrir en algún momento.	Al menos de 1 vez en los últimos 2 años.
4	PROBABLE	El evento probablemente ocurrirá en la mayoría de las circunstancias	Al menos de 1 vez en el último año.
5	CASI SEGURO	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.

Figura 2. Tabla de Probabilidad

Tabla de Impacto: Son las consecuencias potenciales que genera el hecho que se materialice en el riesgo.

TABLA DE IMPACTO			
TIPO	**NIVEL**	**DESCRIPTOR**	**DESCRIPCIÓN** En caso que el riesgo se materialice el impacto u afectación sería.....
CONFIDENCIALIDAD EN LA INFORMACIÓN	1	INSIGNIFICANTE	Se afecta a una persona en particular.
	2	MENOR	Se afecta a un grupo de trabajo interno del proceso.
	3	MODERADO	Se afecta a todo el proceso.
	4	MAYOR	La afectación se da a nivel estratégico.
	5	CATASTRÓFICO	La afectación se da a nivel institucional.
CREDIBILIDAD O IMAGEN	1	INSIGNIFICANTE	Se afecta al grupo de funcionarios y contratistas del proceso.
	2	MENOR	Se afecta a todos los funcionarios y contratistas de la entidad.
	3	MODERADO	Se afecta a los usuarios de la Sede Central de la entidad.
	4	MAYOR	Se afecta a los usuarios de las Direcciones Territoriales.
	5	CATASTRÓFICO	Se afecta a los usuarios de la Sede Central y de las Direcciones Territoriales.
LEGAL	1	INSIGNIFICANTE	Se producen multas para la entidad.
	2	MENOR	Se producen demandas para la entidad.
	3	MODERADO	Se producen investigaciones disciplinarias.
	4	MAYOR	Se producen investigaciones fiscales.
	5	CATASTRÓFICO	Se producen intervenciones y o sanciones para la entidad por parte de un Ente de control u otro Ente regulador.
OPERATIVO	1	INSIGNIFICANTE	Se tendrían que realizar ajustes a una actividad concreta del proceso.
	2	MENOR	Se tendrían que realizar ajustes en los procedimientos del proceso.
	3	MODERADO	Se tendrían que realizar ajustes en la interacción de procesos.
	4	MAYOR	Se presentarían intermitencias o dificultades en la operación del proceso
	5	CATASTRÓFICO	Se presentaría paro o no operación del proceso.

Figura 3. Tabla de Impacto

Matriz de Calificación, Evaluación y respuesta a los riesgos: Representa la Zona en la que se encuentra el riesgo a la que se enfrenta inicialmente un proceso o la Entidad en ausencia de controles.

CONCEPTO		IMPACTO				
		1	2	3	4	5
PROBABILIDAD		INSIGNIFICANTE (1)	MENOR (2)	MODERADO (3)	MAYOR (4)	CATASTRÓFICO (5)
	VALOR	1	2	3	4	5
RARA VEZ (1)	1	11	12	13	14	15
IMPROBABLE (2)	2	21	22	23	24	25
POSIBLE (3)	3	31	32	33	34	35
PROBABLE (4)	4	41	42	43	44	45
CASI SEGURO (5)	5	51	52	53	54	55

ZONA DE RIESGO BAJA
ZONA DE RIESGO MODERADA
ZONA DE RIESGO ALTA
ZONA DE RIESGO EXTREMA

Figura 4. Matriz de Calificación, Evaluación y respuesta a los riesgos

Basados en las figuras presentadas anteriormente, se presenta el análisis del riesgo inherente para E.S.E Hospital San Juan de Dios de Pamplona:

Activo de Información	**Probabilidad**	**Impacto**	Zona de Riesgo
Canal de datos	Posible	Mayor	Zona De Riesgo Alta
Políticas de Seguridad Digital	Probable	Mayor	Zona De Riesgo Alta
Directorio Activo	Posible	Menor	Zona De Riesgo Moderada
Copias de Respaldo	Probable	Mayor	Zona De Riesgo Extrema
Información Personal	Casi Seguro	Mayor	Zona De Riesgo Extrema

Tabla 4. Análisis del riesgo inherente

4. IDENTIFICACIÓN DE CONTROLES

En esta etapa, se establecieron los controles que se realizan para mitigar el riesgo inherente, teniendo como referencia las opciones del manejo del riesgo, la descripción del mismo y el responsable de ejecutar su control:

Activo de Información	Opciones de manejo del riesgo	Descripción del control	Responsable de ejecutar el control
Canal de datos	Reducir el riesgo	Monitorear el canal de datos de la entidad	Oficina de Informática y Estadística
Políticas de Seguridad Digital	Reducir el riesgo	Socializar las políticas de seguridad con cada uno de los funcionarios de la entidad	Oficina de Informática y Estadística
Directorio Activo	Reducir el riesgo	Se cuenta con el Profesional Universitario en Informática y Estadística quien asigna los derechos de acceso de acuerdo a las solicitudes realizadas	Oficina de Informática y Estadística
Copias de Respaldo	Reducir el riesgo	Se cuenta con el manual de Seguridad de la Información	Oficina de Informática y Estadística

Información Personal	Reducir el riesgo	Bloqueo personal en cada una de las maquinas	Oficina de Informática y Estadística

Tabla 4. Identificación de Controles

5. PLAN DE TRATAMIENTO DE RIESGOS

Luego de elegir los controles más adecuados para tener un nivel de riesgo aceptable para los procesos, se diseñó el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información, en el cual se tienen en cuenta la reducción del riesgo, los controles, las actividades y los responsables de la ejecución, y así medir periódicamente la ejecución de los mismos mediante un indicador definido para cada activo de la información.

Activo de Información	Opciones de manejo del riesgo	Controles	Actividad	Objetivo del Control	Responsable de Ejecutar el control	Periodo / Fecha de Ejecución	Indicador
Canal de datos	Reducir el riesgo	Mantenimiento de los equipos de red	Contratar los servicios para el mantenimiento de los equipos de red	Realizar un adecuado soporte a los dispositivos de red de la Entidad.	Oficina de Informática y Estadística	Trimestralmente	No de mantenimientos realizados / No de mantenimientos programados

Políticas de Seguridad Digital	Reducir el riesgo	Sensibilización de las políticas de seguridad a los funcionarios de la entidad	Realizar campañas de sensibilización con el objetivo de apropiar las responsabilidades descritas en las políticas de seguridad de la información	Fortalecer la implementación de las políticas de seguridad	Oficina de Informática y Estadística	Trimestralmente	No de sensibilizaciones realizadas / No de sensibilizaciones programadas
Directorio Activo	Reducir el riesgo	Procedimiento de derechos de acceso	Construir y formalizar el procedimiento de derechos de acceso	Fortalecer la implementación de las políticas de seguridad	Oficina de Informática y Estadística	Anualmente	NA

Copias de Respaldo	Reducir el riesgo	Socializar el manual de seguridad de la información con los funcionarios de la Oficina de Informática y Estadística	Plan de sensibilización del manual de seguridad de la información	Reducir la perdida de información	Oficina de Informática y Estadística	Trimestralmente	No de sensibilizaciones realizadas / No de sensibilizaciones programadas
Información Personal	Reducir el riesgo	Establecer política de control de acceso	Socializar la política y el procedimiento de control de acceso	Limitar el acceso a información de la entidad	Oficina de Informática y Estadística	Trimestralmente	No de Actividades ejecutadas / No de Actividades planeadas

Tabla 5. Plan de Tratamiento de Riesgos

BIBLIOGRAFÍA

- Guía 7 Gestión de riegos. Modelo de Seguridad y Privacidad de la Información. Ministerio de Tecnologías de la Información y las Comunicaciones, estrategia 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, estrategia de Gobierno en Línea.
- Guía para la administración del riesgo y el diseño de controles en entidades públicas. Función pública, octubre 2018, versión 4.
- Anexo 4, lineamiento para la gestión de riesgos de seguridad digital en entidades públicas. Ministerio de tecnologías de la información y las comunicaciones, 2018.