GESTIÓN DE TECNOLOGIAS DE LA INFORMACIÓN Y LA COMUNICACIÓN.

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

ENERO 2023

CONTENIDO

INTRODUCCIÓN

1. CONTEXTUALIZACIÓN ORGANIZACIONAL

En la actualidad la tecnología se ha convertido en un aliado estratégico para el avance de cualquier empresa o institución debido a que entrega herramientas especializadas que permiten agilizar procesos, dinamizar grupos de trabajo, asegurar el flujo, disposición y el correcto manejo de la información, así como la toma de decisión basadas en datos.

La tecnología como pilar fundamental en cualquier institución, debe ser capaz de responder a los diferentes retos del día a día, así como al constante cambio que deben sufrir las instituciones de educación superior debido a su misma naturaleza y a la dinámica actual, la cual se centra en la virtualidad, el acceso rápido, ágil y desde cualquier lugar del mundo a plataformas integradas que permitan al estudiante y al docente interactuar constantemente sin estar en un espacio físico en común y disponiendo de cualquier tipo de equipo final (computador, portátil, Tablet, dispositivo móvil)

Como eje primordial de la institución, el ISER apuesta a un cambio en todo lo relacionado a las tecnologías de la información y la comunicación, buscando estar a la vanguardia educativa, y con miras a fortalecer todos sus procesos misionales, estratégicos, de evaluación y apoyo.

Basados en esta estrategia se planea en el presente documento una serie de proyectos y políticas que permitan realizar un cambio tecnológico buscando cumplir con los requerimientos en materia de virtualidad para ampliar la oferta académica, renovar, dinamizar y modernizar las herramientas TIC y brindar a los estudiantes, docentes y administrativos una plataforma especializada que sea un motor para cumplir con la misión y visión de la institución.

1.1. MISIÓN

Incorporar e implementar el uso de las tecnologías de la información y la comunicación como herramienta fundamental para el apoyo a los diferentes procesos institucionales, velando por el correcto funcionamiento de las plataformas tecnológicas, así como la renovación y modernización de la misma.

1.2. VISIÓN

El proceso de gestión de las tecnologías de la información y la comunicación tiene como visión consolidar una infraestructura tecnológica moderna y eficaz que permita garantizar el funcionamiento de la institución, la confidencialidad, seguridad y análisis de la información, así como el buen desempeño de las herramientas tic como eje transversal de todos los procesos.

1.3. VALORES

- Honestidad.
- Solidaridad / generosidad.
- Tolerancia / respeto.
- Responsabilidad.
- Perseverancia.

1.4. OBJETIVOS ESTRATÉGICOS

2. OBJETIVOS

2.1. OBJETIVO GENERAL

Identificar y controlar los riesgos asociados a los diferentes procesos institucionales y que están enmarcados en riesgos de seguridad y privacidad de la información. Con el fin de salvaguardar los activos de información, el manejo de medios, control de acceso y gestión de los usuarios encargados de dichos procesos.

2.2. OBJETIVOS ESPECÍFICOS

- Consolidar una administración de riesgos acorde con las necesidades de la Institución.
- Proteger los activos de información de acuerdo a su clasificación y criterios de Confidencialidad, Integridad y Disponibilidad.
- Crear conciencia a nivel institucional de la importancia y la necesidad de una correcta gestión del riesgo de seguridad de la información.

3. MARCO NORMATIVO

- Decreto Nacional 2573 de 2014 por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones. Este decreto está orientado en su artículo 1 a definir los lineamientos dentro de la estrategia Gobierno en Línea para optimizar las Tecnologías de la Información y las comunicaciones que permitan la gestión y participación de un estado eficiente y participativo entre otros; Incorporando Conceptos Como Arquitectura Empresarial Para La Gestión De Tecnologías De La Información.
- NTC / ISO 27001:2013 Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI).
- NTC/ISO 31000:2009 Gestión del Riesgo. Principios y directrices.
- Decreto Nacional 2573 de 2014 "por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.

Artículo 1°. Objeto. Definir los lineamientos, instrumentos y plazos de la estrategia de Gobierno en Línea para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones, con el fin de contribuir con la construcción de un Estado abierto, más eficiente, más transparente y más participativo y que preste mejores servicios con la colaboración de toda la sociedad".

"Artículo 3°: Definiciones. Para la interpretación del presente decreto, las expresiones aquí utilizadas deben ser entendidas con el significado que a continuación se indica:

Arquitectura Empresarial: Es una práctica estratégica que consiste en analizar integralmente las entidades desde diferentes perspectivas o dimensiones, con el propósito de obtener, evaluar y diagnosticar su estado actual y establecer la transformación necesaria. El objetivo es generar valor a través de las Tecnologías de la Información para que se ayude a materializar la visión de la entidad.

Marco De Referencia De Arquitectura Empresarial Para La Gestión De Tecnologías De La Información: Es un modelo de referencia puesto a disposición de las instituciones del Estado colombiano para ser utilizado como orientador estratégico de las arquitecturas empresariales, tanto sectoriales como institucionales. El marco establece la estructura conceptual, define lineamientos, incorpora mejores prácticas y orienta la implementación para lograr una

administración pública más eficiente, coordinada y transparente, a través del fortalecimiento de la gestión de las Tecnologías de la Información".

"Artículo 5°. **Componentes.** Los fundamentos de la Estrategia serán desarrollados a través de 4 componentes que facilitarán la masificación de la oferta y la demanda del Gobierno en Línea.

1. TIC para Servicios. Comprende la provisión de trámites y servicios a través de medios electrónicos, enfocados a dar solución a las principales necesidades y demandas de los ciudadanos y empresas, en condiciones de calidad, facilidad de uso y mejoramiento continuo.

2. TIC para el Gobierno abierto. Comprende las actividades encaminadas a fomentar la construcción de un Estado más transparente, participativo y colaborativo involucrando a los diferentes actores en los asuntos públicos mediante el uso de las Tecnologías de la Información y las Comunicaciones.

3. TIC para la Gestión. Comprende la planeación y gestión tecnológica, la mejora de procesos internos y el intercambio de información. Igualmente, la gestión y aprovechamiento de la información para el análisis, toma de decisiones y el mejoramiento permanente, con un enfoque integral para una respuesta articulada de gobierno y para hacer más eficaz la gestión administrativa entre instituciones de Gobierno.

4. Seguridad y privacidad de la Información. Comprende las acciones transversales a los demás componentes enunciados, tendientes a proteger la información y los sistemas de información, del acceso, uso, divulgación, interrupción o destrucción no autorizada.

Parágrafo 1°. TIC para el gobierno abierto comprende algunos de los aspectos que hacen parte de Alianza para el Gobierno Abierto, pero no los cobija en su totalidad.

Artículo 6°. Instrumentos. Los instrumentos para la implementación de la estrategia de Gobierno en Línea serán los siguientes:

Manual de Gobierno en Línea. Define las acciones que corresponde ejecutar a las entidades del orden nacional y territorial respectivamente."

Marco de referencia de arquitectura empresarial para la gestión de Tecnologías de la Información. Establece los aspectos que los sujetos obligados deberán adoptar para dar cumplimiento a las acciones definidas en el Manual de gobierno en Línea.

4. ALCANCE

Se define el alcance del presente plan de tratamiento de riesgos de seguridad y privacidad de la información, en los procesos institucionales que tienen servicios de infraestructura tecnológica y que manejan información institucional.

5. RESPONSABILIDADES

El líder del proceso de GTIC es el responsable de llevar a cabo el plan y la difusión a las partes interesadas para el conocimiento y aplicabilidad del mismo.

6. DEFINICIONES

- **ACTIVO DE INFORMACIÓN**: En relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la Organización. Análisis de riesgos: Es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado. Amenaza: Es la causa potencial de una situación de incidente y no deseada por la organización.

- **ADMINISTRACIÓN DEL RIESGO**: Conjunto de elementos de control que al Interrelacionarse brindan a la entidad la capacidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.

- **ANÁLISIS DE RIESGO:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

- **BASE DE DATOS PERSONALES**: Conjunto organizado de datos personales que sea objeto de tratamiento.

- **CAUSA:** Son todo aquello que se pueda considerar fuente generadora de eventos (riesgos). Las fuentes generadoras o agentes generadores son las personas, los métodos, las herramientas, el entorno, lo económico, los insumos o materiales entre otros.

- **CONFIDENCIALIDAD:** Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. CONSECUENCIA: Resultado de un evento que afecta los objetivos.

- **CRITERIOS DEL RIESGO:** Términos de referencia frente a los cuales la importancia de un riesgo se evaluada. CONTROL: Medida que modifica el riesgo.

- **DISPONIBILIDAD:** Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

- **EVALUACIÓN DE RIESGOS:** Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.

- **EVENTO:** Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico. Estimación del riesgo. Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.

- **EVITACIÓN DEL RIESGO:** Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.

- **FACTORES DE RIESGO:** Situaciones, manifestaciones o características medibles u observables asociadas a un proceso que generan la presencia de riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad. Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, se compone de la evaluación y el tratamiento de riesgos.

- **GRAVEDAD:** Se refiere a la magnitud resultante de los daños provocados por un siniestro. Esta es subdividida en ninguna, insignificante, marginal, crítica y catastrófica y se definen según el factor de evaluación (víctimas, pérdidas económicas, suspensión de operación, daño ambiental).

- **IDENTIFICACIÓN DEL RIESGO**: Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.

- **INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN**: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad

7. CONTENIDO PTRSI

METODOLOGIA PARA LA IDENTIFICACION DEL RIESGO.

Ilustración 1. Estructura general de la metodología de riesgos

Fuente: http://www.esap.edu.co/portal//wp-content/uploads/2019/03/Plan-de-Tratamiento-de-Riesgos-de-Seguridad-y-Privacidad-de-la-Informaci%C3%B3n-v_1.0.pdf

La gestión del riesgo dentro de la seguridad de la información se puede también enmarcar dentro del ciclo de planear, hacer, verificar y actuar (PHVA) tal como se muestra en la siguiente ilustración (ISO 27001:2013):

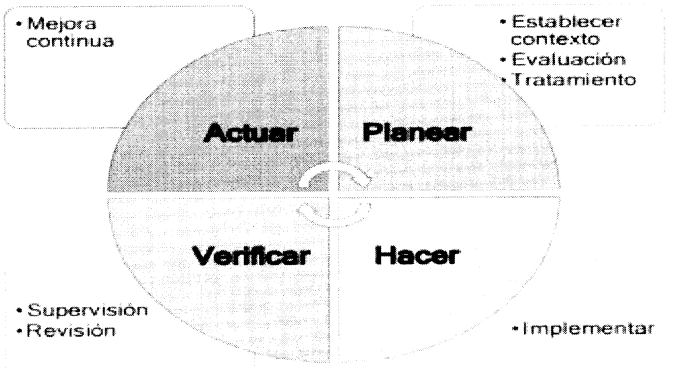

Ilustración 2. Ciclo PHVA y la gestión de riesgos

Fuente: http://www.esap.edu.co/portal//wp-content/uploads/2019/03/Plan-de-Tratamiento-de-Riesgos-de-Seguridad-y-Privacidad-de-la-Informaci%C3%B3n-v_1.0.pdf

ACTIVIDADES

El Plan de Tratamiento de riesgos de seguridad y privacidad de la información del ISER, está enmarcado en las siguientes actividades, las cuales permitirán minimizar los riesgos presentes en los diferentes procesos y que tiene relación con la seguridad de la información.

PROGRAMACIÓN Y AGENDAMIENTO DE ENTREVISTAS

En esta fase se seleccionan los procesos incluidos en el alcance y se realizara una entrevista a cada líder de proceso con el fin de identificar los potenciales riesgos.

ENTREVISTA CON LOS LÍDERES DE PROCESO

Se entrevista a cada líder de proceso, se explica la metodología y en conjunto se procede a realizar la identificación de los riesgos, los cuales se consignan en la Matriz de Riesgos.

IDENTIFICACIÓN Y CALIFICACIÓN DE RIESGOS

En esta fase, el líder de proceso evalúa el nivel de impacto vs. Probabilidad y los controles existentes para calcular el nivel de riesgo.

VALORACIÓN DEL RIESGO RESIDUAL

En esta fase se hace una proyección de la eficacia de los controles para calcular el riesgo residual.

MAPAS DE CALOR DONDE SE UBICAN LOS RIESGOS

Luego se procede a ubicar los riesgos en un mapa de calor para visualizar su comportamiento a medida que se van aplicando los controles.

PLAN DE TRATAMIENTO DE RIESGOS

Cada líder de proceso debe aprobar e implementar el plan de tratamiento de riesgos propuesto.

Fuente: http://www.esap.edu.co/portal//wp-content/uploads/2019/03/Plan-de-Tratamiento-de-Riesgos-de-Seguridad-y-Privacidad-de-la-Informaci%C3%B3n-v_1.0.pdf

CRONOGRAMA

ACTIVIDADES	febrero	marzo	abril	mayo	JULIO	Julio	AGOSTO	SEPTIEMBRE	OCTUBRE	NOVIEMBRE	DICIEMBRE
PROGRAMACIÓN Y AGENDAMIENTO DE ENTREVISTAS											
ENTREVISTA CON LOS LÍDERES DE PROCESO											
IDENTIFICACIÓN Y CALIFICACIÓN DE RIESGOS											
VALORACIÓN DEL											

RIESGO RESIDUAL											
MAPAS DE CALOR DONDE SE UBICAN LOS RIESGOS											
PLAN DE TRATAMIENTO DE RIESGOS											
SEGUIMIENTO Y CONTROL											

8. INDICADORES DE CUMPLIMIENTO

Numero de actividades realizadas / Numero de actividades propuestas.

9. SEGUIMIENTO Y CONTROL

El seguimiento y control será realizara de manera trimestral con el líder de GTIC y el área de planeación.

10. ANEXOS

Ninguno

11. REFERENCIAS BIBLIOGRÁFICAS

https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

12. HISTORIA DE MODIFICACIONES

FECHA	VERSIÓN	DESCRIPCIÓN DEL CAMBIO

13. RESPONSABLE

JOSE DARIO GUERRERO SILVA

PU GTIC