Calle 8 # 8 - 155 Barrio Chapinero - Pamplona, N/S
iserpam@iser.edu.co
+57 (7) 568 25 97

Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

Presentado Por:

Gestión de Tecnologias de la Información y la Comunicación.

INSTITUTO SUPERIOR DE EDUCACIÓN RURAL ISER

PAMPLONA, ENERO DEL 2022

Calle 8 # 8 - 155 Barrio Chapinero - Pamplona, N/S
iserpam@iser.edu.co
+57 (7) 568 25 97

Calle 8 # 8 - 155 Barrio Chapinero - Pamplona, N/S
iserpam@iser.edu.co
+57 (7) 568 25 97

1. INTRODUCCIÓN

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.

2. MARCO NORMATIVO

Calle 8 # 8 - 155 Barrio Chapinero - Pamplona, N/S
iserpam@iser.edu.co
+57 (7) 568 25 97

- 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

Calle 8 # 8 - 155 Barrio Chapinero - Pamplona, N/S
iserpam@iser.edu.co
+57 (7) 568 25 97

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

Calle 8 # 8 - 155 Barrio Chapinero - Pamplona, N/S
iserpam@iser.edu.co
+57 (7) 568 25 97

deberán adoptar para dar cumplimiento a las acciones definidas en el Manual de gobierno en Línea.

3. CONTEXTO ORGANIZACIONAL

El Instituto Superior de Educación Rural ISER cuenta con un plan de desarrollo 2015-2020, el cual está a puertas de cumplir su ciclo, dentro de este plan de desarrollo iniciado en la vigencia 2015 se plantearon una serie de proyectos, que hoy en día ya en su mayoría han sido culminados, y los cuales respondiendo al año en que se plantearon buscaban iniciar con una renovación tecnológica.

El horizonte se había visualizado hacia el año 2020, y la visión institucional se había planteado para el 2019, teniéndose que renovar este año junto con la misión institucional.

El plan de desarrollo se proyectó a una vigencia de 5 años, basado en un Plan Prospectivo de Desarrollo Institucional "JUNTOS A CRECER," 2015- 2020 que conlleva al desarrollo de las políticas, programas, proyectos, indicadores y metas de la institución.

A continuación, se ilustra los ejes estratégicos del plan de desarrollo en estos se observa la línea número 5 de “infraestructura física y tic” la cual el PROCESO DE Medios y Tecnologias de la Información y la Comunicación tiene bajo su responsabilidad el desarrollo de los proyectos y planes

Calle 8 # 8 - 155 Barrio Chapinero - Pamplona, N/S
iserpam@iser.edu.co
+57 (7) 568 25 97

Fuente:http://www.iser.edu.co/iser/hermesoft/portalIG/home_1/recursos/documentos_generales/2016/11112016/plan_desarrollo_version_02.pdf

4. 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 la plataforma tecnológica, así como la renovación y modernización de la misma.

5. VISIÓN

Calle 8 # 8 - 155 Barrio Chapinero - Pamplona, N/S
iserpam@iser.edu.co
+57 (7) 568 25 97

El proceso de medios y 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 la plataforma tecnológica como eje transversal de todos los procesos.

6. OBJETIVO GENERAL

Presentar el Plan de Tratamiento para los riesgos de seguridad y privacidad de la información, de los diferentes procesos identificados en el ISER.

7. OBJETIVOS ESPECIFICOS

- Identificar los riesgos asociados a los procesos que hacen parte del manejo de la información institucional.
- Calcular el nivel de riesgo presente para cada proceso.
- Establecer el plan de tratamiento de riesgos.
- Realizar seguimiento y control a la eficacia del plan de tratamiento de riesgos

8. 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):

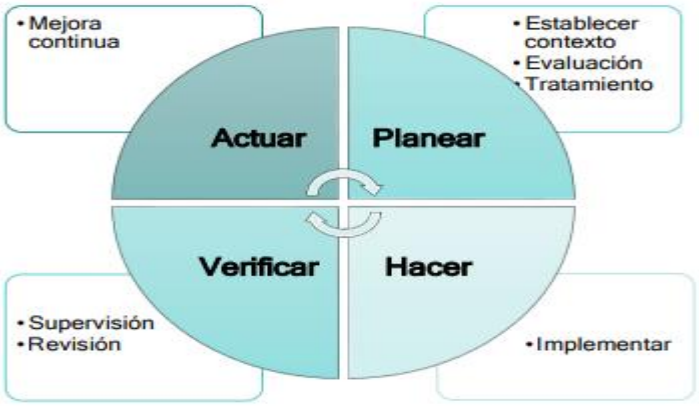

Ilustración 2. Ciclo PHVA y la gestión de riesgos

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

9. ACTIVIDADES

Calle 8 # 8 - 155 Barrio Chapinero - Pamplona, N/S
iserpam@iser.edu.co
+57 (7) 568 25 97

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.

9.1. 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.

9.2. 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.

9.3. 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.

9.4. VALORACIÓN DEL RIESGO RESIDUAL

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

9.5. 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.

9.6. PLAN DE TRATAMIENTO DE RIESGOS

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

9.7. SEGUIMIENTO Y CONTROL

El seguimiento y control será realizado según la guía de control del riesgo establecida para los riesgos de seguridad dela información.

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

10. 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											

11. GLOSARIO

- **Activo:** cualquier elemento que tenga valor para la organización.
- **Análisis del riesgo:** Se estima el riesgo con el fin de proporcionar bases que logre la evaluación y la naturaleza del riesgo.
- **Causa:** Elemento específico que origina el evento.

Calle 8 # 8 - 155 Barrio Chapinero - Pamplona, N/S
iserpam@iser.edu.co
+57 (7) 568 25 97

- **Contexto externo:** Ambiente externo en el cual la organización busca alcanzar sus objetivos (tecnológico, legal, regional, etc.).
- **Contexto interno1:** Ambiente interno en el cual la organización busca alcanzar sus objetivos (gobierno, políticas, estructura organizacional, etc.).
- **Controles:** Procesos, políticas y/o actividades que pueden modificar el riesgo.
- **Criterios de riesgos:** Términos de referencia frente a los cuales se evaluará la importancia del riesgo.
- **Evaluación del Riesgo:** Comparar los resultados del análisis de riesgo frente a los controles implementados, con el fin de determinar el riesgo final.
- **Evento:** Posible ocurrencia de Incidente o amenaza de Seguridad de la Información.
- **Fuente:** Elemento que por sí solo o en combinación tiene el potencial intrínseco para dar lugar a riesgo; a fuente del riesgo puede ser tangible o intangible.
- **Gestión del riesgo:** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.
- **Identificación del riesgo:** Se determinan las causas, fuentes del riesgo y los eventos con base al contexto el proceso, que pueden afectar el logro de los objetivos del mismo.
- **Riesgo aceptable:** Riesgo en que la organización decide que puede convivir y/o soportar dado a sus obligaciones legales, contractuales y/o intereses propios.
- **Riesgo residual:** Nivel de riesgo que permanece luego de tomar medidas de tratamiento.
- **Riesgo:** Posibilidad o probabilidad de que un evento pueda afectar las funciones de la entidad e impactar el logro de sus objetivos.

Calle 8 # 8 - 155 Barrio Chapinero - Pamplona, N/S
iserpam@iser.edu.co
+57 (7) 568 25 97

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