GESTION DE LAS TECNOLOGIAS DE LA INFORMACION Y LA COMUNICACION

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

ENERO 2023

CONTENIDO

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 el plan anual de mantenimiento de herramientas TIC buscando mantener en correcto funcionamiento los recursos informáticos 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

Presentar el Plan de Seguridad y Privacidad de la Información, como documento que dirige la implementación de controles de seguridad en materia de la información digital, según la norma ISO 27001, este documento expone las prioridades de implementación de los controles en relación a seguridad de la información enmarcado en el ciclo de mejoramiento continuo PHVA (planear, hacer, verificar y actuar).

2.2. OBJETIVOS ESPECÍFICOS

- Comunicar e implementar la estrategia de seguridad de la información.

- Implementar y apropiar el Modelo de Seguridad y Privacidad de la Información – MSPI, con el objetivo de proteger la información y los sistemas de información, de acceso, uso, divulgación, interrupción o destrucción no autorizada.

- Hacer uso eficiente y seguro de los recursos de TI (Humano, Físico, Financiero, Tecnológico, etc.), para garantizar la continuidad de la prestación de los servicios.

- Asegurar los recursos de TI (Humano, Físico, Financiero, Tecnológico, etc.), para garantizar la continuidad de la prestación de los servicios.

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.

• 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.

Decreto 1078 de 2015 Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

NTC / ISO 27001:2013 Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos.

NTC/ISO 27002:2013 Tecnología de la información. Técnicas de seguridad. Código de Práctica para controles de seguridad de la información.

4. ALCANCE

El Plan de Seguridad y Privacidad de la Información considera los controles de la norma NTC/ISO 27001:2013, el análisis de riesgos realizado, los procesos de la institución, y los lineamientos del

Modelo de Seguridad y Privacidad de la Información - MSPI de la Estrategia de Gobierno en Línea – GEL con el fin de determinar la estrategia de implementación de los controles de seguridad requeridos para el ISER.

5. RESPONSABILIDADES

6. DEFINICIONES

- **Activo:** En cuanto a la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

- Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

- Confidencialidad: La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

- Contratistas: Entenderemos por contratista aquella persona natural o jurídica que ha celebrado un contrato de prestación de servicios o productos con una entidad.

- Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

- Disponibilidad: Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

- Guía: documento técnico que describe el conjunto de normas a seguir en los trabajos relacionados con los sistemas de información.

- Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

- Norma: Principio que se impone o se adopta para dirigir la conducta o la correcta realización de una acción o el correcto desarrollo de una actividad.

- Parte interesada: (Stakeholder) Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

- Política del SGSI: Manifestación expresa de apoyo y compromiso de la alta dirección con respecto a la seguridad de la información.

- Política: Es la orientación o directriz que debe ser divulgada, entendida y acatada por todos los miembros de la entidad.

- Privacidad de datos: La privacidad de datos, también llamada protección de datos, es el aspecto de la tecnología de la información (TI) que se ocupa de la capacidad que una

7. CONTENIDO PSPI

8. ACTIVIDADES

El plan de seguridad y privacidad de la información comprende un número de actividades cuyo fin principal es establecer una guía que permita crear y fortalecer la políticas institucionales en el ámbito de la seguridad de la información que junto con el PETIC y otros lineamientos y herramientas, nos permitirán avanzar en la creación del sistema de gestión de seguridad de la información SGSI.

REALIZAR EL DIAGNÓSTICO DEL ESTADO ACTUAL DE LOS EQUIPOS INFORMÁTICOS DEL INSTITUTO SUPERIOR DE EDUCACION RURAL INSTITUTO SUPERIOR DE EDUCACIÓN RURAL ISER.

Se debe realizar un estudio técnico del estado actual, cantidad, nivel de obsolescencia de los equipos computacionales, periféricos y demás equipos informáticos del INSTITUTO SUPERIOR DE EDUCACION RURAL INSTITUTO SUPERIOR DE EDUCACIÓN RURAL ISER, con el fin de determinar a ciencia cierta con que elementos cuenta la institución y cuál es su estado.

REALIZAR EL DIAGNÓSTICO DEL ESTADO ACTUAL DEL CENTRO Y LA RED DE DATOS DEL INSTITUTO SUPERIOR DE EDUCACION RURAL INSTITUTO SUPERIOR DE EDUCACIÓN RURAL ISER.

Se debe realizar un estudio técnico del estado actual del centro de datos del INSTITUTO SUPERIOR DE EDUCACION RURAL INSTITUTO SUPERIOR DE EDUCACIÓN RURAL ISER, incluyendo Servidores, cuarto de equipos, condiciones ambientales y de seguridad, con el fin de determinar a ciencia cierta cuál es el verdadero estado de los servidores institucionales, así como de las condiciones físicas, ambientales y de seguridad en las que operan los mismos.

PRESENTAR UNA PROPUESTA INICIAL Y UN PLAN DE TRABAJO PARA LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN Y SEGURIDAD DE LA INFORMACIÓN EN EL INSTITUTO SUPERIOR DE EDUCACION RURAL INSTITUTO SUPERIOR DE EDUCACIÓN RURAL ISER.

Se debe documentar todo los productos obtenidos de las anteriores actividades realizadas, con el fin de establecer un plan de trabajo para la implementación del sistema de gestión de seguridad de la información SGSI en el INSTITUTO SUPERIOR DE EDUCACION RURAL INSTITUTO SUPERIOR DE EDUCACIÓN RURAL ISER.

REALIZAR EL DIAGNÓSTICO DEL ESTADO ACTUAL DE LOS SISTEMAS DE INFORMACIÓN INSTITUCIONAL.

Se debe realizar un estudio técnico del estado actual de todos los sistemas de información institucional, el cual debe incluir disponibilidad del servicio, fallos en los sistemas, actualizaciones, fallas de seguridad, vulnerabilidades, fallas de funcionamiento, respaldo de la información, facilidad

en la obtención de informes, con el fin de determinar las ventajas y desventajas ofrecidos por cada uno, su nivel de apropiación frente a los usuarios finales, usuarios funcionales y administradores del sistema, así como su grado de utilidad.

ESTABLECER LOS ACTIVOS DE INFORMACIÓN DE TI.

Luego de realizado los diagnósticos, se debe realizar o actualizar el inventario detallado del estado y disponibilidad de toda la infraestructura tecnológica de la institución, buscando con este proceso generar un plan de inversión tecnológica en donde se realice la renovación de aquellos equipos, periféricos o sistemas de información cuya vida útil o utilidad ya no sean muy significativas para el INSTITUTO SUPERIOR DE EDUCACION RURAL INSTITUTO SUPERIOR DE EDUCACIÓN RURAL ISER.

REALIZAR UN DIAGNÓSTICO DEL ESTADO ACTUAL INSTITUTO SUPERIOR DE EDUCACION RURAL INSTITUTO SUPERIOR DE EDUCACIÓN RURAL ISER, EN TODO LO REFERENTE A SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

Se debe realizar un estudio detallado que abarque desde diferentes puntos de vista cómo se maneja la seguridad y privacidad de la información en el INSTITUTO SUPERIOR DE EDUCACION RURAL INSTITUTO SUPERIOR DE EDUCACIÓN RURAL ISER, que métodos, modelos y guías se aplican para velar por el correcto uso y disposición de la información, así como los riesgos presentes en el manejo de la misma.

CRONOGRAMA

ACTIVIDADES	Enero	Febrero	Marzo	Abril	mayo	junio	agosto	septiembre	Octubre	Noviembre	Diciembre
REALIZAR EL DIAGNÓSTICO DEL ESTADO ACTUAL DE LOS EQUIPOS INFORMÁTICOS DEL INSTITUTO SUPERIOR DE EDUCACION RURAL INSTITUTO SUPERIOR DE EDUCACIÓN RURAL ISER.											
REALIZAR EL DIAGNÓSTICO DEL ESTADO ACTUAL DEL CENTRO Y LA RED DE DATOS DEL INSTITUTO SUPERIOR DE EDUCACION											

RURAL INSTITUTO SUPERIOR DE EDUCACIÓN RURAL ISER.										
REALIZAR EL DIAGNÓSTICO DEL ESTADO ACTUAL DE LOS SISTEMAS DE INFORMACIÓN INSTITUCIONAL.										
ESTABLECER LOS ACTIVOS DE INFORMACIÓN DE TI.										
REALIZAR UN DIAGNÓSTICO DEL ESTADO ACTUAL INSTITUTO SUPERIOR DE EDUCACION RURAL INSTITUTO SUPERIOR DE EDUCACIÓN RURAL ISER, EN TODO LO REFERENTE A SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.										
PRESENTAR UNA PROPUESTA INICIAL Y UN PLAN DE TRABAJO PARA LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN Y SEGURIDAD DE LA INFORMACIÓN EN EL INSTITUTO SUPERIOR DE EDUCACION RURAL INSTITUTO SUPERIOR DE EDUCACIÓN RURAL ISER.										

9. INDICADORES DE CUMPLIMIENTO

Número de actividades realizadas/ Número de actividades planteadas en el plan

10. SEGUIMIENTO Y CONTROL

El seguimiento y control se realizara de manera trimestral atendiendo a las actividades e indicadores planteados.

11. ANEXOS

Ninguno

12. REFERENCIAS BIBLIOGRÁFICAS

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

13. HISTORIA DE MODIFICACIONES

FECHA	VERSIÓN	DESCRIPCIÓN DEL CAMBIO

14. RESPONSABLE

JOSE DARIO GUERRERO SILVA

Pu GTIC