GESTION DE LAS TECNOLOGIAS DE LA INFORMACION Y LA COMUNICACION

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

ENERO 2024

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 objetivo del plan es mejorar la seguridad digital para todos los procesos del ISER aplicando a todos los niveles funcionales y organizacionales, propendiendo por la confidencialidad, integridad y disponibilidad de los servicios de información. Al final de la ejecución de este plan, se contará con procesos y procedimientos más maduros a nivel de seguridad digital.

5. RESPONSABILIDADES

- Líder del proceso de gestión de Tecnologías de información y la comunicación, será el responsable de realizar el seguimiento al cumplimiento del plan de seguridad y privacidad de la información.

- Equipo de TI Es responsabilidad del personal designado realizar las siguientes actividades:

    - Apoyar al líder del proceso de GTIC en la ejecución del plan de seguridad y privacidad de la información.

- Usuarios Es responsabilidad de los usuarios:

    - El buen uso y manejo que se le dé a los servicios tecnológicos (hardware y software).
    - Atender las recomendaciones establecidas para la ejecución del PSPI.

6. DEFINICIONES

- Activo: en relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de ésta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización. (ISO/IEC 27000).

- Activos de Información y recursos: se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo. (CONPES 3854 de 2016).

- Archivo: conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o Entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).

- Amenazas: causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

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

- Auditoría: proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).

- Autorización: consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3) 15 Plan de seguridad y privacidad de la información Bases de Datos Personales: conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)

- Ciberseguridad: protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa almacena y transporta mediante los servicios de información que se encuentran interconectados.

- Ciberespacio: físico y virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que se usa para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

- 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.

- Datos Personales: cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

- Datos Personales Públicos: es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).

- Datos Personales Privados: es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).

- Datos Personales Mixtos: para efectos de este documento es la información que contiene datos personales públicos junto con datos privados o sensibles.

- Datos Personales Sensibles: se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)

- Derecho a la Intimidad: derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el

pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

- Encargado del Tratamiento de Datos: persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. (Ley 1581 de 2012, art 3)

- Gestión de incidentes de seguridad de la información: procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

- Información Pública Clasificada: es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

- Información Pública Reservada: es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

- Ley de Habeas Data: se refiere a la Ley Estatutaria 1266 de 2008.

- Ley de Transparencia y Acceso a la Información Pública: se refiere a la Ley Estatutaria 1712 de 2014.

- Plan de continuidad del negocio: plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

- Plan de tratamiento de riesgos: documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

- Responsable del Tratamiento de Datos: persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art. 3).

- Riesgo: posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

- Seguridad de la información: preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso o digital. (ISO/IEC 27000).

- Seguridad digital: preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales.

- Titulares de la información: personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)

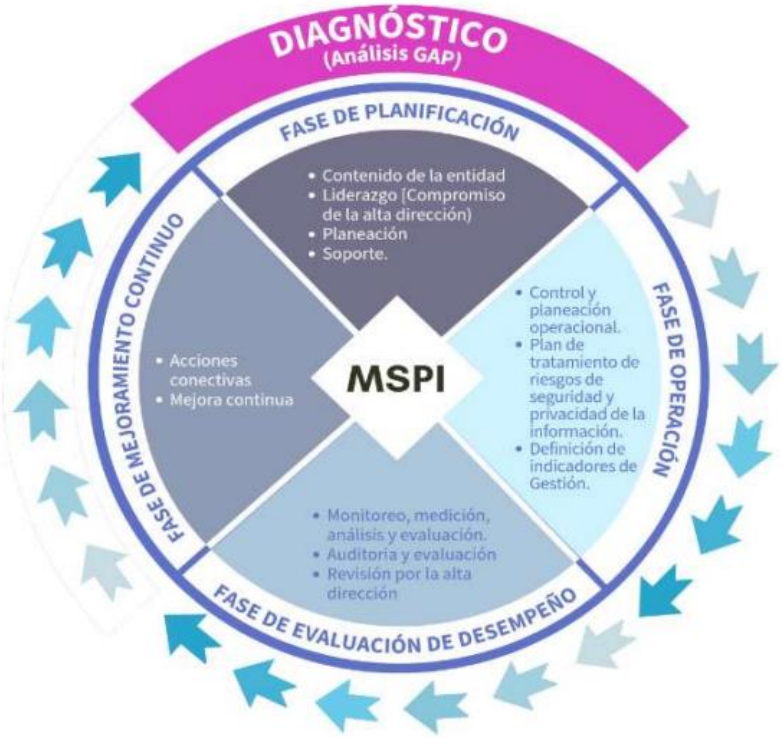
- Tratamiento de Datos Personales: cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

- Trazabilidad: cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o Entidad. (ISO/IEC 27000).

- Vulnerabilidad: debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000)

7. METODOLOGÍA.

La metodología que se aplicará para este plan corresponde a lo que se conoce como Planear, Hacer, Verificar y Actuar que en el nuevo modelo indicado por MinTIC corresponde a:



8. Cumplimiento de la implementación.

Para asegurar el cumplimiento del plan de trabajo descrito en este documento, se realizará un seguimiento trimestral por parte de la Oficina de planeación y será un punto de apoyo para fortalecer las actividades ejecutadas

9. ACTIVIDADES

A continuación, se detallan las actividades que se desarrollarán para fortalecer el modelo de seguridad y privacidad de la información del ISER.

IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN Al momento de generar controles es necesario conocer primero qué es lo que se va a proteger, por lo que se debe realizar, como mínimo, una capacitación con los lideres de proceso para identificar y/o actualizar los activos de información que aportan valor agregado al proceso y por tanto necesitan ser protegidos de potenciales riesgos. Teniendo identificados los activos de información se realiza la respectiva clasificación de acuerdo con la triada: integridad, confidencialidad y disponibilidad para garantizar que la información recibe los niveles de protección adecuados. Una vez establecida la matriz de activos, ésta debe ser publicada en el Sistema de Gestión de la calidad - SGC. Para llevar a cabo la capacitación mencionada anteriormente, es necesario validar si existe alguna nueva reglamentación sobre el procedimiento que se está llevando actualmente en la entidad para realizar el ajuste y la publicación en el SGC.

Las tareas que se desarrollarán son:

- Definir los lideres de cada área para identificación de activos.
- Actualizar metodología en caso de ser necesario.
- Capacitar a los lideres sobre la metodología a aplicar.
- Actualizar activos de información.
- Validar la actualización realizada.
- Consolidar la información recopilada y cargarla en el SGC.
- Publicar los activos de información en los sistemas correspondientes

GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN Eli líder del proceso de GTIC será el encargado junto con el apoyo del líder de planeación estratégica de validar y/o actualizar el procedimiento para la administración de riesgos de seguridad donde se incluye el apartado de seguridad de la información y seguridad digital. Es así como se brindará la capacitación preferiblemente al mismo equipo humano que participó en la identificación de activos de información permitiendo así, que se generen las salvaguardas correspondientes y, de ser necesario, la creación de planes de mejoramiento para la eliminación o mitigación de los riesgos, con el fin de llevarlo a valores aceptables por cada proceso de la entidad. El seguimiento a las salvaguardas y a los planes de mejora los realizará el líder del proceso de planeación estratégica en conjunto con el líder Control Interno, para asegurar que se cumplan las fechas establecidas.

Las tareas que se desarrollarán son:

- Actualizar de ser necesario los lineamientos de tratamiento de riesgos
- Capacitar a los lideres de proceso sobre la metodología a aplicar Identificar riesgos de seguridad digital para los activos de información identificados en la actividad anterior.
- Actualizar mapa de riesgos.
- Realizar seguimiento a los controles y planes de mejora.

APROPIACIÓN DEL SISTEMA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Para que un modelo de seguridad y privacidad de la información tenga resultados exitosos, es necesario que todos los lineamientos se socialicen con los colaboradores de la entidad, para promover una cultura digital, atentos a los riesgos de seguridad digital en las labores diarias, dentro de las instalaciones del ISER o en la modalidad de teletrabajo. Por lo anterior es necesario definir las temáticas que serán socializadas por los diferentes medios dispuestos por el ISER, entre los cuales se encuentran el correo electrónico, redes sociales, intranet. Es importante, así mismo, realizar ejercicios de ingeniería social para evaluar el nivel de conciencia de los usuarios finales con respecto a mensajes falsos con los cuales puede comprometer la seguridad de la información de los activos que maneja.

Las tareas que se desarrollarán son:

- Definir temáticas a sensibilizar
- Crear piezas de sensibilización para enviar por los medios dispuestos
- Enviar piezas de sensibilización
- Realizar ejercicios de ingeniería social

PLAN DE RECUPERACIÓN DE DESASTRES Con la finalidad de reducir las afectaciones que puedan llegar a existir ante la materialización de un riesgo de seguridad digital, es necesario actualizar la estrategia de recuperación de desastres, para lo cual, se debe iniciar con la actualización del BIA (Business Continuity Plan) para determinar los sistemas más críticos y los que se deben recuperar primero. Con este insumo se actualizará la estrategia del DRP (Disaster Recovery Plan) y la manera en que periódicamente se deberá probar la efectividad de este. Una vez cumplido con estos documentos se debe publicar la información en el SGC.

Las tareas que se desarrollarán son:

- Actualizar documentación del Análisis de Impacto del Negocio
- Actualizar la documentación de estrategias del plan de recuperación de desastres
- Realizar pruebas de las estrategias del plan de recuperación
- Ajustar documentación de la estrategia de ser necesaria de acuerdo con la tarea anterior.

AUDITORÍAS Una parte esencial para mejorar el MSPI es realizar auditorías a las políticas y controles definidos en la declaración de aplicabilidad; por ello, desde el proceso de gestión de tecnologías de la información y la comunicación se participará activamente en estas sesiones de trabajo y en los planes de mejora, si se encuentra alguna oportunidad de mejora.

SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN Participar en las sesiones de comités de gestión y desempeño para presentar los avances realizados al MSPI, planes de mejoramiento y los indicadores que se tengan definidos y recibir la retroalimentación correspondiente por parte del comité.

ACTUALIZACIÓN Y CREACIÓN DE POLÍTICAS Actualizar cuando se requiera la documentación sobre los manuales, políticas y procedimientos y publicarlas en el SGC.

Las tareas que se desarrollarán son:

- Validar las políticas y procedimientos existentes
- Actualizar políticas y procedimientos en caso de ser necesario
- Publicar las políticas y/o procedimientos con los ajustes correspondientes

REVISIÓN DE CONTROLES Validar el cumplimiento de los controles definidos en las políticas y ejecutar acciones de mejora, en caso de requerirse.

Las tareas que se desarrollarán son:

- Validar la correcta implementación de los controles definidos
- Realizar ajuste a los controles en caso de ser necesario
- Por lo anterior, es necesario validar al inicio de cada vigencia las actualizaciones del instrumento de MinTIC, para adoptar las medidas correspondientes en este plan.

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 las 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

Actividad	Tarea	Responsable	Comienzo	Fin
identificar de activos de información	Definir los lideres de cada proceso para identificación de activos	Lideres de proceso	6/02/2024	28/02/2024
	Actualizar metodología en caso de ser necesario	Líder GTIC	6/02/2024	6/03/2024
	Capacitar a los lideres y personal de apoyo sobre la metodología a aplicar	líder de GTIC y lideres de proceso.	18/03/2024	31/03/2024
	Actualizar activos de información	líder de GTIC y lideres de proceso.	3/04/2024	3/05/2024
	Validar la actualización realizada	Líder GTIC	6/05/2024	19/05/2024
	Consolidar la información recopilada y cargarla en el SGC	Líder GTIC y líder planeación estratégica.	19/05/2024	3/06/2024
	Publicar los activos de información en los sistemas correspondientes	Líder GTIC – líder proceso comunicación estratégica.	5/06/2024	10/06/2024
Gestionar riesgos de seguridad de la información	Actualizar de ser necesario los lineamientos de tratamiento de riesgos	Líder GTIC, líder planeación estratégica y líder control interno.	6/02/2024	20/05/2024
	Capacitar a los lideres sobre la metodología a aplicar	Líder GTIC	13/06/2024	15/07/2024
	Identificar riesgos de seguridad digital para los activos de información identificados en la actividad anterior	líder de GTIC y lideres de proceso.	17/07/2024	14/08/2024
	Actualizar mapa de riesgos	Líder GTIC y líder planeación estratégica.	14/08/2024	30/08/2024
	Realizar seguimiento a los controles y planes de mejora	Líder GTIC, líder planeación estratégica y líder control interno.	30/08/2024	16/12/2024
Apropiación del SGSI	Definir temáticas a sensibilizar	Líder GTIC	6/02/2024	15/02/2024
	Diligenciar los formatos a implementar.	Líder GTIC	15/02/2024	15/02/2024
	Crear piezas de sensibilización para enviar por los medios dispuestos	Líder GTIC – líder proceso comunicación estratégica.	15/02/2024	1/11/2024
	Enviar piezas de sensibilización	Líder GTIC – líder proceso comunicación estratégica.	1/03/2024	15/11/2024

	Realizar ejercicios de ingeniería social	Líder GTIC	6/02/2024	29/11/2024
Crear plan de recuperación de desastres	Actualizar documentación del Análisis de Impacto del Negocio	Líder GTIC	6/02/2024	15/04/2024
	Actualizar la documentación de estrategias del plan de recuperación de desastres	Líder GTIC	15/04/2024	15/05/2024
	Realizar pruebas de las estrategias del plan de recuperación	Líder GTIC	15/05/2024	15/11/2024
	Ajustar documentación de la estrategia de ser necesaria de acuerdo a la tarea anterior	Líder GTIC	15/05/2024	15/11/2024
Participar en auditorias	Participar en las auditorias internas y externas que sean requeridas	Líder GTIC	6/02/2024	30/12/2024
Seguimiento al SGSI	Participar en las sesiones de comités de gestión del desempeño para mostrar los avances sobre el SGSI	Líder GTIC	6/02/2024	30/12/2024
Actualizar Politicas	Validar las políticas y procedimientos existentes	Líder GTIC	6/02/2024	29/11/2024
	Actualizar políticas y procedimientos en caso de ser necesario	Líder GTIC	6/02/2024	29/11/2024
	Publicar las políticas y/o procedimientos con los ajustes correspondientes	Líder GTIC y líder planeación estratégica.	6/02/2024	29/11/2024
Revisar controles	Validar la correcta implementación de los controles definidos	Líder GTIC y líder planeación estratégica.	6/02/2024	29/11/2024
	Realizar ajuste a los controles en caso de ser necesario	Líder GTIC y líder planeación estratégica.	6/02/2024	29/11/2024

10. INDICADORES DE CUMPLIMIENTO

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

11. SEGUIMIENTO Y CONTROL

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

12. ANEXOS

Matriz de seguridad y privacidad de la información.

13. REFERENCIAS BIBLIOGRÁFICAS

https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf
articles-419313_recurso_6.pdf (mineducacion.gov.co)

14. HISTORIA DE MODIFICACIONES

FECHA	VERSIÓN	DESCRIPCIÓN DEL CAMBIO

15. RESPONSABLE

JOSE DARIO GUERRERO SILVA

Pu GTIC