MANUAL DE GESTIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Sede Central / Av. Pastrana Borrero - Cra. 1
Sede Administrativa / Cra. 5 No. 23 - 40
www.usco.edu.co / Neiva - Huila
PBX: 875 4753
PBX: 875 3686
Línea Gratuita Nacional: 018000 968722

Control de Cambios

Versión	Fecha	Descripción	Elaboró	Vo Bo	Vo Bo
1.0	01/02/24	Versión Inicial	Martha Liliana Hermosa T. Nancy Catherine Molina S. Isabel Cristina Cleves R	German Andrés Sánchez Ortegón Asesor Seguridad de la Información	Erick Richard Rincón Cárdenas Asesor Privacidad de la Información

.

Sede Central / Av. Pastrana Borrero - Cra. 1
Sede Administrativa / Cra. 5 No. 23 - 40
www.usco.edu.co / Neiva - Huila
PBX: 875 4753
PBX: 875 3686
Línea Gratuita Nacional: 018000 968722

Contenido

1. PRESENTACIÓN DE LA UNIVERSIDAD SURCOLOMBIANA 6
1.1. Misión 6
1.2. Visión 6
1.3. Mapa de Procesos 7
1.4. Ubicación 8
2. PRESENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 8
2.1. Objetivo 9
2.2. Alcance 9
3. SISTEMA DE GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 9
4. CONTEXTO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD SURCOLOMBIANA 11
4.1. Contexto Interno y Externo 11
4.2 Partes Interesadas 12
4.3 Alcance del Sistema de Gestión de seguridad y privacidad de la Información para la certificación 13
4.4 Sistema de gestión de seguridad y privacidad de la información 13
5. LIDERAZGO 13
5.1 Liderazgo y compromiso 14
5.2. Política de Seguridad y Privacidad de la Información 15
5.3 Roles, responsabilidades y autoridades 16
6. PLANIFICACIÓN 17
6.1 Acciones para abordar riesgos y oportunidades 17
6.2 Objetivos de seguridad y privacidad de la información 17
6.3 Planificación de los cambios 18
7. APOYO 19
7.1 Recursos 19
7.2 Competencia 20
7.3 Toma de conciencia 21
7.4 Comunicación 22
7.5 Información documentada 22

8. OPERACIÓN 23
8.1 Planificación y control de la operación 23
8.2 Evaluación de los riesgos para la seguridad de la información 24
8.3 Tratamiento de los riesgos para la seguridad de la información 24
9. EVALUACIÓN DE DESEMPEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN 24
9.1 Seguimiento, medición, análisis y evaluación 24
9.2 Auditoría interna 25
9.3 Revisión por la dirección 25
10. MEJORA 26
10.1 Mejora continua 26
10.2 No conformidad y acción correctiva 26
11. CONTROLES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 26

Sede Central / Av. Pastrana Borrero - Cra. 1
Sede Administrativa / Cra. 5 No. 23 - 40
www.usco.edu.co / Neiva - Huila
PBX: 875 4753
PBX: 875 3686
Línea Gratuita Nacional: 018000 968722

TABLA DE GRÁFICAS

Grafica 1. Mapa de procesos 7
Gráfica 2. Ciclo PHVA 10

Sede Central / Av. Pastrana Borrero - Cra. 1
Sede Administrativa / Cra. 5 No. 23 - 40
www.usco.edu.co / Neiva - Huila
PBX: 875 4753
PBX: 875 3686
Línea Gratuita Nacional: 018000 968722

1. PRESENTACIÓN DE LA UNIVERSIDAD SURCOLOMBIANA

1.1. Misión

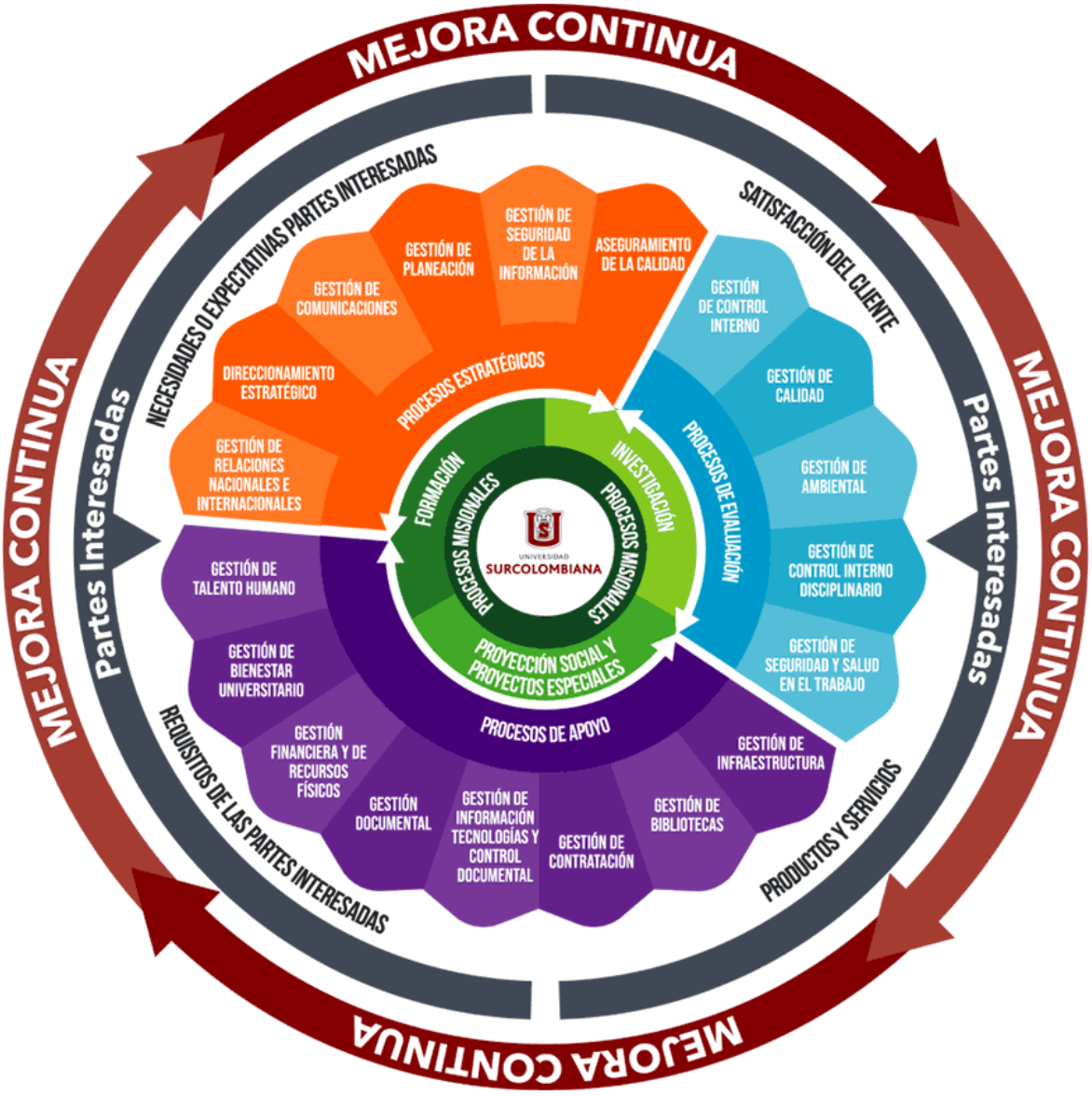
La Universidad Surcolombiana orienta y lidera la formación integral, humana y crítica de profesionales e investigadores, fundamentada en conocimientos disciplinares, de las profesiones, interdisciplinares y multiculturales, mediante procesos académicos, sociales y políticos transformadores, comprometidos prioritariamente con la construcción de una nación democrática, deliberativa, participativa y en paz, soportada en el desarrollo humano, social, sostenible y sustentable en la región Surcolombiana; su accionar será orientado por la ética cívica, el diálogo multicultural, la preservación y defensa del medio ambiente y el pensamiento complejo, con proyección nacional e internacional.

1.2. Visión

En el año 2024, la Universidad Surcolombiana consolidará el liderazgo de los procesos de formación integral y crítica de profesionales y será vanguardia en generación de conocimientos mediante la investigación y en la formación de investigadores, que promuevan los procesos de apropiación, producción y aplicación de los conocimientos, en la construcción de una sociedad democrática, deliberativa, participativa, con el fin de que éstos contribuyan a la solución de los problemas relevantes de la realidad regional, con proyección nacional e internacional y perspectiva de sustentabilidad ambiental, equidad, justicia, pluralismo, solidaridad y respeto por la dignidad humana.

Sede Central / Av. Pastrana Borrero - Cra. 1
Sede Administrativa / Cra. 5 No. 23 - 40
www.usco.edu.co / Neiva - Huila
PBX: 875 4753
PBX: 875 3686
Línea Gratuita Nacional: 018000 968722

1.3. Mapa de Procesos



Gráfica 1. Mapa de Procesos

Sede Central / Av. Pastrana Borrero - Cra. 1
Sede Administrativa / Cra. 5 No. 23 - 40
www.usco.edu.co / Neiva - Huila
PBX: 875 4753
PBX: 875 3686
Línea Gratuita Nacional: 018000 968722

1.4. Ubicación

Las sedes de la Universidad Surcolombiana están ubicadas en puntos estratégicos para atender los requerimientos de bachilleres y profesionales, prestando un buen servicio y contribuyendo a la formación integral de todos los usuarios:

Sede Central Avenida Pastrana Borrero - Carrera 1 Neiva-Huila
Facultad de Salud Calle 9 Carrera 14. Contiguo al Hospital Universitario Hernando Moncaleano" Neiva- Huila
Sede Postgrados Cr. 5 No 23-40 Neiva- Huila
Sede la Plata Municipio de La Plata - Huila
Sede Garzón Municipio de Garzón - Huila
Sede Pitalito Municipio de Pitalito - Huila

2. PRESENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La información es un recurso que, como el resto de los activos, tiene valor para la Universidad Surcolombiana, "en adelante la Universidad", que permite el desarrollo continuo de la misión y el cumplimiento del objetivo de esta, lo cual genera la necesidad de implementar reglas y medidas que permitan proteger la confidencialidad, integridad y disponibilidad en todo el ciclo de vida de la información y sus activos asociados, incluyendo la información de identificación personal.

El establecimiento, seguimiento, mejora continua y aplicación de la Política de seguridad y privacidad de la información garantiza un compromiso ineludible de protección a la misma frente a las amenazas y contribuye a minimizar los riesgos asociados a pérdida de información y/o accesos no autorizados a la infraestructura tecnológica y asegurar el eficiente cumplimiento de las funciones misionales de la institución apoyadas en un correcto sistema de información.

El presente manual describe el Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI) definido por la Universidad, el cual se complementa con el Manual de Políticas de Seguridad y Privacidad de la Información, las cuales se encuentran enfocadas al cumplimiento de la normatividad legal colombiana vigente y a las buenas prácticas de seguridad y privacidad de la información, basadas en las normas NTC ISO IEC 27001 y NTC ISO IEC 27701, el Modelo de Seguridad y Privacidad de la Información de la estrategia de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia y a las obligaciones contractuales establecidas.

La seguridad y privacidad de la información es para la Universidad una labor prioritaria que exhorta a todos los involucrados a velar por el cumplimiento de los lineamientos establecidos en el presente manual.

2.1. Objetivo

Describir los elementos del sistema de gestión de seguridad y privacidad de la Información de la Universidad Surcolombiana y presentar en forma clara y coherente los elementos que conforman la política y los objetivos de dicho sistema, que deben conocer y cumplir todos los directivos, funcionarios, contratistas, terceros, aprendices, practicantes, docentes, estudiantes y comunidad en general que tengan algún tipo de relación con la Universidad.

2.2. Alcance

2.2.1. Alcance de la aplicación del Manual

El Manual del Sistema de Gestión de Seguridad y Privacidad de la Información de la Universidad Surcolombiana y sus directrices son de aplicación y obligatorio cumplimiento por parte de funcionarios administrativos, docentes, estudiantes, contratistas y/o terceros de la Universidad Surcolombiana, para todas las sedes de Neiva, Pitalito, Garzón y La Plata.

3. SISTEMA DE GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Universidad Surcolombiana ha establecido, implementado, mantenido y mejorado continuamente el Sistema de Gestión de la Seguridad y Privacidad de la Información mediante la formulación, desarrollo, evaluación de lineamientos, planes, programas, proyectos y metodologías que garanticen la disponibilidad, confidencialidad e integridad de la información.

Un sistema de gestión utiliza un marco de recursos para lograr los objetivos de una organización. El sistema de gestión incluye la estructura organizativa, las políticas, las actividades de planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos. En términos de seguridad y privacidad de la información, un sistema de gestión permite que la Universidad:

a) satisfaga los requisitos de seguridad de la información de los clientes y otras partes interesadas;
b) mejore los planes y actividades;
c) cumpla con los objetivos de seguridad de la información de la organización;
d) cumpla los reglamentos, la legislación y los mandatos del sector educativo; y

Sede Central / Av. Pastrana Borrero - Cra. 1
Sede Administrativa / Cra. 5 No. 23 - 40
www.usco.edu.co / Neiva - Huila
PBX: 875 4753
PBX: 875 3686
Línea Gratuita Nacional: 018000 968722

e) administre los activos de información de una manera organizada que facilite la mejora continua y el ajuste a las metas organizacionales actuales.

El Sistema de Gestión de la Seguridad y Privacidad de la Información de la Universidad Surcolombiana adopta el Ciclo PHVA (Planificar, Hacer, Verificar y Actuar) de mejora continua ver gráfico 1:

Planear (planificación del sistema de gestión de la seguridad y privacidad de la información) Establece la política y objetivos de seguridad y privacidad de la Información, así como los procesos y procedimientos del SGSPI relevantes, para gestionar el riesgo y mejorar la seguridad y privacidad de la información, a fin de entregar resultados conforme a las políticas y objetivos generales de la organización.

Hacer (Implementación y Operación del sistema de gestión de la seguridad y privacidad de la información) Implementa y opera la política de seguridad y privacidad de la información, controles, procesos y procedimientos del SGSPI.

Verificar (Monitoreo y Revisión del Sistema de Gestión de la seguridad y privacidad de la información).

Revisa y evalúa el desempeño (eficiencia y efectividad) del SGSPI, a través de auditorías internas, revisión de la Dirección, entre otras herramientas.

Actuar (Mantenimiento y Mejora del Sistema de Gestión de la Seguridad y Privacidad de la Información).

Tomar medidas necesarias para mejorar el desempeño del SGSPI, con base en los resultados de la auditoría interna al SGSPI, la revisión de la Dirección u otra información relevante.

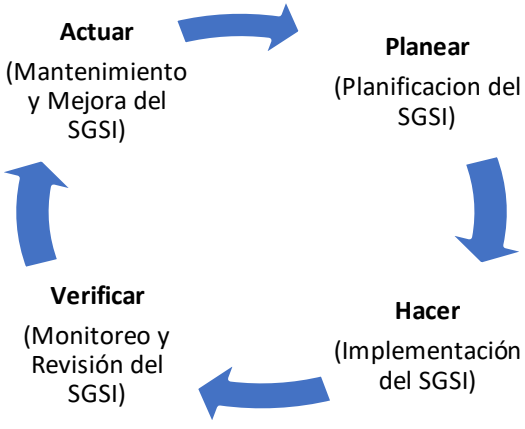


Gráfico 2. Ciclo PHVA

Sede Central / Av. Pastrana Borrero - Cra. 1
Sede Administrativa / Cra. 5 No. 23 - 40
www.usco.edu.co / Neiva - Huila
PBX: 875 4753
PBX: 875 3686
Línea Gratuita Nacional: 018000 968722

4. CONTEXTO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD SURCOLOMBIANA

Es el punto de partida para desarrollar el Sistema de Gestión de seguridad y Privacidad de la Información que consiste en identificar las cuestiones internas y externas que afectan la capacidad para lograr los resultados previstos.

El análisis de estas cuestiones tiene tres propósitos para la Universidad:

- comprender el contexto para decidir el alcance del SGSI;
- analizar el contexto para determinar los riesgos y las oportunidades; y
- asegurar que el SGSI está adaptado a las cuestiones externas e internas cambiantes.

La definición del contexto también considera las necesidades y expectativas de todas las partes interesadas. En otras palabras, los temas que puedan afectar a la seguridad y privacidad de la información por la influencia de las cuestiones externas e internas en las actividades de la Universidad. Se trata de identificar la influencia en la seguridad y privacidad de la información.

La Universidad Surcolombiana para determinar las cuestiones externas e internas que afectan su capacidad para lograr los resultados previstos en el sistema de gestión de seguridad y privacidad de la Información, identifica y evalúa los factores de riesgo externos e internos generadores de eventos en los que se originen pérdidas por riesgo en la seguridad y privacidad de la información y aprovecha las oportunidades que permitan potencializar el logro de los resultados previstos. También se revisan los cambios ocurridos en cuestiones externas e internas que afecten al sistema de gestión de seguridad y privacidad de la Información. Está disponible como información documentada en el Portal Institucional https://www.usco.edu.co/es/transparencia/ plan de desarrollo institucional y sus modificaciones, plan de acción de ejecución del plan de desarrollo, proyecto educativo universitario.

4.1. Contexto Interno y Externo

Para identificar las cuestiones internas y externas del sistema de gestión de seguridad de la información se utilizó la metodología DOFA. Cada proceso realiza el análisis y se consolida en el documento ES-GSI-MR-01 MATRIZ DE CONTEXTO DE LA ORGANIZACIÓN.

Para el seguimiento y revisión de la información sobre el entorno interno y externo se realizan reuniones anuales con los procesos para actualizar el contexto organizacional.

Sede Central / Av. Pastrana Borrero - Cra. 1
Sede Administrativa / Cra. 5 No. 23 - 40
www.usco.edu.co / Neiva - Huila
PBX: 875 4753
PBX: 875 3686
Línea Gratuita Nacional: 018000 968722

4.2. Partes Interesadas

Una parte interesada es toda aquella persona interna y/o externa u organización que tiene o puede tener capacidad de afectarnos como institución, o puede sentirse afectada en temas de seguridad de la Información. Para el análisis y elaboración de la matriz de partes interesadas pertinentes al sistema de gestión de seguridad de la información de la Universidad Surcolombiana se llevaron a cabo reuniones con los líderes de procesos, quienes identificaron las diferentes partes interesadas, las clasificaron dentro de las categorías internas o externas; igualmente por cada parte interesada se enumeran las necesidades, expectativas, intereses, requisitos sobre la seguridad de la información de la Universidad Surcolombiana. Está disponible como información documentada ES-GSI-MR-03 MATRIZ IDENTIFICACIÓN DE PARTES INTERESADAS PERTINENTES SGSI.

Una vez identificadas las partes interesadas y sus requisitos, se realiza el proceso de evaluación del nivel de impacto, en las variables de poder e interés, que cada uno de los requisitos/intereses tiene relacionados al Sistema de Gestión de Seguridad y Privacidad de la Información.

Definida la valoración se procede a realizar la clasificación y priorización de los grupos de interés pertinentes al sistema de gestión de seguridad y privacidad de la información de Universidad Surcolombiana. Sus resultados se pueden ver como información documentada en: ES-GSI-CP-01 CARACTERIZACIÓN DEL PROCESO DEL SISTEMA DE GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

Para el seguimiento de las partes interesadas, la Universidad aplica un instrumento a través del Sistema de información de encuestas, el cual permite evaluar el cumplimiento de los requisitos de seguridad y privacidad de la información que se abordan a través del sistema de gestión.

4.2.1. Marco Normativo

La norma internacional NTC ISO IEC 27001 contiene los estándares para implementar la gestión de la seguridad de la información permitiendo el aseguramiento, la confidencialidad e integridad de los datos, así como de los sistemas que la procesan, basándose en la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos. Estos requisitos se complementan con los requisitos legales, normativos y contractuales, los cuales se encuentran disponibles como información documentada en ES-GSI-MR-02 MATRIZ DE REQUISITOS LEGALES Y REGLAMENTARIOS.

Sede Central / Av. Pastrana Borrero - Cra. 1
Sede Administrativa / Cra. 5 No. 23 - 40
www.usco.edu.co / Neiva - Huila
PBX: 875 4753
PBX: 875 3686
Línea Gratuita Nacional: 018000 968722

4.3. Alcance del Sistema de Gestión de seguridad y privacidad de la Información para la certificación

El alcance para la certificación en las normas NTC ISO IEC 27001 y NTC ISO IEC 27701 es:

"Gestión de seguridad y privacidad de la información para la prestación de servicios de diseño, formación, investigación y proyección social y proyectos especiales en educación superior a través de programas de pregrado y posgrado ofrecidos en las instalaciones de la Universidad Surcolombiana en la sede de Neiva".

Se excluyen de la certificación las sedes de Pitalito, Garzón y La Plata.

La inclusión y la exclusión de los controles del anexo A de la norma NTC ISO IEC 27001 y los controles de los anexos A y B de la norma NTC ISO IEC 27701 se encuentran documentados con sus justificaciones en el documento ES-GSI-DA-06 DECLARACIÓN DE APLICABILIDAD del Sistema de Gestión de Seguridad y Privacidad de la Información.

4.4. Sistema de gestión de seguridad y privacidad de la información

En el mapa de procesos de la Universidad se identifican los procesos misionales formación, investigación y proyección social y proyectos especiales que hacen parte del alcance definido para la certificación del SGSPI.

El proceso que lidera el Sistema de Gestión de Seguridad y Privacidad de la Información se denomina Gestión de Seguridad de la Información. Ver ES-GSI-CP-01 CARACTERIZACIÓN DEL PROCESO.

5. LIDERAZGO

La alta dirección demuestra el liderazgo y compromiso con respecto al SGSPI. El liderazgo y el compromiso son esenciales para la eficacia del mismo.

La alta dirección se define en la Universidad como el grupo de personas que dirige y controla la Institución al más alto nivel. Tiene la responsabilidad total por el sistema. Delega la autoridad en la Universidad a través del proceso Gestión de seguridad y privacidad de la información, conservando la responsabilidad total del sistema.

Sede Central / Av. Pastrana Borrero - Cra. 1
Sede Administrativa / Cra. 5 No. 23 - 40
www.usco.edu.co / Neiva - Huila
PBX: 875 4753
PBX: 875 3686
Línea Gratuita Nacional: 018000 968722

5.1. Liderazgo y compromiso

La alta dirección realiza la revisión por la dirección, promueve la mejora continua y demuestra su compromiso mediante lo siguiente:

a) el establecimiento de la política de seguridad y privacidad de la información y los objetivos de seguridad y privacidad de la información, que sean compatibles con la dirección estratégica de la Universidad;

b) asegurando que los requisitos y controles del SGSPI estén integrados a los procesos de la Institución;

c) asegurando la disponibilidad de recursos para un SGSPI eficaz. Los recursos necesarios para el SGSPI incluyen: recursos financieros, personal, instalaciones, infraestructura técnica.

La necesidad de recursos depende del contexto de la institución, tal como el tamaño, complejidad y requisitos internos y externos. La revisión por la dirección proporciona información que indica si los recursos son suficientes para la Universidad;

d) la alta dirección debe comunicar la necesidad de gestión de la seguridad y privacidad de la información en la Universidad y la necesidad de cumplir los requisitos del SGSPI.

e) la alta dirección debe asegurar que el SGSPI logre el(los) resultados previstos apoyando la implementación de todos los procesos de gestión de la seguridad y privacidad de la información, y en particular solicitando y revisando informes sobre el estado y la eficacia del SGSPI. Estos informes se pueden obtener de mediciones, revisiones por la dirección e informes de auditoría. La alta dirección también puede establecer objetivos de desempeño para el personal clave involucrado en el SGSPI;

f) la alta dirección dirige y apoya a las personas de la Universidad que están involucradas directamente con la seguridad y privacidad de la información y el SGSPI. No hacerlo puede tener un impacto negativo sobre la eficacia del mismo.

La retroalimentación de la alta dirección incluye la forma como las actividades planificadas están alineadas con las necesidades estratégicas de la Universidad y también la priorización de las diferentes actividades en el SGSPI;

g) la alta dirección hace una valoración de las necesidades de recursos durante las revisiones por la dirección, establece los objetivos para la mejora continua y hace seguimiento a la eficacia de las actividades planificadas;

Sede Central / Av. Pastrana Borrero - Cra. 1
Sede Administrativa / Cra. 5 No. 23 - 40
www.usco.edu.co / Neiva - Huila
PBX: 875 4753
PBX: 875 3686
Línea Gratuita Nacional: 018000 968722

h) la alta dirección apoya a las personas a las cuales se les han asignado roles y responsabilidades relacionadas con la gestión de la seguridad y privacidad de la información, de manera que estén motivadas y estén en capacidad de dirigir y apoyar actividades de seguridad de la información dentro de su proceso.

Está disponible como información documentada en el Portal Institucional https://www.usco.edu.co/es/transparencia/ plan de desarrollo institucional y sus modificaciones, plan de acción de ejecución del plan de desarrollo, plan de capacitación institucional, plan estratégico de tecnologías de la información y de las comunicaciones.

5.2. Política de Seguridad y Privacidad de la Información

La política de seguridad y privacidad de la información describe la importancia estratégica del SGSPI y está disponible como información documentada. La política dirige las actividades de seguridad y privacidad de la información en la Institución.

La política expresa cuáles son las necesidades de seguridad y privacidad de la información en el contexto real y contiene declaraciones de intención de alto nivel y orientación concerniente a seguridad y privacidad de la información.

Todas las otras políticas, procedimientos, actividades y objetivos relacionados con seguridad y privacidad de la información están alineados con la política de seguridad y privacidad de la información.

La política de seguridad y privacidad de la información refleja la misionalidad de la Universidad, su cultura, cuestiones e inquietudes con relación a la seguridad y privacidad de la información. El alcance de la política de seguridad y privacidad de la información está de acuerdo con el propósito y cultura de la institución y busca un equilibrio entre su legibilidad y su integridad

La política de seguridad y privacidad de la información referencia los objetivos de seguridad y privacidad de la información para la Universidad y contiene una declaración clara de la alta dirección con relación a su compromiso de cumplir los requisitos relacionados con seguridad y privacidad de la información. Así mismo, la alta dirección apoya la mejora continua en todas las actividades. Se incluye este principio en la política, de manera que las personas dentro del alcance del SGSPI estén conscientes de él.

La política de seguridad y privacidad de la información se comunica a todas las personas que están dentro del alcance del SGSPI. Por tanto, su formato y lenguaje son apropiados para que lo puedan entender fácilmente todos los receptores, y está disponible como información documentada. Ver Resolución No. 085 de 2021 política y objetivos del SGSI.

Sede Central / Av. Pastrana Borrero - Cra. 1
Sede Administrativa / Cra. 5 No. 23 - 40
www.usco.edu.co / Neiva - Huila
PBX: 875 4753
PBX: 875 3686
Línea Gratuita Nacional: 018000 968722

5.3. Roles, responsabilidades y autoridades

La alta dirección asegura que las responsabilidades y autoridades para los roles pertinentes a la seguridad y privacidad de la información se asignan y comunican en toda la institución, con la finalidad de asegurar la conformidad del SGSPI con los requisitos de la NTC ISO IEC 27001 y NTC ISO IEC 27701 y asegurar que se reporte a la alta dirección el desempeño del SGSPI.

La alta dirección asegura que las autoridades y responsabilidades por el SGSPI se asignen de manera que el sistema de gestión cumpla los requisitos establecidos en la NTC ISO IEC 27001 y NTC ISO IEC 27701.

Se asignan las siguientes responsabilidades y las autoridades relacionadas con las actividades de seguridad y privacidad de la información:

a) coordinar el establecimiento, implementación, mantenimiento, reporte de desempeño y mejora del SGSPI;

b) asesorar con relación a la valoración y tratamiento de riesgos de seguridad de la información;

c) diseñar procesos y sistemas de seguridad y privacidad de la información;

d) establecer estándares acerca de la determinación, configuración y operación de controles de seguridad y privacidad de la información;

e) gestionar los incidentes de seguridad y privacidad de la información; y

f) revisar y auditar el SGSPI;

g) a parte de los roles relacionados específicamente con seguridad y privacidad de la información, las responsabilidades y autoridades de seguridad de la información pertinentes se incluyen dentro de otros roles. Por ejemplo, las responsabilidades de seguridad y privacidad de la información se incorporan en los roles de: líderes de procesos, dueños de información y activos asociados.

h) las funciones o personas que coordinan la seguridad y privacidad de la información: dueños de riesgos, grupo de profesionales CITCD; y usuarios de información.

Los roles, responsabilidades y autoridades dentro del SGSPI se encuentran documentados en AP-THU-DA-03 ROLES, RESPONSABILIDADES Y AUTORIDADES DE LA INSTITUCIÓN.

Sede Central / Av. Pastrana Borrero - Cra. 1
Sede Administrativa / Cra. 5 No. 23 - 40
www.usco.edu.co / Neiva - Huila
PBX: 875 4753
PBX: 875 3686
Línea Gratuita Nacional: 018000 968722

6. PLANIFICACIÓN

6.1. Acciones para abordar riesgos y oportunidades

La gestión de riesgos es la columna vertebral de la gestión de seguridad y privacidad de la información de la Universidad Surcolombiana, para identificar sus

necesidades con respecto al SGSPI con la finalidad de proteger sus activos de información de las amenazas y vulnerabilidades a las que están expuestos y proponer las medidas adecuadas para mitigar dichos riesgos.

En ese sentido, la información y otros activos asociados bajo el alcance del sistema de gestión de seguridad y privacidad de la información deberán ser sometidos a un proceso de análisis y gestión de riesgos que incluye la valoración de los riesgos de seguridad y privacidad de la información, su tratamiento y los criterios de aceptación del riesgo para identificar los niveles de riesgo aceptables. La descripción de la metodología para la gestión de riesgos de seguridad y privacidad de la información se documenta en ES-GSI-DA-01 METODOLOGÍA PARA LA GESTIÓN DE RIESGOS.

La identificación y priorización de los activos de información y otros activos asociados se documenta en ES-SGI-MR-05 MATRIZ DE INVENTARIO DE ACTIVOS DE LA INFORMACIÓN y ES-SGI-MR-08 REGISTRO ACTIVOS DE INFORMACIÓN-RAI

Las actividades de valoración de riesgos (identificación, análisis y evaluación) y tratamiento se documentan en ES-GSI-MR-06 MATRIZ RIESGOS.

Las actividades de comunicación y consulta, monitoreo y revisión, se realizan a través de los lineamientos definidos en los apartados 7.4 y 9.1 de este documento. De igual manera, la información relacionada a riesgos y oportunidades es una entrada a la revisión por la Dirección, definida en el apartado 9.3 de este documento.

6.2. Objetivos de seguridad y privacidad de la información

La Universidad Surcolombiana establece los objetivos y los planes de seguridad y privacidad de la información para cumplirlos en las funciones y niveles pertinentes.

Los objetivos de seguridad y privacidad de la información ayudan a implementar las metas estratégicas de la Universidad y la política de seguridad y privacidad de la información. De este modo, los objetivos del SGSPI son los objetivos de seguridad

Sede Central / Av. Pastrana Borrero - Cra. 1
Sede Administrativa / Cra. 5 No. 23 - 40
www.usco.edu.co / Neiva - Huila
PBX: 875 4753
PBX: 875 3686
Línea Gratuita Nacional: 018000 968722

y privacidad de la información para garantizar confidencialidad, integridad y disponibilidad de la información. Los objetivos de seguridad y privacidad de la información también ayudan a especificar y medir el desempeño de los controles y procesos de seguridad y privacidad de la información de acuerdo con la política de seguridad y privacidad de la información.

Los requisitos que se han tenido en cuenta al establecer los objetivos son los determinados cuando se comprende la organización y su contexto al igual que las necesidades y expectativas de las partes interesadas definidas en el capítulo 4 de este documento.

Los resultados de las valoraciones y tratamientos del riesgo se usan como entrada a la revisión regular de los objetivos, para asegurar que siguen siendo apropiados a las circunstancias de la Universidad.

Los objetivos de seguridad y privacidad de la información son:

a) coherentes con la política de seguridad y privacidad de la información;

b) medibles, si es posible; esto significa que es importante estar en capacidad de determinar si se ha cumplido o no un objetivo;

c) están vinculados a los requisitos de seguridad y privacidad de la información aplicables y a los resultados de la valoración y tratamiento de riesgos;

d) comunicados; y actualizados, cuando sea apropiado.

La Universidad conserva la información documentada sobre los objetivos de seguridad de la información y planifica cómo cumplirlos ver ES-GSI-MR-07 MATRIZ DE PLANIFICACIÓN PARA EL LOGRO DE OBJETIVOS DEL SGSPI

6.3. Planificación de los cambios

La planificación de cambios determina la necesidad de cambios en el Sistema de Gestión de Seguridad y Privacidad de la Información de la USCO con el fin de adaptarse a cambios en el entorno de la institución, así como para asegurarse de que cualquier cambio propuesto se planifica, introduce e implementa de una manera controlada.

Planificar un cambio de manera adecuada puede ayudar a evitar consecuencias negativas como reproceso, o cancelación o aplazamiento de un servicio; también puede dar lugar a consecuencias positivas como la reducción de salidas no conformes, o reducir los incidentes por errores humanos.

El propósito de planificar los cambios es mantener la integridad del Sistema de

Sede Central / Av. Pastrana Borrero - Cra. 1
Sede Administrativa / Cra. 5 No. 23 - 40
www.usco.edu.co / Neiva - Huila
PBX: 875 4753
PBX: 875 3686
Línea Gratuita Nacional: 018000 968722

Gestión de Seguridad y Privacidad de la Información y la capacidad de la Universidad para asegurar la disponibilidad, confidencialidad e integridad de la información y activos asociados durante el cambio.

La Institución considera acciones que puedan reducir el potencial de impactos negativos del cambio, como empezar realizando una prueba del cambio antes de su implementación plena, o determinar las acciones a tomar si el cambio no se implementa de manera exitosa.

El nivel de planificación y acción requeridos variará dependiendo de las consecuencias potenciales del cambio.

La información documentada de los cambios se encuentra documentados en la MATRIZ DE PLANIFICACIÓN DE CAMBIOS DEL SISTEMA DE GESTIÓN DE CALIDAD-SGC.

7. APOYO

7.1. Recursos

La Universidad determina y suministra los recursos para establecer, implementar, mantener y mejorar continuamente el SGSPI. Los recursos son fundamentales para llevar a cabo cualquier tipo de actividad. Las categorías de recursos incluyen:

a) personas para manejar y llevar a cabo las actividades;

b) tiempo para llevar a cabo las actividades y para permitir que los resultados se estabilicen antes de dar un nuevo paso;

c) recursos financieros para adquirir, desarrollar e implementar lo necesario;

d) información para apoyar decisiones, medir el desempeño de las acciones y mejorar el conocimiento; e

e) infraestructura y otros medios que se pueden adquirir o construir, tales como tecnología, herramientas y materiales, independientemente de si son productos de tecnología de la información o no.

Estos recursos se mantienen alineados con las necesidades del SGSPI y en consecuencia se adaptan cuando se requiera. La información documentada sobre esta actividad se plasma en el Plan de desarrollo institucional y sus respectivos planes de acción mediante Resoluciones y Acuerdos que los formalizan.

Sede Central / Av. Pastrana Borrero - Cra. 1
Sede Administrativa / Cra. 5 No. 23 - 40
www.usco.edu.co / Neiva - Huila
PBX: 875 4753
PBX: 875 3686
Línea Gratuita Nacional: 018000 968722

7.2. Competencia

La Universidad determina la competencia de las personas necesarias para el desempeño de seguridad y privacidad de la información y asegura que las personas sean competentes.

La competencia es la capacidad de aplicar conocimiento y habilidades para el logro de los resultados previstos, y está influenciada por el conocimiento, la experiencia y la sabiduría.

La competencia puede ser específica (por ejemplo, con relación a la tecnología o a áreas de gestión específicas) o generales (por ejemplo, habilidades blandas, fiabilidad y temas gerenciales y tecnológicos básicos). Se relaciona con las personas que trabajan bajo el control de la Institución. Esto significa que la competencia se gestiona para los empleados y para otras personas, según sea necesario.

La adquisición de competencias y habilidades nuevas o superiores se logra interna y externamente por medio de la experiencia, formación (por ejemplo, cursos, seminarios y talleres), tutorías o contratación de personas externas. Para competencia que solo es necesaria de manera temporal para una actividad específica o durante un período de tiempo corto, por ejemplo, para cubrir una necesidad temporal inesperada de personal interno, la USCO puede contratar recursos externos, cuya competencia se ha de describir y verificar.

La Universidad:

a) determina la competencia esperada para cada cargo y rol dentro del SGSPI y la documentan las diferentes Resoluciones que modifican el Manual de Funciones, requisitos y de competencias laborales y responsabilidades de la Universidad.

b) asigna los roles dentro del SGSPI AP-THU-DA-03 ROLES, RESPONSABILIDADES Y AUTORIDADES DE LA INSTITUCIÓN a las personas con la competencia requerida mediante:

   1) la identificación de las personas dentro de la organización, que tengan la competencia (por ejemplo, con base en su educación, experiencia o certificaciones);

   2) planifica e implementa acciones para que las personas dentro de la organización obtengan la competencia (por ejemplo, mediante formación, tutoría, reasignación de los empleados actuales); o

Sede Central / Av. Pastrana Borrero - Cra. 1
Sede Administrativa / Cra. 5 No. 23 - 40
www.usco.edu.co / Neiva - Huila
PBX: 875 4753
PBX: 875 3686
Línea Gratuita Nacional: 018000 968722

3) contrata nuevas personas que tengan la competencia (por ejemplo, por servicios);

c) evalúa la eficacia de las acciones

d) verifica que las personas sean competentes para sus roles, y AP-THU-FO-08- EVALUACIÓN DEL DESEMPEÑO LABORAL NIVEL PROFESIONAL

e) asegura que la competencia evolucione con el tiempo de acuerdo con las necesidades y que cumpla las expectativas. Ver AP-THU-FO-30 DETECCIÓN DE NECESIDADES A PARTIR DE FUNCIONES, AP-THU-FO-31 DETECCIÓN DE NECESIDADES POR DEPENDENCIAS, AP-THU-FO-32 DETECCIÓN DE NECESIDADES JEFES DE ÁREA, AP-THU-DA-04 FORMACIÓN DEL PERSONAL PARA LOS SISTEMAS DE GESTIÓN

La información documentada apropiada como evidencia de la competencia que afecta el desempeño de seguridad de la información y de cómo las personas pertinentes cumplen con esta competencia está almacenada en las carpetas de las historias laborales de los funcionarios.

7.3. Toma de conciencia

Las personas que realizan trabajo bajo el control de la Universidad toman conciencia de la política de seguridad de la información, su contribución a la eficacia del SGSPI, los beneficios de mejorar el desempeño de seguridad de la información y las implicaciones de no cumplir los requisitos del SGSPI.

La toma de conciencia de las personas que trabajan bajo el control de la Institución hace referencia a que tienen la comprensión y la motivación necesarias acerca de lo que se espera de ellos con relación a seguridad y privacidad de la información.

La toma de conciencia involucra a las personas que tienen que conocer, comprender, aceptar y apoyar los objetivos establecidos en la política de seguridad de la información; y permite seguir las reglas para ejecutar correctamente sus tareas diarias de apoyo a la seguridad y privacidad de la información. Adicionalmente, las personas que realizan trabajo bajo el control de la Universidad también necesitan conocer, comprender y aceptar las implicaciones de incumplir los requisitos del SGSPI. Las implicaciones pueden ser consecuencias negativas para la seguridad de la información o consecuencias indeseadas para la persona.

Una gran parte del personal de la entidad no necesita conocer el contenido detallado de la política, pero sí debe conocer, comprender, aceptar e implementar los objetivos y requisitos de seguridad de la información derivados de la política, que

Sede Central / Av. Pastrana Borrero - Cra. 1
Sede Administrativa / Cra. 5 No. 23 - 40
www.usco.edu.co / Neiva - Huila
PBX: 875 4753
PBX: 875 3686
Línea Gratuita Nacional: 018000 968722

afectan su rol laboral. Estos requisitos pueden estar incluidos en las normas o procedimientos cuyo cumplimiento se espera para la realización de su trabajo.

Cada empleado realiza la solicitud de formación de acuerdo con las necesidades de su cargo o rol dentro de la Universidad a través del diligenciamiento del formato AP-THU-FO-24 SOLICITUD INDIVIDUAL DE AVAL PARA CAPACITACIÓN.

La información documentada sobre esta actividad y su resultado son obligatorios solo en la forma y en la medida que la Universidad determine como necesaria para la eficacia de su sistema de gestión en las Resoluciones de aprobación anual del plan de capacitación.

7.4 Comunicación

La Universidad determina las necesidades de comunicaciones internas y externas relacionadas con el SGSPI.

La comunicación es un proceso clave dentro del SGSPI, y es necesaria con las partes interesadas internas y externas. Puede ser entre las partes interesadas internas a todos los niveles de la Institución o entre ésta y las partes externas interesadas. La comunicación se puede iniciar dentro de la organización o por una parte externa interesada.

La comunicación determina qué contenido es necesario comunicar, por ejemplo, políticas de seguridad de la información, objetivos, procedimientos, sus cambios, conocimiento de los riesgos de seguridad de la información, requisitos para los proveedores y retroalimentación sobre el desempeño de seguridad de la información; el momento preferido u óptimo para las actividades de comunicación; quién está involucrado en las actividades de comunicación y cuál es la audiencia objetivo de cada esfuerzo de comunicación; quién va a iniciar las actividades de comunicación, por ejemplo, puede haber contenido específico para el cual se requiere que la comunicación la inicie una persona u organización específica; y qué procesos están impulsando o iniciando actividades de comunicación, y a qué procesos están dirigidas las actividades de comunicación o son afectados por ellas. La comunicación se lleva a cabo regularmente o cuando surjan necesidades de divulgación de información. Puede ser proactiva o reactiva.

El cumplimiento de este requisito se encuentra como información documentada en ES-CMU-MR-01 MATRIZ DE COMUNICACIÓN.

7.5 Información documentada

La Universidad determina la información documentada en el SGSPI como lo determinan las normas NTC ISO IEC 27001 y la NTC ISO IEC 27701 y en general toda aquella que ha determinado como necesaria para la eficacia del SGSPI.

Sede Central / Av. Pastrana Borrero - Cra. 1
Sede Administrativa / Cra. 5 No. 23 - 40
www.usco.edu.co / Neiva - Huila
PBX: 875 4753
PBX: 875 3686
Línea Gratuita Nacional: 018000 968722

La información documentada para la Universidad es necesaria para definir y comunicar los objetivos, la política, directrices, instrucciones, controles, procesos, procedimientos de seguridad de la información y qué personas o grupos de personas se espera que lo hagan, y cómo se espera que lo lleven a cabo. También es necesaria la información documentada para las auditorías del SGSPI y para mantener un SGSPI estable cuando se cambian las personas que están en los roles clave. Además, es necesario contar con información documentada para registrar las acciones, decisiones y resultados de los procesos de SGSPI y los controles de seguridad de la información.

8. OPERACIÓN

8.1. Planificación y control de la operación

La Universidad planifica, implementa y controla los procesos para cumplir sus requisitos de seguridad de la información. Conserva la información documentada necesaria para obtener confianza en que los procesos se llevan a cabo de la forma planificada en la documentación de cada uno de los procesos. Controla los cambios planificados, revisa las consecuencias de los cambios no previstos y asegura que se identifiquen, definan y controlen los procesos contratados externamente.

La información documentada contiene:

- información acerca de objetivos, riesgos, requisitos y directrices de seguridad de la información;

- información acerca de los procesos y procedimientos por seguir; y

- registros de las entradas y los resultados de los procesos (incluidos planes y resultados de las actividades operacionales).

Una vez finalizada la implementación de los controles, los procesos son gestionados, se les hace seguimiento y se revisan para asegurar que continúan cumpliendo los requisitos determinados luego de comprender las necesidades y expectativas de las partes interesadas.

Los cambios en la operación del SGSPI pueden ser planificados o se pueden presentar de manera imprevista. Siempre que la Universidad haga cambios al SGSPI (como resultado de planificación o no previstos y valora las consecuencias potenciales de los cambios para controlar cualquier efecto adverso.

La Institución adquiere confianza en la eficacia de la implementación de los planes, mediante la documentación de las actividades y usando información documentada como entrada a los procesos de evaluación del desempeño especificados.

Sede Central / Av. Pastrana Borrero - Cra. 1
Sede Administrativa / Cra. 5 No. 23 - 40
www.usco.edu.co / Neiva - Huila
PBX: 875 4753
PBX: 875 3686
Línea Gratuita Nacional: 018000 968722

8.2. Evaluación de los riesgos para la seguridad de la información

La Universidad lleva a cabo valoraciones de riesgos de seguridad de la información y retiene información documentada sobre sus resultados.

Cuando se llevan a cabo valoraciones de riesgos de seguridad de la información, la Universidad ejecuta el proceso definido en el capítulo 6.1 de este documento. Estas valoraciones se ejecutan de acuerdo con un cronograma definido con antelación, o en respuesta a cambios significativos o a incidentes de seguridad de la información.

Los resultados de las valoraciones de seguridad de la información se retienen en información documentada como evidencia en ES-GSI-MR-06 MATRIZ RIESGOS.

La información documentada de las valoraciones de riesgos de seguridad de la información es esencial para el tratamiento de riesgos de seguridad de la información y es valiosa para la evaluación del desempeño.

8.3. Tratamiento de los riesgos para la seguridad de la información

Para tratar los riesgos de seguridad y privacidad de la información, la Universidad lleva a cabo el proceso de tratamiento de riesgos de seguridad de la información definido en el capítulo 6.1 de este documento. Durante la operación del SGSI, siempre que la valoración de riesgos esté actualizada se llevan a cabo actualizaciones en la aplicación del tratamiento de riesgos y se actualiza el plan de tratamiento de riesgos correspondiente. Se implementa nuevamente el plan de tratamiento de riesgos.

Los resultados del tratamiento de riesgos de seguridad de la información se retienen en información documentada como evidencia de que el proceso se ha llevado a cabo en la forma definida en ES-GSI-MR-06 MATRIZ RIESGOS.

9. EVALUACIÓN DE DESEMPEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

9.1. Seguimiento, medición, análisis y evaluación

La Institución evalúa el desempeño de la seguridad y privacidad de la información y la eficacia del SGSPI. El objetivo del seguimiento y de la medición es ayudar a la Universidad a juzgar, si el resultado planificado de las actividades de seguridad y privacidad de la información, incluidas la valoración del tratamiento de los riesgos, se han logrado en la forma prevista.

El seguimiento determina el estado de un sistema, proceso o actividad, mientras

Sede Central / Av. Pastrana Borrero - Cra. 1
Sede Administrativa / Cra. 5 No. 23 - 40
www.usco.edu.co / Neiva - Huila
PBX: 875 4753
PBX: 875 3686
Línea Gratuita Nacional: 018000 968722

que la medición es un proceso para determinar un valor. De manera que el seguimiento se puede lograr mediante una sucesión de mediciones similares durante un período de tiempo.

La información documentada relacionada al seguimiento y medición del SGSPI se encuentra en EV-CAL-FO-04 FICHA TÉCNICA DE INDICADORES DE GESTIÓN y ES-GSI-MR-08 MATRIZ DE SEGUIMIENTO MEDICIÓN ANÁLISIS Y EVALUACIÓN.

9.2 Auditoría interna

La evaluación del SGSPI se lleva a cabo a intervalos planificados por medio de auditorías internas y brinda a la alta dirección aseguramiento del estado de este.

Las auditorías internas brindan información acerca de si el SGSPI cumple los propios requisitos de la Universidad para su Sistema de seguridad y privacidad de la información al igual que los de la NTC ISO IEC 27001 y NTC ISO IEC 27701. Los requisitos propios de la Universidad incluyen:

a) los requisitos establecidos en la política y en los procedimientos de seguridad de la información;

b) los requisitos generados por el marco para establecimiento de objetivos de seguridad de la información, que incluyen los resultados del proceso de tratamiento de riesgos;

c) los requisitos legales y contractuales; y

d) los requisitos sobre la información documentada.

El programa de auditoría describe el marco general para el grupo de auditorías planificadas para la Universidad y se mantiene como información documentada al igual que sus resultados en: EV-CAL-FO-13 PROGRAMA DE AUDITORÍAS INTERNAS DE LOS SISTEMAS DE GESTIÓN, EV-CAL-FO-14 PLAN DE AUDITORIAS INTERNAS DE LOS SISTEMAS DE GESTIÓN, EV-CAL-FO-18 EVALUACIÓN DE AUDITORES INTERNOS DE LOS SISTEMAS DE GESTIÓN, EV-CAL-FO-16 INFORME DE AUDITORÍA INTERNA DE LOS SISTEMAS DE GESTIÓN, EV-CAL-PR-03 AUDITORÍAS INTERNAS DE LOS SISTEMAS DE GESTIÓN

9.3. Revisión por la dirección

El propósito de la revisión por la dirección es asegurar la idoneidad, adecuación y eficacia continuas del SGSPI. La idoneidad se refiere a la alineación continua con los objetivos de la Universidad, mientras que la adecuación y la eficacia se refieren

Sede Central / Av. Pastrana Borrero - Cra. 1
Sede Administrativa / Cra. 5 No. 23 - 40
www.usco.edu.co / Neiva - Huila
PBX: 875 4753
PBX: 875 3686
Línea Gratuita Nacional: 018000 968722

al diseño adecuado y a la integración organizacional del SGSPI, al igual que a la implementación eficaz de los procesos y controles que son promovidos por el mismo.

La alta dirección revisa el SGSPI en los intervalos planificados y se encuentra como información documentada en ES-DE-FO-02 INFORME DE REVISIÓN POR LA DIRECCIÓN

10. MEJORA

10.1. Mejora continua

La Universidad Surcolombiana mejora continuamente la idoneidad, la adecuación y la eficacia del SGSI de acuerdo al procedimiento EV-CAL-PR-02 ACCIONES CORRECTIVAS, MEJORAS U OPORTUNIDADES DE MEJORA

10.2 No conformidad y acción correctiva

Una no conformidad es el incumplimiento de un requisito del SGSPI. Los requisitos son las necesidades o expectativas que están establecidas, son implícitas u obligatorias.

La Universidad reacciona a las no conformidades, las evalúa y emprende las correcciones y las acciones correctivas si son necesarias y las trabaja a través del procedimiento EV-CAL-PR-02 ACCIONES CORRECTIVAS, MEJORAS U OPORTUNIDADES DE MEJORA

11. CONTROLES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Los controles de seguridad y privacidad de la información se definen en el Manual de Políticas de Seguridad y Privacidad de la Información.

Sede Central / Av. Pastrana Borrero - Cra. 1
Sede Administrativa / Cra. 5 No. 23 - 40
www.usco.edu.co / Neiva - Huila
PBX: 875 4753
PBX: 875 3686
Línea Gratuita Nacional: 018000 968722