PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Control de Cambios

Version	Fecha	Descripción	Elaboró
1.0	30-01-2020	Version Inicial	Mag. Martha Liliana Hermosa Trujillo Ing. Isabel Cristina Cleves Rodriguez
2.0	26-01-2021	Actualización	Mag. Martha Liliana Hermosa Trujillo Ing. Isabel Cristina Cleves Rodriguez German Andrés Sánchez Ortegón

TABLA DE CONTENIDO

TABLA DE CUADROS

1. OBJETIVO

Definir las actividades del plan de Seguridad y Privacidad de la Información para la implementación, gestión, verificación y mejora continua del Sistema de Gestión de Seguridad de la Información – SGSI de la Universidad Surcolombiana.

2. ALCANCE

El alcance del Plan de Seguridad y Privacidad de la Información se aplica a los procesos de la Universidad Surcolombiana, en concordancia con el alcance del Sistema de Gestión de Seguridad de la Información – SGSI.

3. MARCO NORMATIVO Y REFERENCIA

Los siguientes documentos de referencia, normativos, vinculantes hacen parte integral del presente documento, sus consideraciones, alcance y construcción:

- **Constitución Política de Colombia 1991**. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data. Artículo 20. Libertad de Información.
- **Decreto 612 de 2018,** Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las Entidades del Estado.
- **Decreto 1008 de 2018**, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.
- **Ley 23 de 1982** de Propiedad Intelectual - Derechos de Autor.
- **Ley 594 de 2000** - Ley General de Archivos.
- **Ley 527 de 1999**, por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.
- **Ley Estatutaria 1266 de 2008**, por la cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales.
- **Ley 1273 de 2009**, "Delitos Informáticos" protección de la información y los datos.
- **Ley 1437 de 2011**, "Código de procedimiento administrativo y de lo contencioso administrativo".
- **Ley 1581 de 2012**, "Protección de Datos personales".
- **Decreto 2609 de 2012**, por la cual se reglamenta la ley 594 de 200 y ley 1437 de 2011

- **Decreto 1377 de 2013**, por la cual se reglamenta la ley 1581 de 2012
- **Ley 1712 de 2014,** "De transparencia y del derecho de acceso a la información pública nacional"
- **Ley 962 de 2005**. "Simplificación y Racionalización de Trámite. Atributos de seguridad en la Información electrónica de entidades públicas;"
- **Ley 1150 de 2007**. "Seguridad de la información electrónica en contratación en línea"
- **Ley 1341 de 2009**. "Tecnologías de la Información y aplicación de seguridad".
- **Decreto 2952 de 2010**. "Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008"
- **Decreto 886 de 2014**. "Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012"
- **Decreto 1083 de 2015**. "Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012"
- **CONPES 3701 de 2011** Lineamientos de Política para Ciberseguridad y Ciberdefensa
- **CONPES 3854 de 2016** Política Nacional de Seguridad digital.
- **Resolución 79B de 2020.** Por la cual se crea el Comité de Seguridad de la Información de la Universidad Surcolombiana
- **Resolución 289 de 2019.** Por la cual se adopta la Política General del Modelo de Seguridad y Privacidad de la Información y el Manual de la Política Seguridad y Privacidad de la Información de la Universidad Surcolombiana
- **Resolución 290 de 2019.** Por la cual se adopta la Política de tratamiento y Protección de datos personales de la Universidad Surcolombiana
- **Resolución P4042 de 2019.** Por medio de la cual se crea, organiza y conforma un grupo interno de trabajo de seguridad de la Información y Protección de Datos personales y se asignan funciones de coordinador a un empleado público de la Universidad Surcolombiana
-

3. REQUISITOS TÉCNICOS

- NTC ISO IEC 27001 Sistemas de gestión de la seguridad de la información
- GTC ISO IEC 27002 Tecnología de la Información. Técnicas de Seguridad. Código de Práctica para Controles de Seguridad de la Información
- NTC ISO lEC 27005 Tecnología de la Información. Técnicas de Seguridad. Gestión del Riesgo en la Seguridad de la Información.
- NTC ISO 19011 Directrices para la Auditoria de los Sistemas de Gestión.
- Modelo de Seguridad y Privacidad de la Información, Ministerio de Tecnologías y Sistemas de Información.
- Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5 - Diciembre de 2020

4. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la administración de la Universidad Surcolombiana con respecto a la protección de los activos de información (funcionarios, contratistas, terceros, aprendices, practicantes, docentes, estudiantes, la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Entidad y apoyan la implementación del Modelo de Seguridad y Privacidad de la Información; por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información..

5. OBJETIVOS DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Universidad Surcolombiana, para asegurar la dirección estratégica de la Entidad, establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información, estos últimos correspondientes a:

- ✓ Minimizar el riesgo de los procesos misionales de la entidad.
- ✓ Cumplir con los principios de seguridad de la información.
- ✓ Cumplir con los principios de la función administrativa.
- ✓ Mantener la confianza de los funcionarios, contratistas y terceros.
- ✓ Apoyar la innovación tecnológica.

- ✓ Implementar el sistema de gestión de seguridad de la información.
- ✓ Proteger los activos de información.
- ✓ Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- ✓ Fortalecer la cultura de seguridad de la información en los funcionarios, contratistas, terceros, aprendices, practicantes, docentes, estudiantes de la Universidad Surcolombiana y la ciudadanía en general.
- ✓ Garantizar la continuidad del negocio frente a incidentes.

6. ALCANCE DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

EL SGSI es aplicable a los activos de información de todos los procesos de la Universidad Surcolombiana, a las sedes de Neiva Pitalito, Garzón y la Plata, comprende las políticas, procedimientos y controles para la preservación de confidencialidad, integridad y disponibilidad de la información, en concordancia con la declaración de aplicabilidad y el alcance definido para el diseño y prestación de servicios de formación, investigación y proyección social y proyectos especiales en educación superior a través de programas de pregrado y posgrado.

7. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

El Comité de Seguridad de la Información, fue creado en la Universidad Surcolombiana mediante acto administrativo Resolución 079B del 17 de febrero del año 2020 como órgano responsable de la implementación, aplicabilidad y funcionalidad de la Política de Seguridad de la Información, Política de Protección de Datos Personales y del Plan de Contingencia y Continuidad Informático, y el cual tiene dentro de sus funciones garantizar, hacer seguimiento y/o verificación de la implementación del Sistema de Gestión de Seguridad de la Información SGSI de la Universidad Surcolombiana.

8. PLAN DE IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Plan de implementación para la dimensión de Seguridad y Privacidad de la Información comprende el siguiente cronograma:

Gestión	Actividades	Tareas	Responsable de la Tarea	Fechas Programación Tareas	
				Fecha Inicio	Fecha Final
Activos de Información	Definir lineamientos para el levantamiento de activos de información	Elaboración metodología e instrumento de levantamiento de activos de información	Grupo de Seguridad de la Información	01/2021	03/2021
	Levantamiento Activos de Información	Socializar la Matriz de Inventarios de Activos de Información.	Grupo de Seguridad de la Información	01/2021	03/2021
		Validar activos de información en el instrumento levantado en la vigencia anterior	Lider del Proceso- Grupo de Seguridad de la Información	01/2021	02/2021
		Identificar nuevos activos de información en cada proceso	Líder del Proceso- Grupo de Seguridad de la Información	01/2021	12/2021
		Revisar la Matriz de Activos de Información y retroalimentar a los procesos con las modificaciones.	Grupo de Seguridad de la Información	01/2021	12/2021
		Realizar correcciones a la Matriz de activos de Información, Cambios físicos de la ubicación de activos de información	Líder del Proceso	01/2021	12/2021
		Realizar informe de actualización a los activos de información por alguna de las siguientes novedades: Actualizaciones al proceso al que pertenece el activo, Adición de actividades al proceso, Inclusión de un nuevo activo, Cambios o migraciones de sistemas de información en donde se almacenan o reposan activos de la ubicación ya inventariados, Materialización de riesgos que cambien la criticidad del activo.	Líderes de los Proceso	01/2021	12/2021
	Publicación de Activos de Información	Validar y aceptar los activos de información para su publicación en el Portal Institucional	Líder del Proceso - Grupo de Seguridad de la Información	01/2021	12/2021
		Consolidar el instrumento de activos de Información.	Grupo de Seguridad de la Información	01/2021	03/2021

Gestión	Actividades	Tareas	Responsable de la Tarea	Fechas Programación Tareas	
				Fecha Inicio	Fecha Final
		Publicar los instrumentos de activos de información consolidado	Centro de Información, Tecnologías y Control Documental	03/2021	12/2021
	Registros activos de información ley 1712	Actualizar el instrumento de Registro Activos de Información con el insumo de los instrumentos de activos de Información.	Grupo de Seguridad de la Información	01/2021	12/2021
		Enviar a control de legalidad el instrumento de Registro Activos de información.	Grupo de Seguridad de la Información - Oficina Asesora Jurídica.	01/2021	12/2021
		Aval para la Publicación del Registro Activos de Información en el sitio web de la Entidad.	Oficina Asesora Jurídica	01/2021	12/2021
	Reporte Datos Personales	Reportar al responsable de Seguridad de la Información y Oficial de Datos personales la información recolectada en el instrumento de activos de información, correspondiente a bases de datos .	Grupo de Seguridad de la Información	01/2021	12/2021
Gestión de Riesgos	Actualización de lineamientos de riesgos	Actualizar política y guía metodológica de gestión de riesgos	Grupo de Seguridad de la Información	01/2021	12/2021
	Sensibilización	Socialización de la Guía Metodológica de Gestión de Riesgos de Seguridad y privacidad de la Información	Grupo de Seguridad de la Información	01/2021	12/2021
	Identificación de Riesgos y Oportunidades de Seguridad y Privacidad de la Información	Identificación, Análisis y Evaluación de Riesgos y Oportunidades - Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Grupo de Seguridad de la Información	01/2021	12/2021
		Realimentación, revisión y verificación de los riesgos identificados (ajustes)	Grupo de Seguridad de la Información	01/2021	12/2021
	Aceptación de Riesgos Identificados	Aceptación, aprobación Riesgos y Oportunidades identificados y planes de tratamiento	Comité de Seguridad de la Información	01/2021	12/2021

Gestión	Actividades	Tareas	Responsable de la Tarea	Fechas Programación Tareas	
				Fecha Inicio	Fecha Final
	Evaluación de riesgos residuales	Evaluación de riesgos residuales	Grupo de Seguridad de la Información	01/2021	12/2021
	Seguimiento Fase de Tratamiento	Seguimiento Estado plan de tratamiento de riesgos y oportunidades identificadas y verificación de evidencias	Grupo de Seguridad de la Información	01/2021	12/2021
	Mejoramiento	Identificación de oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos residuales	Grupo de Seguridad de la Información	01/2021	12/2021
		Actualización Guía Gestión de Riesgos Seguridad de la información, de acuerdo a los cambios solicitados.	Grupo de Seguridad de la Información	06/2021	12/2021
	Monitoreo y Revisión	Generación, presentación y reporte de indicadores	Grupo de Seguridad de la Información	01/2021	12/2021
Gestión de Incidentes de Seguridad de la Información	Elaboración de política y procedimiento de gestión de incidentes de seguridad	Elaboración del procedimiento de gestión de incidentes basados en la GTC ISO IEC 27035	Grupo de Seguridad de la Información	01/2021	03/2021
	Publicar y Socializar la política y el procedimiento actualizado de incidentes de seguridad de la información	Publicar la política y el procedimiento de gestión de incidentes de Seguridad de la Información	Grupo de Seguridad de la Información	02/2021	04/2021
		Socializar la política y el procedimiento de gestión de incidentes de Seguridad de la Información	Grupo de Seguridad de la Información	01/2021	12/2021
	Gestionar los incidentes de Seguridad de la Información identificados	Gestionar los incidentes de seguridad de la información de acuerdo a lo establecido en el procedimiento definido.	Grupo de Seguridad de la Información	01/2021	12/2021
	Eventos / vulnerabilidades	Realizar seguimiento a los informes de eventos y vulnerabilidades asociados a SGSI	Grupo de Seguridad de la Información	01/2021	12/2021

Gestión	Actividades	Tareas	Responsable de la Tarea	Fechas Programación Tareas	
				Fecha Inicio	Fecha Final
Plan de Cambio y Cultura de Seguridad y Privacidad de la Información	Elaborar el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información	Elaborar el documento del Plan de Gestión de Cultura Organizacional en Apropiación del SGSI	Oficial de Seguridad de la Información- Grupo de Seguridad de la Información	02/2021	04/2021
		Publicar y Socializar el Plan de Gestión de Cultura Organizacional en Apropiación del SGSI	Oficial de Seguridad de la Información- Grupo de Seguridad de la Información	01/2021	12/2021
	Ejecutar el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información	Implementar las estrategias del Plan de Gestión de Cultura Organizacional en Apropiación del SGSI	Oficial de Seguridad de la Información- Grupo de Seguridad de la Información	01/2021	12/2021
	Analizar el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información	Analizar los instrumentos de medición del Plan de Gestión de Cultura Organizacional en Apropiación del SGSI	Oficial de Seguridad de la Información- Grupo de Seguridad de la Información	03/2021	06/2021
	Creación de la Matriz de verificación de Requisitos Legales de Seguridad de la Información	Crear la Matriz de verificación de Requisitos Legales de Seguridad de la Información	Oficina Asesora Jurídica, Oficial de Seguridad de la Información	01/2021	12/2021
	Revisión de la Matriz de verificación de Requisitos Legales de Seguridad de la Información	Evidenciar el cumplimiento de los Requisitos Legales de Seguridad de la Información	Oficina Asesora Jurídica, Oficial de Seguridad de la Información	01/2021	12/2021
Plan de Continuidad del Negocio	Documentación del Análisis de Impacto de la Operación	Realizar Análisis de Impacto del Negocio	Comité de Seguridad de la Información	06/2021	07/2021
		Socialización del Análisis de Impacto del Negocio	Grupo de Seguridad de la Información - Equipo de Continuidad del Negocio	06/2021	07/2021

Gestión	Actividades	Tareas	Responsable de la Tarea	Fechas Programación Tareas	
				Fecha Inicio	Fecha Final
	Documentación de Valoración de Riesgos de Interrupción	Elaboración del documento de Valoración de Riesgos de interrupción para el plan de continuidad de la operación	Grupo de Seguridad de la Información - Equipo de Continuidad del Negocio	06/2021	07/2021
		Socialización del documento de Valoración de Riesgos de interrupción	Grupo de Seguridad de la Información - Equipo de Continuidad del Negocio	07/2021	12/2021
	Documentación de Estrategias de Continuidad	Actualización del documento Estrategias de Continuidad de la Operación	Grupo de Seguridad de la Información - Equipo de Continuidad del Negocio	07/2021	12/2021
		Publicación Estrategias de Continuidad de la Operación	Grupo de Seguridad de la Información - Equipo de Continuidad del Negocio	07/2021	12/2021
	Documentación del Plan de continuidad de la Operación	Crear Documentación del Plan de continuidad de la Operación	Grupo de Seguridad de la Información - Equipo de Continuidad del Negocio	06/2021	12/2021
		Aprobación del Plan de continuidad de la Operación	Grupo de Seguridad de la Información - Equipo de Continuidad del Negocio	07/2021	12/2021
Acciones correctivas mejoras SGSI	Reporte del estado de las Acciones Correctivas y Oportunidades de Mejora	Generar reporte del estado actual de las AC y OM	Calidad	08/2021	12/2020
		Solicitar realizar las ACPM o plan de tratamiento según sea requerido.	Calidad	08/2021	12/2021
	Generar observaciones o recomendaciones a los acompañamientos realizados a los Procesos	Hacer seguimiento a las observaciones o recomendaciones dejadas a los acompañamientos realizados a los Procesos	Calidad- Oficina Control Interno	08/2021	12/2021

Gestión	Actividades	Tareas	Responsable de la Tarea	Fechas Programación Tareas	
				Fecha Inicio	Fecha Final
Planeación	Revisión Manual Políticas de Seguridad de la Información y Política de Protección de Datos Personales y Resoluciones de Seguridad de la Información y protección de Datos personales	Actualizar Manual Políticas de Seguridad de la Información y Resolución de Seguridad de la información	Oficial de Seguridad de la Información	03/2021	05/2021
		Informe cumplimiento de los controles por dominios asignados (Políticas, Manual, etc.)	Oficial de Seguridad de la Información	03/2021	05/2021
Gobierno Digital	Gobierno Digital	Actualizar el documento de autodiagnóstico de la entidad en la implementación de Seguridad y Privacidad de la Información.	Oficial de Seguridad de la Información	02/2021	04/2021
		Revisar y alinear la documentación del SGSI de la Universidad al MSPI, de acuerdo con la Normatividad vigente.	Oficial de Seguridad de la Información	02/2021	12/2021
		Revisar el avance de implementación del Plan de Seguridad Digital en la Entidad	Oficial de Seguridad de la Información- Grupo de seguridad de la Información	01/2021	12/2021
		Reuniones de Socialización de los avances de la implementación del plan de Seguridad Digital y la Estrategia del Modelo de Seguridad y Privacidad de la Información	Oficial de Seguridad de la Información	02/2021	12/2021
Auditorías Internas y Externas	Participación en las auditorías internas y externas de la norma NTC ISO IEC 27001	Participar en las auditorías internas y externas de la norma NTC ISO IEC 27001	Todos los procesos	06/2021	12/2021
Revisión de los controles del anexo A la norma NTC	Revisión de los controles del anexo A de la norma NTC ISO IEC 27001	Aplicar la herramienta diseñada para realizar la validación del cumplimiento los controles del anexo A de la norma NTC ISO IEC 27001.	Oficial de Seguridad de la Información	01/2021	12/2021

Gestión	Actividades	Tareas	Responsable de la Tarea	Fechas Programación Tareas	
				Fecha Inicio	Fecha Final
ISO IEC 27001					
Indicadores SGSI	Provisión de información a los indicadores de medición del SGSI	Formular, Implementar y actualizar los indicadores del SGSI	Oficial de Seguridad de la Información	06/2021	12/2021
		Reportar indicadores	Líderes de Procesos	04/2021	12/2021
Vulnerabilidades	Definir lineamientos para ejecutas las pruebas de vulnerabilidades y pentest	Definir los lineamientos y el alcance para la realización de pruebas de vulnerabilidades	Grupo interno de seguridad de la Información. Director Centro de Información, Tecnologías y control documental	03/2021	04/2021
	Contratar Análisis de Vulnerabilidades y Pentest	Definir estudios previos y procesos de contratación para realizar el pentest y análisis de vulnerabilidades teniendo en cuenta el alcance y la metodología	Grupo interno de seguridad de la Información. Director Centro de Información, Tecnologías y control documental	03/2021	04/2021
	Ejecutar las pruebas de vulnerabilidades y pentest	Ejecución de las pruebas de vulnerabilidades y pentest de acuerdo al alcance y la metodología establecida	Consultor – Grupo de Seguridad de la Información	03/2021	06/2021
	Ejecutar plan de remediación	Ejecutar el plan de remediación sobre los sistemas y plataforma de acuerdo a los resultados del análisis de vulnerabilidades y pentest	Grupo de Seguridad de la Información – Director Centro de Información, Tecnologías y Control Documental	06/2021	12/2021
Protección de datos personales	Implementar programa de gestión de datos personales	Aprobar, implementar y monitorear el Programa integral de gestión de datos personales	Oficial De Seguridad y Comité de Seguridad de la Información	02/2021	12/2021

Tabla1. Plan de implementación del modelo de seguridad y privacidad de la información.

9. DOCUMENTOS ASOCIADOS

- Política General de Seguridad y privacidad de la Información Universidad Surcolombiana
- Manual de la Política General del Modelo de Seguridad y Privacidad de la Información Universidad Surcolombiana
- Política de Tratamiento de Protección de Datos personales Universidad Surcolombiana

10. RESPONSABLE DEL DOCUMENTO

Responsable de Seguridad de la Información y Oficial de Protección de Datos Personales.

11. TERMINOS Y DEFINICIONES

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

Activo de Información: En relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la Organización

Alta Dirección: Persona o grupo de personas que dirige y controla una organización (3.50) al nivel más alto

Amenaza: Causa potencial de un incidente no deseado, que puede causar daños a un sistema u organización

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y para determinar el nivel de riesgo

Ataque: Intentar destruir, exponer, alterar, deshabilitar, robar u obtener acceso no autorizado o hacer un uso no autorizado de un activo

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencia de auditoría y evaluarla objetivamente para determinar hasta qué punto se cumplen los criterios de auditoría.

Comunicación y Consulta de Riesgos.: Conjunto de procesos continuos e iterativos que una organización lleva a cabo para proporcionar, compartir u obtener información, y para dialogar con las partes interesadas con respecto a la gestión de riesgos

Confiabilidad: Propiedad de la conducta y resultados esperados consistentes

Confidencialidad: Propiedad por la que la información no se pone a disposición o se divulga a personas, entidades o procesos no autorizados

Conformidad: Cumplimiento de un requisito

Consecuencia: Resultado de un evento que afecta a los objetivos

Continuidad de la Seguridad de la Información: Procesos y procedimientos para garantizar la continuidad de las operaciones de seguridad de la información

Control de Acceso: medios para garantizar que el acceso a los activos esté autorizado y restringido según los requisitos comerciales y de seguridad"

Control: Medida que modifica un riesgo

Criterios de Riesgo: Términos de referencia contra los cuales se evalúa la importancia del riesgo

Disponibilidad: Propiedad de ser accesible y utilizable a solicitud de una entidad autorizada

Estándar de Implementación de Seguridad: Documento que especifica formas autorizadas para realizar la seguridad.

Evaluación de Riesgos: Proceso global de identificación de riesgos, análisis de riesgos y evaluación de riesgos

Evento de Seguridad de la Información: Ocurrencia identificada de un sistema, servicio o estado de red que indica un posible incumplimiento de la política de seguridad de la información o falla de los controles o una situación desconocida que puede ser relevante para la seguridad

Evento: Ocurrencia o cambio de un conjunto particular de circunstancias

Gestión de Incidentes de Seguridad de la Información: Conjunto de procesos para detectar, informar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, se compone de la evaluación y el tratamiento de riesgos

Gobernanza de la Seguridad de la Información: Sistema por el cual las actividades de seguridad de la información de una organización son dirigidas y controladas

Identificación de Riesgo: Proceso de búsqueda, reconocimiento y descripción de riesgos

Incidente de Seguridad de la Información: Un evento o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones comerciales y amenazar la seguridad de la información

Indicador: Medida que proporciona una estimación o evaluación.

Información Documentada: Se refiere a la información necesaria que una organización debe controlar y mantener actualizada tomando en cuenta y el soporte en que se encuentra. La información documentada puede estar en cualquier formato (audio, video, ficheros de texto etc.) así como en cualquier tipo de soporte o medio independientemente de la fuente de dicha información.

Instalaciones de Procesamiento de Información: Cualquier sistema de procesamiento de información, servicio o infraestructura, o la ubicación física que lo alberga

Integridad: Propiedad de la exactitud y la integridad

Mejora Continua: Actividad recurrente para mejorar el rendimiento

Método de Medida: Secuencia lógica de operaciones, descrita genéricamente, utilizada en la cuantificación de un atributo con respecto a una escala específica

Monitoreo: Determinar el estado de un sistema, un proceso o una actividad

Necesidad de Información: Conocimiento necesario para gestionar objetivos, riesgos y problemas.

Nivel de Riesgo: Magnitud de un riesgo expresada en términos de la combinación de consecuencias y su probabilidad

No Conformidad: Incumplimiento de un requisito

Organización: Persona o grupo de personas que tiene sus propias funciones con responsabilidades, autoridades y relaciones para lograr sus objetivos

Política: Intenciones y dirección de una organización, según lo expresado formalmente por su alta dirección

Probabilidad: Posibilidad de que algo suceda

Proceso: Conjunto de actividades interrelacionadas o interactivas que transforman entradas en salidas

Proceso de Gestión de Riesgos: Aplicación sistemática de políticas de gestión procedimientos y prácticas a las actividades de comunicación, consulta, establecimiento del contexto e identificación, análisis, evaluación, tratamiento, seguimiento y revisión de riesgos

Propietario de Riesgo: Persona o entidad con la responsabilidad y autoridad para gestionar un riesgo (3.61)

Requisito: Necesidad o expectativa que se declara, generalmente implícita u obligatoria

Revisión: Actividad realizada para determinar la idoneidad, adecuación y eficacia de la materia para alcanzar los objetivos establecidos

Riesgo Residual: Riesgo restante después del tratamiento de riesgo

Riesgo: Efecto de la incertidumbre sobre los objetivos

Riesgo de seguridad de la información: Posibilidad de que una amenaza concreta que pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información; estos daños consisten en la afectación de la confidencialidad, integridad o disponibilidad de la información. Cuando la amenaza se convierta en una oportunidad se debe tener en cuenta en el beneficio que se genera.

Seguridad de Información: Preservación de la confidencialidad, integridad y disponibilidad de la información

Sistema de Gestión de Seguridad de la Información (SGSI) Profesional: Persona que establece, implementa, mantiene y mejora continuamente uno o más procesos del sistema de administración de seguridad de la información

Seguridad de la Información: Este principio busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano

Sistema De Gestión: Conjunto de elementos interrelacionados o interactivos de una organización para establecer políticas y objetivos y procesos para alcanzar esos objetivos

Sistema de Información: Conjunto de aplicaciones, servicios, activos de tecnología de la información u otros componentes de manejo de información

SGSI: Sistema de Gestión de Seguridad de la Información.

Tratamiento de Riesgo: Proceso para modificar riesgo

Vulnerabilidad: Debilidad de un activo o control que puede ser explotado por una o más amenazas