La educación es de todos

Mineducación

República de Colombia
Ministerio de Educación Nacional

INSOR
Instituto Nacional para Sordos

PLAN DE TRABAJO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN VIGENCIA 2019

Contenido

INTRODUCCIÓN

El Instituto Nacional para Sordos-INSOR presenta a la ciudadanía y a los grupos de interés el plan de seguridad y privacidad de la información para la vigencia 2019, donde se establece un conjunto de actividades, que permiten garantizar la protección y la privacidad de los datos preservando la confidencialidad, integridad y disponibilidad de la información, contribuyendo al cumplimiento de la misión y objetivos estratégicos de la entidad. Basados en la Norma Técnica Colombiana ISO 27001:2013 y lo establecido en el Decreto 1008 de 14 de junio 2018, donde se establece para las entidades del estado los habilitadores transversales: Seguridad de la información, Arquitectura de TI y Servicios Ciudadanos Digitales.

OBJETIVOS

Objetivo general

Preservar la confidencialidad, integridad y disponibilidad de la información del Instituto Nacional para Sordos-INSOR.

Objetivo Específico

1. Identificar los riesgos de seguridad y privacidad de la información de cada proceso del INSOR que puedan afectar la confidencialidad, integridad y disponibilidad de la información.
2. Realizar cumplimiento a la estrategia de gobierno digital y a lo dispuesto en la norma ISO 27001:2013.
3. Realizar campañas de sensibilización en seguridad y privacidad de la información para el INSOR.

ALCANCE

El plan de seguridad y privacidad de la información aplica a todos los procesos del Instituto Nacional para Sordos-INSOR, donde se desarrolle recolección, procesamiento, almacenamiento, recuperación, intercambio y consulta de información, al cumplimiento de la misión y objetivos estratégicos de la entidad.

DEFINICIONES

Administración del riesgo: Se entiende por administración de riesgos al proceso de identificación, control y minimización o eliminación, a un costo

aceptable, de los riesgos de seguridad que podrían afectar a la información. Dicho proceso es cíclico y debe llevarse a cabo en forma periódica.

Autenticación: Provisión de credenciales (usuario y contraseña) para poder acceder a recursos protegidos en equipos de cómputo.

Autenticidad: busca asegurar la validez de la información en tiempo, forma y distribución. Así mismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

Auditabilidad: define que todos los eventos de un sistema deben poder ser registrados para su control posterior.

Confiabilidad de la Información: es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

Confidencialidad: garantizar que todos los recursos informáticos estén protegidos contra uso no autorizado o revelaciones accidentales. La información deberá ser considerada como privada y restringida. Se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

Disponibilidad: garantizar que la información crítica y la capacidad de procesamiento puedan ser resguardadas y recuperadas rápida y completamente en caso de que ocurra alguna contingencia que interrumpa la continuación de las operaciones. Se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Evaluación del riesgo: Se entiende por evaluación de riesgos a la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, también se fundamenta en comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo, la probabilidad de que ocurran y su potencial impacto en la operatoria del Organismo.

Firewalls: son dispositivos de seguridad, que permiten filtrar contenidos y proteger las aplicaciones de accesos no autorizados o ataques de tipo hacker.

Incidente de seguridad: Un incidente de seguridad es un evento adverso en un sistema de computadores, o red de computadores, que compromete la confidencialidad, integridad o disponibilidad, la legalidad y confiabilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes.

Integridad: establecer mecanismos para garantizar que toda la información que se maneje se encuentre libre de errores y/o corrupción de cualquier índole. se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

Legalidad: referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.

Lugar seguro: Sitio físico o electrónico que protege la información de accesos no autorizados, perdida, robo, daño, fuga. Cuya recuperación es inmediata para personas autorizadas.

No repudio: se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

Protección a la duplicación: consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el Objeto de simular múltiples peticiones del mismo remitente original.

Sistema de Información: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

Responsable de Seguridad y privacidad de la información: Es la persona que cumple la función de supervisar el cumplimiento de la presente Política y de asesorar en materia de seguridad de la información a los integrantes del Organismo que así lo requieran.

Tecnología de la Información: Se refiere al hardware y software operados por el Organismo o por un tercero que procese información en su nombre, para llevar a cabo una función propia del Organismo, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

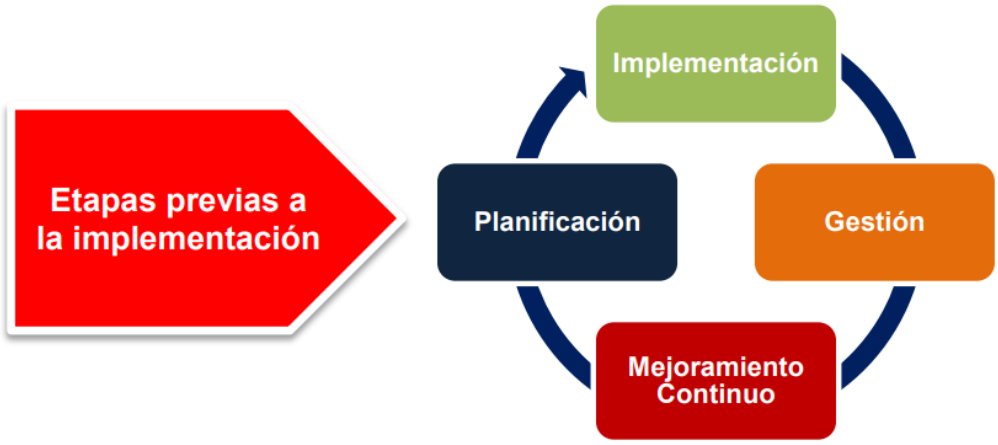
Tercero: Empresa con contrato temporal que presta servicios directos o indirectos, bien sea en las instalaciones del INSTITUTO NACIONAL PARA SORDOS, o en sus propias instalaciones y que emplea algunos de los recursos informáticos y de comunicaciones del INSTITUTO NACIONAL PARA SORDOS.

Usuario: funcionarios, contratistas o terceros que hacen uso de los servicios informáticos del Instituto Nacional para Sordos-INSOR.

METODOLOGIA DE IMPLEMENTACIÓN

La metodología de implementación del Plan de Seguridad y Privacidad para el Instituto Nacional para Sordos-INSOR, se basa en el ciclo PHVA (Planificar-

Hacer-Verificar-Actuar) y lo establecido en el Modelo de Seguridad y Privacidad del Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC de acuerdo a la Norma Técnica Colombiana ISO27001:2013 y lo establecido en el Decreto 1008 de 14 de junio 2018:



Ciclo de operación del Modelo de Seguridad y Privacidad de la Información

A la fecha se realizaron las actividades de planificación que incluyen el contexto de la entidad, planeación, soporte, estado actual de la información.

En las actividades de implementación se incluyen la elaboración de procedimientos, guías y manuales, control y planeación operacional, plan de sensibilización de seguridad de la información.

Pendiente por realizar: tratamiento de riesgos dentro de la fase de implementación, la fase de evaluación de desempeño y mejora continua.

CUMPLIMIENTO DE LA IMPLEMENTACIÓN

El Instituto Nacional para Sordos-INSOR en su modelo de seguridad y privacidad de la información se encuentra en la fase de implementación.

NIVEL DE MADUREZ DE SGSI

Según el modelo de privacidad y seguridad de la información establecido por el Ministerio de Tecnologías de Información el INSOR se encuentra en el nivel 3 de implementación donde se deben ejecutar las acciones trazadas en la

etapa previa de planeación de manera que la entidad diseñe un modelo de privacidad que le permita cumplir con los mínimos legales y generar una política privacidad que le permita la correcta gestión de la información.

PLAN DE ACTIVIDADES DEL SGSI

N	Actividad	Fecha Inicio	Fecha Final	Responsable	Producto
1. ACTIVOS DE INFORMACIÓN					
1.1	Actualización activos de información	Mayo	Noviembre	Todos los procesos	Matriz de activos
1.2	Publicación activos de información	Diciembre	Diciembre	Oficina Asesora de Planeación y Sistemas	Matriz de activos
2. RIESGOS DE SEGURIDAD DE LA INFORMACIÓN					
2.1	Actualización metodología riesgos seguridad	Febrero	Marzo	Oficina Asesora de Planeación y Sistemas	Matriz de riesgos
2.2	Identificación de análisis de riesgos de seguridad de la información	Febrero	Diciembre	Todas las áreas y procesos del INSOR	Matriz de riesgos
2.3	Comunicación de riesgos de seguridad de la información	Abril	Diciembre	Oficina Asesora de Planeación y Sistemas	Actas, correos electrónicos
2.4	Tratamiento de riesgos de seguridad de la información	Febrero	Diciembre	Todas las áreas y procesos del INSOR	Actas, correos electrónicos
2.5	Seguimiento y revisión de riesgos de seguridad	Junio	Diciembre	Oficina Asesora de Planeación y Sistemas	Informe
3. PLAN DE SENSIBILIZACIÓN SEGURIDAD DE LA INFORMACIÓN					

3.1	Actualización plan de sensibilización	Febrero	Diciembre	Oficina Asesora de Planeación y Sistemas	Matriz de sensibilización de seguridad de la información
3.2	Ejecución del plan de sensibilización	Febrero	Diciembre	Oficina Asesora de Planeación y Sistemas	Informe de ejecución
3.3	Ejecución indicadores de sensibilización	Marzo	Diciembre	Oficina Asesora de Planeación y Sistemas	Hoja de vida de indicadores
4. DOMINIOS DE LA NORMA ISO 270001:2013					
4.1	Revisión manual y política de seguridad de la información	Febrero	Abril	Oficina Asesora de Planeación y Sistemas	Documento y manual
4.2	Revisión de controles de la norma ISO 270001:2013	Mayo	Diciembre	Oficina Asesora de Planeación y Sistemas	Declaración de aplicabilidad
5. INDICADORES DE GESTIÓN SGSI					
5.1	Reporte indicadores de SGSI	Marzo	Diciembre	Oficina Asesora de Planeación y Sistemas	Hoja de vida de indicadores

PROCESO GESTIÓN TIC -INSOR

Elaboro: Oficina Asesora de Planeación y Sistemas
Revisó: Comité de Gestión y Desempeño
Aprobó: 31 – enero 2019