Encuesta de Percepción y Satisfacción Sistema de Gestión de Seguridad y Privacidad 2025.

El objetivo de este formulario es medir la percepción y satisfacción de los colaboradores del SENA frente a los temas de seguridad y privacidad de la información durante la presente vigencia, evaluando su comprensión general y el nivel de apropiación de las prácticas institucionales. Los resultados servirán como insumo para planear las actividades de concientización de la siguiente vigencia y fortalecer la cultura de seguridad y privacidad de la información en la Entidad.

Datos de Registro

1. Nombres y Apellidos (Completos) *

   Alcira Lucia Garcia Gonzalez

2. Ingrese su correo Institucional *

   algarcia@sena.edu.co

3. Tipo de vinculación *

   - (●) Contratista
   - ( ) Planta - Carrera administrativa
   - ( ) Planta - Provisional
   - ( ) Planta - Libre nombramiento y remoción
   - ( ) Pasante

- Aprendiz
- Otro

Registre su Dependencia.

4. **Dirección General / Regional** *

- Amazonas
- Antioquia
- Arauca
- Atlántico
- Bolívar
- Boyacá
- Caldas
- Caquetá
- Cauca
- Cesar
- Córdoba
- Cundinamarca
- Chocó
- Dirección General

- Distrito Capital
- Huila
- Guajira
- Magdalena
- Meta
- Nariño
- Norte de Santander
- Quindío
- Risaralda
- Santander
- Sucre
- Tolima
- Valle del Cauca
- Casanare
- Putumayo
- San Andrés
- Guainía
- Guaviare
- Vaupés
- Vichada

5. **Boyacá** *

- ( ) Centro de la Innovación Agroindustrial y de Servicios
- ( ) Centro Industrial de Mantenimiento y Manufactura
- ( ) Centro Minero
- (•) Centro de Gestión Administrativa y Fortalecimiento Empresarial
- ( ) Centro de Desarrollo Agropecuario y Agroindustrial
- ( ) Despacho Regional Boyacá

Participación

6. ¿Con qué frecuencia lee los boletines "Martes de Seguridad"? *

- ( ) Siempre
- ( ) Casi Siempre
- (•) A veces
- ( ) Nunca

7. ¿Cuál es el lema central de la campaña de Seguridad y Privacidad de la Información? *

- (•) Cuidar la información es asegurar el cumplimiento de nuestra misión.

- La protección de los datos impulsa y respalda nuestra labor institucional.
- Protegiendo la información, fortalecemos nuestra misión
- Cuando preservamos la información, fortalecemos los objetivos del SENA

8. ¿Conoce o ha consultado el Manual de Políticas de Seguridad y Privacidad de la Información (GOR-M-002) *

- (●) SI
- ( ) No

9. Describa las actividades desarrolladas por el/la dinamizador(a) SIGA o TIC relacionadas con la socialización de los controles de la norma ISO 27001:2022 en su dependencia durante la presente vigencia. *

Durante la vigencia, el/la dinamizador(a) SIGA/TIC realizó charlas informativas, envió material digital y socializó los controles de la ISO 27001:2022, enfocándose en buenas prácticas de seguridad, manejo adecuado de la información y prevención de incidentes. También brindó acompañamiento y

Seguridad Comportamental y Controles Físicos (Énfasis en Prevención de Errores Humanos)

El 60% de los ciberataques se originan por errores humanos evitables. Esta sección evalúa la adopción de las prácticas "no negociables"

10. ¿Utiliza contraseñas únicas para cada sistema (correo, Sofia Plus, CompromISO, plataformas personales)? *

- (●) Si

- ○ No

11. ¿Almacena sus contraseñas en notas adhesivas, agendas o cuadernos, conversaciones de WhatssApp navegadores o archivos sin cifrar? *

- ◉ Si
- ○ No

12. Al ausentarse de su escritorio (incluso por 5 minutos), ¿bloquea su equipo (Windows + L)? *

- ◉ Si
- ○ No

13. ¿Porta su carné institucional siempre visible mientras está en las instalaciones del SENA? *

- ◉ Si
- ○ No

14. Si observa a un visitante sin carné en un área segura (ej. sala de servidores), ¿Cuál es su acción inmediata? *

Reportar de inmediato al personal de seguridad o responsable del área y solicitar al visitante que se identifique y cumpla el protocolo de ingreso.

Manejo de Información y Canales Autorizados (Los Riesgos de Fuga)

Se centra en la gestión de información confidencial y el uso de plataformas no institucionales.

15. ¿Cuál es mi canal preferido para Compartir Información de Gran Tamaño? *

- [ ] CompromISO
- [x] OneDrive institucional
- [ ] WeTransfer
- [ ] Correo institucional

16. Un documento con información disciplinaria Etapa de instrucción, ¿bajo qué clasificación debe etiquetarse? *

- ( ) Pública
- ( ) Pública Clasificada
- (•) Pública Reservada

17. ¿Por qué razón la Entidad debería establecer el bloqueo o restricción de puertos USB? *

- (•) Para evitar la copia no autorizada de información y reducir riesgos de malware.
- ( ) Para impedir que los equipos se apaguen accidentalmente.
- ( ) Para mejorar la velocidad del internet institucional.
- ( ) Para que los funcionarios usen únicamente dispositivos personales.

Conciencia de Amenazas Emergentes y Reporte de Incidentes

Evalúa la preparación ante los riesgos más sofisticados y la efectividad del procedimiento de reporte.

18. Recibe un correo urgente que pide su clave y tiene un logo ligeramente pixelado. ¿Qué debe hacer antes de hacer clic? *

- ○ Hacer clic rápidamente para evitar perder acceso a la cuenta.
- ○ Ignorar el mensaje y eliminarlo sin informar a nadie.
- ◉ Verificar el remitente, no abrir enlaces y reportar a la mesa de servicio el correo sospechoso.
- ○ Responder el correo para confirmar si es auténtico.

19. Si sospecha que su equipo tiene un virus (está lento o con comportamiento extraño), ¿Cuál es el primer paso? *

- ◉ Desconectarlo de la red y reportar inmediatamente al equipo de mesa de servicio.
- ○ Descargar el primer antivirus que encuentre en internet.
- ○ Reiniciar varias veces hasta que funcione normalmente.
- ○ Ignorar el problema y continuar trabajando para no interrumpir las actividades.

Alineación Estratégica y Cumplimiento

Verifica la comprensión del marco estratégico.

20. El Modelo de Seguridad y Privacidad de la Información (MSPI) solo solo se implementa en la Dirección General, en Regionales y Centros no aplica.

- [x] Falso
- [ ] Verdadero

21. ¿Cuál de los componentes del Modelo de Seguridad y Privacidad de la Información considera que debe fortalecerse más en su dependencia?

- [x] Controles de Personas
- [ ] Controles Organizacionales
- [ ] Controles Tecnológicos

Preguntas Finales.

22. El Sistema de Gestión de Seguridad y Privacidad de la Información contempla:

- [ ] Gestión de Riesgos
- [ ] Gestión de Incidentes
- [ ] Gestión de Activos
- [ ] Gestión de Servicios Tecnológicos
- [x] Todas las Anteriores

23. ¿Cuál cree que es su nivel de conocimiento en temas de seguridad y privacidad de la información? *

- [ ] Bajo

- (●) Medio
- ( ) Alto

24. ¿Sabe como reportar un incidente de Seguridad de la Información? *

- (●) Si
- ( ) No

Microsoft 365

Este contenido lo creó el propietario del formulario. Los datos que envíes se enviarán al propietario del formulario. Microsoft no es responsable de las prácticas de privacidad o seguridad de sus clientes, incluidas las que adopte el propietario de este formulario. Nunca des tu contraseña.

Microsoft Forms | Encuestas, cuestionarios y sondeos con tecnología de inteligencia artificial Crear mi propio formulario

Privacidad y cookies | Términos de uso