# SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

## CONTROLES ORIENTADOS A LAS PERSONAS (A.6.1 - A.6.8)

**Proyecto:** SchoolMe  
**Ubicación:** Neiva, Huila, Colombia  
**Versión:** 1.0  
**Fecha de vigencia:** Enero 2025

## TABLA DE CONTENIDO

1. Política de Cribado (A.6.1)
2. Política de Términos y Condiciones de Empleo (A.6.2)
3. Política de Concientización y Capacitación (A.6.3)
4. Política de Proceso Disciplinario (A.6.4)
5. Política de Terminación o Cambio de Empleo (A.6.5)
6. Política de Acuerdos de Confidencialidad (A.6.6)
7. Política de Trabajo Remoto (A.6.7-A.6.8)

# 1. POLÍTICA DE CRIBADO (A.6.1)

## 1.1 OBJETIVO

Verificar antecedentes, identidad y calificaciones de todo personal antes de su incorporación al proyecto SchoolMe para reducir riesgos de seguridad de la información.

## 1.2 ALCANCE

Esta política aplica para:

* Aprendices SENA (desarrolladores)
* Personal administrativo del colegio
* Docentes con acceso a sistemas
* Acudientes con acceso a la plataforma

## 1.3 RESPONSABILIDADES

* **Aprendices SENA de RRHH:** Ejecución del proceso de cribado y archivo de documentación
* **Líder de desarrollo:** Validación de competencias técnicas de candidatos
* **Coordinador del proyecto:** Aprobación final de incorporación

## 1.4 PROCESO DE CRIBADO

### Paso 1: Solicitud de documentación

El candidato debe completar y entregar:

* Formulario de datos personales de SchoolMe
* Copia de cédula de ciudadanía legible
* Certificados académicos (diplomas, actas de grado)
* Mínimo 2 referencias laborales o académicas (nombre, cargo, teléfono)

### Paso 2: Verificación de identidad

* Validar que la cédula corresponda al candidato (foto y datos)
* Registrar número de documento en expediente digital
* Verificar vigencia del documento

### Paso 3: Validación de referencias

* Contactar vía telefónica o correo a las referencias proporcionadas
* Consultar sobre desempeño, responsabilidad y ética profesional
* Documentar resultados en formato de verificación

### Paso 4: Validación de competencias técnicas (solo desarrolladores)

* Líder de desarrollo realiza entrevista técnica
* Evalúa conocimientos en las tecnologías del proyecto
* Documenta resultado en formato de evaluación técnica

### Paso 5: Archivo y aprobación

* Todos los documentos se digitalizan y archivan en carpeta segura de SchoolMe
* RRHH emite concepto favorable o desfavorable
* Coordinador aprueba incorporación

## 1.5 CRITERIOS DE RECHAZO

Se rechaza la incorporación si:

* Referencias negativas sobre conducta o desempeño
* Inconsistencias graves en información proporcionada
* No cumple con competencias técnicas mínimas requeridas
* Antecedentes que representen riesgo para la seguridad de datos

## 1.6 ALMACENAMIENTO

Todos los documentos del proceso de cribado se almacenan en:

* Carpeta digital segura con acceso restringido
* Respaldo en repositorio cifrado
* Conservación mínima: duración del contrato + 1 año

## 1.7 VIGENCIA

Esta política entra en vigencia desde su publicación y debe revisarse anualmente.

# 2. POLÍTICA DE TÉRMINOS Y CONDICIONES DE EMPLEO (A.6.2)

## 2.1 OBJETIVO

Establecer las responsabilidades del personal respecto a la seguridad de la información desde el momento de su vinculación al proyecto SchoolMe.

## 2.2 ALCANCE

Aplica para todo personal que tenga acceso a:

* Sistemas y plataforma SchoolMe
* Datos de estudiantes y acudientes
* Código fuente y documentación técnica
* Infraestructura tecnológica del proyecto

## 2.3 CONTRATO DE APRENDIZAJE SENA

Para aprendices SENA se utilizará:

* Plantilla oficial del contrato de aprendizaje SENA
* Anexo de Seguridad de la Información SchoolMe (documento adjunto)

## 2.4 CLÁUSULAS OBLIGATORIAS DE SEGURIDAD

Todo contrato o acuerdo de vinculación debe incluir:

### Cláusula 1: Cumplimiento de políticas

"El colaborador se compromete a cumplir estrictamente la Política de Seguridad de la Información de SchoolMe y todas sus actualizaciones durante la vigencia de su vinculación."

### Cláusula 2: Protección de la información

"El colaborador es responsable de proteger la confidencialidad, integridad y disponibilidad de toda información a la que tenga acceso en el marco de sus funciones, incluyendo datos personales de estudiantes, acudientes, código fuente y documentación técnica."

### Cláusula 3: Uso aceptable de recursos

"El colaborador utilizará los recursos tecnológicos (equipos, sistemas, redes) exclusivamente para fines relacionados con sus funciones en SchoolMe, evitando usos personales o no autorizados."

### Cláusula 4: Reporte de incidentes

"El colaborador debe reportar inmediatamente cualquier incidente de seguridad, vulnerabilidad o sospecha de compromiso de información al Líder de Seguridad o Coordinador del proyecto."

### Cláusula 5: Sanciones

"El incumplimiento de las políticas de seguridad puede derivar en sanciones que van desde amonestación verbal hasta terminación del contrato de aprendizaje o vinculación, según la gravedad de la falta."

### Cláusula 6: Revisión periódica

"El colaborador acepta que estas cláusulas pueden ser actualizadas y revisadas periódicamente, comprometiéndose a conocer y cumplir las nuevas versiones notificadas."

## 2.5 PROCESO DE FIRMA

1. RRHH prepara contrato con anexo de seguridad
2. Candidato lee y firma documento
3. Copia se entrega al colaborador
4. Original se archiva en expediente
5. Registro se ingresa en control de contratos firmados

## 2.6 VIGENCIA

Las cláusulas de seguridad permanecen vigentes durante toda la relación laboral o contractual y se extienden según acuerdos de confidencialidad post-vinculación.

# 3. POLÍTICA DE CONCIENTIZACIÓN Y CAPACITACIÓN (A.6.3)

## 3.1 OBJETIVO

Asegurar que todo el personal y partes interesadas conozcan y cumplan sus responsabilidades de seguridad de la información mediante programas de entrenamiento continuo.

## 3.2 ALCANCE

Aplica para:

* Todos los aprendices SENA
* Personal administrativo con acceso a sistemas
* Docentes usuarios de la plataforma
* Nuevos ingresos al proyecto

## 3.3 ESTRUCTURA DEL PROGRAMA

### 3.3.1 Inducción Inicial de Seguridad (Obligatoria)

* **Duración:** 2 horas
* **Momento:** Primera semana de vinculación
* **Responsable:** Líder de desarrollo o desarrollador senior
* **Contenido:**
  + Introducción a ISO 27001 y su importancia
  + Políticas de seguridad de SchoolMe
  + Amenazas comunes (phishing, malware, ingeniería social)
  + Gestión segura de contraseñas
  + Uso correcto de VPN Hostinger
  + Protección de dispositivos y datos
  + Clasificación de información
  + Reporte de incidentes

### 3.3.2 Talleres Trimestrales de Buenas Prácticas

* **Frecuencia:** Cada 3 meses (4 veces al año)
* **Duración:** 1 hora
* **Responsable:** Desarrollador senior asignado
* **Contenido rotativo:**
  + Trimestre 1: Seguridad en desarrollo de código
  + Trimestre 2: Protección de datos personales y GDPR
  + Trimestre 3: Seguridad en trabajo remoto
  + Trimestre 4: Respuesta a incidentes y backup

### 3.3.3 Evaluación Anual de Conocimientos

* **Frecuencia:** Una vez al año (diciembre)
* **Formato:** Cuestionario online de 20 preguntas
* **Aprobación:** Mínimo 80% de respuestas correctas
* **Seguimiento:** Plan de refuerzo para quienes no aprueben

## 3.4 MATERIAL DE CAPACITACIÓN

Se utilizarán los siguientes recursos:

* Presentaciones PowerPoint
* Videos educativos (máximo 10 minutos)
* Guías rápidas en PDF
* Casos prácticos y simulaciones
* Repositorio digital de materiales

## 3.5 REGISTRO Y SEGUIMIENTO

Para cada capacitación se debe documentar:

* Lista de asistencia con firma digital
* Fecha, hora y duración
* Tema tratado e instructor
* Material entregado
* Resultados de evaluaciones
* Observaciones y mejoras sugeridas

## 3.6 INDICADORES DE EFECTIVIDAD

* Porcentaje de personal capacitado: Meta 100%
* Porcentaje de aprobación en evaluaciones: Meta >80%
* Reducción de incidentes de seguridad: Monitoreo trimestral

## 3.7 RESPONSABILIDADES

* **Líder de desarrollo:** Planificar y coordinar capacitaciones
* **Desarrollador senior:** Impartir talleres
* **RRHH:** Convocar, registrar asistencia y archivar evidencias
* **Todo el personal:** Asistir y aprobar capacitaciones

# 4. POLÍTICA DE PROCESO DISCIPLINARIO (A.6.4)

## 4.1 OBJETIVO

Definir un proceso formal para abordar vulneraciones a la política de seguridad, considerando la intencionalidad del incumplimiento y aplicando sanciones proporcionales.

## 4.2 ALCANCE

Aplica a todo colaborador de SchoolMe que incumpla políticas, procedimientos o cláusulas contractuales relacionadas con seguridad de la información.

## 4.3 DEFINICIÓN DE FALTAS

### 4.3.1 Faltas Leves

* Olvido ocasional de cerrar sesión en equipo compartido
* No reportar oportunamente un incidente menor
* Uso menor no autorizado de recursos (ejemplo: navegación personal esporádica)
* Primera vez que no cumple con capacitación obligatoria

**Sanción:** Amonestación verbal documentada

### 4.3.2 Faltas Moderadas

* Compartir credenciales con terceros
* Conectarse desde redes públicas sin VPN
* Almacenar información confidencial en dispositivos personales no autorizados
* Reincidencia en faltas leves
* No reportar pérdida de dispositivo corporativo

**Sanción:** Amonestación escrita en expediente + capacitación adicional

### 4.3.3 Faltas Graves

* Divulgación no autorizada de datos de estudiantes o código fuente
* Acceso no autorizado a sistemas o ambientes de producción
* Desactivar controles de seguridad (antivirus, firewall, VPN)
* Instalación de software malicioso o no autorizado
* Modificación no autorizada de código en producción

**Sanción:** Suspensión temporal de acceso a sistemas (3-7 días) + amonestación escrita grave

### 4.3.4 Faltas Gravísimas

* Robo o venta de información confidencial
* Sabotaje a sistemas o infraestructura
* Uso malicioso de accesos para beneficio propio o terceros
* Eliminación intencional de datos críticos
* Falsificación de documentos o evidencias

**Sanción:** Terminación inmediata de contrato de aprendizaje + acciones legales si corresponde

## 4.4 FLUJO DEL PROCESO DISCIPLINARIO

### Paso 1: Detección y reporte

* Cualquier persona detecta o sospecha una falta
* Se reporta al Líder de Seguridad o Coordinador
* Se documenta en Formato de Reporte de Incidente

### Paso 2: Investigación preliminar

* Líder de Seguridad revisa evidencias
* Se determina si procede investigación formal
* Plazo máximo: 48 horas

### Paso 3: Notificación al implicado

* Se notifica formalmente al colaborador
* Se le informa de los hechos que se investigan
* Se programa entrevista (derecho a ser escuchado)

### Paso 4: Entrevista y recolección de pruebas

* Entrevista con el implicado (se levanta acta)
* Se recopilan testimonios si hay testigos
* Se revisan logs, registros, evidencias técnicas

### Paso 5: Análisis y determinación

* Se clasifica la falta según gravedad
* Se considera intencionalidad y antecedentes
* Se determina sanción aplicable

### Paso 6: Aplicación de sanción

* Se notifica por escrito la sanción al colaborador
* Se ejecuta la sanción (amonestación, suspensión, terminación)
* Se documenta en expediente

### Paso 7: Seguimiento

* Se hace seguimiento post-sanción
* Se verifica que no haya reincidencia
* Se cierra el caso

## 4.5 DOCUMENTACIÓN REQUERIDA

* Reporte de Incidente de Seguridad
* Acta de Entrevista con el Implicado
* Evidencias técnicas (logs, capturas, correos)
* Carta de Amonestación (si aplica)
* Acta de Suspensión o Terminación (si aplica)

## 4.6 DERECHOS DEL COLABORADOR

* Ser notificado de los hechos que se investigan
* Ser escuchado y presentar su versión
* Aportar pruebas a su favor
* Conocer la sanción aplicada y sus fundamentos
* Apelar decisiones graves ante el Coordinador del proyecto

## 4.7 PLAZOS

* Investigación preliminar: 48 horas
* Investigación formal: 5 días hábiles máximo
* Apelación: 3 días hábiles desde notificación

## 4.8 CONFIDENCIALIDAD

Todo proceso disciplinario se maneja con confidencialidad, limitando el conocimiento solo a las personas directamente involucradas en la investigación.

# 5. POLÍTICA DE TERMINACIÓN O CAMBIO DE EMPLEO (A.6.5)

## 5.1 OBJETIVO

Proteger los intereses de SchoolMe en la terminación o cambio de empleo, asegurando la devolución de bienes y la continuidad de responsabilidades de confidencialidad.

## 5.2 ALCANCE

Aplica a:

* Terminación de contrato de aprendizaje SENA
* Finalización de vinculación de personal administrativo o docente
* Cambio de rol con diferente nivel de acceso
* Suspensión temporal de actividades

## 5.3 NOTIFICACIÓN

### 5.3.1 Por parte del colaborador

Debe notificar con mínimo 15 días de anticipación a RRHH y su supervisor directo.

### 5.3.2 Por parte de SchoolMe

Se notifica formalmente por escrito según lo establecido en contrato.

## 5.4 PROCESO DE OFFBOARDING (SALIDA)

### Paso 1: Notificación formal (Día 0)

* RRHH recibe notificación de terminación
* Se crea expediente de salida
* Se programa fecha de último día laboral

### Paso 2: Comunicación a TI (Máximo 24h)

* RRHH notifica a aprendices de TI
* Se programa desactivación de accesos
* Se genera checklist personalizado

### Paso 3: Devolución de activos (Último día laboral)

El colaborador debe devolver:

* Laptop o equipo de cómputo asignado
* Celular corporativo (si aplica)
* Llaves físicas de oficinas
* Tarjetas de acceso o identificación
* Dispositivos USB, discos externos
* Documentación física confidencial
* Cualquier otro bien propiedad de SchoolMe

Se llena Formato de Acta de Entrega con firma del colaborador y recibidor.

### Paso 4: Desactivación de accesos (Máximo 24h desde notificación)

TI debe desactivar:

* Cuenta de correo corporativo (@schoolme.com)
* Acceso a VPN Hostinger
* Usuarios en plataforma SchoolMe (admin, docente, etc.)
* Acceso a repositorios de código (GitHub, GitLab)
* Cuentas en herramientas colaborativas (Slack, Trello, etc.)
* Acceso físico a instalaciones (desactivar tarjeta)

TI confirma desactivación por correo a RRHH.

### Paso 5: Transferencia de conocimiento (Últimos 5 días)

* Documentar tareas pendientes
* Transferir responsabilidades a otro colaborador
* Entregar contraseñas de herramientas bajo su custodia (en sobre sellado a RRHH)

### Paso 6: Entrevista de salida (Último día)

* RRHH realiza entrevista de salida
* Se registra retroalimentación
* Se recuerdan obligaciones post-empleo

### Paso 7: Recordatorio de confidencialidad

* Se entrega Carta de Recordatorio de Obligaciones de Confidencialidad
* Recuerda vigencia del NDA (2 años post-vinculación)
* Colaborador firma acuse de recibo

### Paso 8: Cierre de expediente (Día siguiente)

* RRHH verifica completitud del checklist
* Se archivan todos los documentos
* Se emite constancia de terminación

## 5.5 CHECKLIST DE SALIDA

Se utiliza el Formato de Checklist de Offboarding que incluye:

* ☐ Notificación recibida y procesada
* ☐ TI notificado (fecha y hora)
* ☐ Laptop devuelta (estado: \_\_\_\_\_)
* ☐ Celular devuelto (N/A si no aplica)
* ☐ Llaves devueltas
* ☐ Tarjeta de acceso devuelta
* ☐ Correo desactivado (fecha: \_\_\_\_\_)
* ☐ VPN desactivada (fecha: \_\_\_\_\_)
* ☐ Accesos a plataforma revocados (fecha: \_\_\_\_\_)
* ☐ Transferencia de conocimiento completada
* ☐ Entrevista de salida realizada
* ☐ Carta de confidencialidad entregada y firmada
* ☐ Acta de entrega firmada
* ☐ Expediente cerrado

## 5.6 PLAZOS CRÍTICOS

* **Desactivación de accesos:** Máximo 24 horas desde notificación a TI
* **Devolución de activos:** Último día laboral
* **Cierre de expediente:** Máximo 48 horas después del último día

## 5.7 RESPONSABILIDADES

* **RRHH:** Coordinar proceso, verificar checklist, archivar documentos
* **TI:** Desactivar accesos, verificar devolución de equipos, confirmar por correo
* **Supervisor directo:** Facilitar transferencia de conocimiento
* **Colaborador saliente:** Cumplir con devolución y transferencias

## 5.8 CASOS ESPECIALES

### Terminación por falta grave

* Desactivación inmediata de accesos (0 horas)
* Devolución supervisada de activos
* Sin entrevista de salida

### Suspensión temporal

* Desactivación temporal de accesos
* Activos quedan en custodia de RRHH
* Reactivación condicionada al regreso

# 6. POLÍTICA DE ACUERDOS DE CONFIDENCIALIDAD (A.6.6)

## 6.1 OBJETIVO

Mantener la confidencialidad de la información accesible por el personal o partes externas mediante acuerdos contractuales que establezcan obligaciones claras.

## 6.2 ALCANCE

Deben firmar Acuerdo de Confidencialidad (NDA):

* Todos los aprendices SENA
* Personal administrativo del colegio
* Docentes con acceso a plataforma
* Contratistas externos o proveedores
* Visitantes que accedan a información sensible

## 6.3 CLASIFICACIÓN DE INFORMACIÓN

### 6.3.1 Información Pública

Puede divulgarse sin restricciones:

* Material promocional de SchoolMe
* Información publicada en redes sociales oficiales
* Comunicados de prensa

### 6.3.2 Información Interna

Uso interno del proyecto, no se divulga externamente:

* Procedimientos operativos
* Manuales de usuario internos
* Estructura organizacional

### 6.3.3 Información Confidencial

**Requiere protección especial y está cubierta por NDA:**

* **Datos personales:** Nombres, documentos, contactos de estudiantes y acudientes
* **Datos académicos:** Calificaciones, reportes de comportamiento, asistencia
* **Código fuente:** Todo el código de la plataforma SchoolMe
* **Documentación técnica:** Arquitectura, diagramas, documentación de APIs
* **Credenciales:** Usuarios, contraseñas, tokens, certificados
* **Estrategias de negocio:** Planes de desarrollo, roadmap, alianzas
* **Información financiera:** Presupuestos, costos, contratos comerciales

## 6.4 CONTENIDO DEL ACUERDO DE CONFIDENCIALIDAD

### Cláusula 1: Definición de Información Confidencial

Se considera información confidencial todo dato relacionado con SchoolMe que no sea de dominio público, incluyendo pero no limitándose a: datos de estudiantes y acudientes, código fuente, documentación técnica, credenciales de acceso, estrategias de negocio y cualquier información marcada como "Confidencial".

### Cláusula 2: Obligaciones del Firmante

El firmante se compromete a:

* No revelar información confidencial a terceros sin autorización escrita
* No usar información confidencial para fines distintos a sus funciones en SchoolMe
* Proteger la información con el mismo cuidado que protegería su propia información confidencial
* Limitar el acceso a información confidencial solo a personas autorizadas que necesiten conocerla
* Devolver o destruir toda información confidencial al terminar la relación con SchoolMe

### Cláusula 3: Excepciones

No se considera violación de confidencialidad cuando:

* La información es o se vuelve de dominio público sin culpa del firmante
* La información ya era conocida por el firmante antes de la divulgación
* La divulgación es requerida por mandato legal o judicial (previa notificación a SchoolMe)

### Cláusula 4: Vigencia

Este acuerdo permanece vigente durante toda la relación con SchoolMe y por un período adicional de **2 años** después de su terminación.

### Cláusula 5: Consecuencias del Incumplimiento

El incumplimiento de este acuerdo puede resultar en:

* Terminación inmediata de la relación contractual
* Acciones legales civiles y penales
* Reclamación de daños y perjuicios
* Cualquier otra medida permitida por la ley

### Cláusula 6: Jurisdicción

Este acuerdo se rige por las leyes de la República de Colombia y cualquier disputa será resuelta en los tribunales de Neiva, Huila.

## 6.5 PROCESO DE FIRMA

### Para aprendices SENA y personal nuevo:

1. RRHH entrega NDA junto con contrato en proceso de vinculación
2. Se explican las cláusulas y se resuelven dudas
3. Firmante lee, firma y fecha el documento
4. Se escanea y archiva en expediente digital
5. Copia se entrega al firmante
6. Se registra en control de NDAs

### Para contratistas externos:

1. Coordinador solicita a RRHH preparar NDA específico
2. Se envía por correo para revisión
3. Firma digital o física antes de iniciar trabajos
4. Se archiva en carpeta de contratistas

### Para visitantes:

1. Si van a acceder a información sensible, firman NDA simplificado
2. Se archiva en carpeta de visitantes con fecha y motivo

## 6.6 RECORDATORIOS PERIÓDICOS

* Al inicio de cada año se envía correo recordatorio de vigencia del NDA
* En capacitaciones trimestrales se refuerza importancia de confidencialidad
* Al terminar vinculación se entrega carta recordatoria

## 6.7 ALMACENAMIENTO

* NDAs firmados se archivan en expediente de cada persona
* Respaldo digital en carpeta segura cifrada
* Acceso restringido solo a RRHH y Coordinador
* Conservación: 5 años después de terminación de relación

## 6.8 RESPONSABILIDADES

* **RRHH:** Preparar, gestionar firma, archivar y controlar NDAs
* **Coordinador:** Aprobar NDAs para casos especiales
* **Todo el personal:** Cumplir estrictamente con lo firmado

# 7. POLÍTICA DE TRABAJO REMOTO (A.6.7 - A.6.8)

## 7.1 OBJETIVO

Garantizar la seguridad de la información cuando el personal está trabajando de forma remota, protegiendo los datos incluso fuera de las instalaciones físicas de SchoolMe.

## 7.2 ALCANCE

Aplica a:

* Aprendices SENA en modalidad de trabajo remoto
* Personal que ocasionalmente trabaje desde casa
* Colaboradores que accedan a sistemas desde ubicaciones externas

## 7.3 REQUISITOS OBLIGATORIOS DE SEGURIDAD

### 7.3.1 Conectividad

* **Uso obligatorio de VPN Hostinger** para cualquier acceso a sistemas SchoolMe
* **Autenticación de dos factores (2FA)** habilitada en VPN y cuentas críticas
* **Prohibido** acceder a sistemas desde redes públicas sin VPN (cafés, centros comerciales, aeropuertos)

### 7.3.2 Dispositivos

* **Equipo corporativo preferido:** Laptop asignada por SchoolMe con configuraciones de seguridad
* **Cifrado de disco obligatorio:** BitLocker (Windows) o FileVault (Mac) activado
* **Antivirus actualizado:** Verificación semanal de actualizaciones
* **Firewall activo:** No desactivar el firewall del sistema operativo
* **Sistema operativo actualizado:** Instalar parches de seguridad en máximo 7 días

### 7.3.3 Redes Wi-Fi

* **Red doméstica segura:** Cambiar contraseña predeterminada del router
* **Cifrado WPA2 o WPA3:** Nunca usar redes abiertas sin cifrado
* **SSID no predeterminado:** Cambiar nombre de red del fabricante
* **Ocultar SSID:** Recomendado para mayor seguridad

### 7.3.4 Espacio físico de trabajo

* **Espacio privado:** Evitar trabajar en espacios donde terceros puedan ver la pantalla
* **Bloqueo de pantalla:** Activar bloqueo automático después de 5 minutos de inactividad
* **Privacidad visual:** No trabajar con datos confidenciales en lugares públicos
* **Respaldo físico:** No dejar equipos ni documentos a la vista en ausencias

## 7.4 ACCESO A SISTEMAS

### 7.4.1 Credenciales

* **Contraseñas robustas:** Mínimo 12 caracteres, combinando mayúsculas, minúsculas, números y símbolos
* **No compartir credenciales:** Cada usuario debe usar sus propias cuentas
* **Cambio periódico:** Cada 90 días
* **Gestor de contraseñas recomendado:** Uso de herramientas como Bitwarden, 1Password

### 7.4.2 Sesiones

* **Cerrar sesión:** Al finalizar jornada laboral
* **No guardar contraseñas en navegador:** En equipos compartidos
* **Notificación de actividad sospechosa:** Reportar inmediatamente intentos de acceso no autorizados

## 7.5 ALMACENAMIENTO Y RESPALDO

### 7.5.1 Almacenamiento local

* **Evitar almacenamiento local de datos confidenciales:** Usar repositorios en la nube autorizados
* **Cifrado de archivos sensibles:** Si se almacenan localmente, deben cifrarse
* **No usar USB externos:** Salvo autorización expresa y con cifrado

### 7.5.2 Respaldo

* **Respaldo automático:** Configurar backup de código y documentos importantes
* **Repositorios autorizados:** GitHub, Google Drive corporativo, servidor SchoolMe
* **Verificación semanal:** Comprobar que respaldos se ejecuten correctamente

## 7.6 COMUNICACIONES

### 7.6.1 Videoconferencias

* **Herramientas autorizadas:** Google Meet, Zoom con cuenta corporativa, Microsoft Teams
* **Fondos virtuales:** Usar fondos difuminados para no exponer espacio personal
* **Micrófonos y cámaras:** Desactivar cuando no se usen
* **No grabar sin autorización:** Solicitar permiso antes de grabar reuniones

### 7.6.2 Mensajería

* **Canales autorizados:** Slack de SchoolMe, WhatsApp de grupos oficiales
* **No compartir información confidencial por SMS o apps personales**
* **Verificar destinatarios:** Antes de enviar información sensible

### 7.6.3 Correo electrónico

* **Solo usar correo corporativo** para comunicaciones de trabajo
* **Verificar destinatarios:** Especialmente al usar "Responder a todos"
* **Cifrado recomendado:** Para información confidencial
* **Precaución con archivos adjuntos:** Verificar antes de abrir

## 7.7 PROHIBICIONES

### 7.7.1 Estrictamente prohibido:

* Trabajar desde cibercafés o lugares de acceso público compartido
* Permitir que familiares o amigos usen equipos corporativos
* Instalar software no autorizado o pirata
* Conectarse a sistemas SchoolMe sin VPN activada
* Dejar equipos desatendidos y desbloqueados
* Compartir pantalla con personas no autorizadas
* Fotografiar o filmar información confidencial en pantalla
* Imprimir documentos confidenciales sin supervisión

### 7.7.2 Uso de dispositivos personales (BYOD)

* **No permitido por defecto** para acceso a sistemas críticos
* Si es necesario, requiere autorización expresa del Coordinador
* Debe cumplir los mismos requisitos de seguridad que equipos corporativos

## 7.8 INCIDENTES DE SEGURIDAD EN REMOTO

### Reportar inmediatamente si ocurre:

* Pérdida o robo de equipo corporativo
* Sospecha de compromiso de credenciales
* Acceso no autorizado a cuentas
* Infección por malware o virus
* Conexión accidental a red insegura con datos sensibles
* Exposición accidental de información confidencial

**Contacto de emergencia:**

* Líder de Seguridad: [correo/teléfono]
* Coordinador del proyecto: [correo/teléfono]

## 7.9 AUTORIZACIÓN DE TRABAJO REMOTO

### 7.9.1 Proceso de solicitud:

1. Colaborador solicita trabajo remoto a su supervisor
2. Supervisor evalúa y aprueba/rechaza
3. RRHH registra autorización
4. TI verifica configuración de seguridad en equipo
5. Se entrega Guía de Buenas Prácticas para Trabajo Remoto

### 7.9.2 Verificaciones periódicas:

* TI realiza auditoría trimestral de dispositivos remotos
* Verificación de actualizaciones de antivirus y SO
* Comprobación de uso correcto de VPN
* Reporte de auditoría a Coordinador

## 7.10 HORARIOS Y DISPONIBILIDAD

### 7.10.1 Jornada laboral

* Mantener los mismos horarios que en modalidad presencial
* Reportar inicio y fin de jornada en canal designado
* Estar disponible en horarios laborales para comunicaciones

### 7.10.2 Desconexión

* Derecho a desconexión fuera de horario laboral
* No obligación de responder correos/mensajes en horarios no laborales
* Respetar tiempos de descanso de compañeros

## 7.11 EQUIPO Y ERGONOMÍA

### 7.11.1 Recomendaciones

* Silla ergonómica o con soporte lumbar
* Mesa a altura adecuada
* Pantalla a nivel de ojos
* Iluminación apropiada
* Pausas activas cada 2 horas

## 7.12 RESPONSABILIDADES

### Del colaborador en remoto:

* Cumplir todas las medidas de seguridad
* Mantener equipo actualizado y protegido
* Reportar incidentes inmediatamente
* Participar en auditorías de seguridad
* Custodiar equipo corporativo

### De TI:

* Configurar equipos con medidas de seguridad
* Proporcionar acceso VPN
* Realizar auditorías periódicas
* Soporte técnico remoto

### De RRHH:

* Gestionar autorizaciones
* Registrar personal en remoto
* Entregar guías y políticas

### Del Supervisor:

* Aprobar solicitudes
* Verificar cumplimiento
* Reportar incumplimientos

## 7.13 VIGENCIA Y REVISIÓN

Esta política entra en vigencia desde su publicación y se revisa cada 6 meses o cuando cambien las condiciones de trabajo remoto en SchoolMe.

# ANEXOS

## ANEXO A: FORMATOS Y PLANTILLAS

Los siguientes formatos deben ser utilizados para la implementación de estas políticas:

1. **Formato de Datos Personales del Candidato**
2. **Formato de Verificación de Referencias**
3. **Formato de Evaluación Técnica**
4. **Anexo de Seguridad para Contrato SENA**
5. **Lista de Asistencia a Capacitaciones**
6. **Cuestionario de Evaluación Anual**
7. **Formato de Reporte de Incidente de Seguridad**
8. **Acta de Entrevista Disciplinaria**
9. **Carta de Amonestación**
10. **Checklist de Offboarding**
11. **Acta de Entrega de Activos**
12. **Carta de Recordatorio de Confidencialidad Post-Empleo**
13. **Acuerdo de Confidencialidad (NDA) - Empleados**
14. **Acuerdo de Confidencialidad (NDA) - Contratistas**
15. **Formato de Autorización de Trabajo Remoto**
16. **Guía de Buenas Prácticas para Trabajo Remoto**

*Estos formatos se encuentran disponibles en documentos Excel separados.*

## ANEXO B: GLOSARIO

* **Cribado (Screening):** Proceso de verificación de antecedentes
* **NDA:** Non-Disclosure Agreement (Acuerdo de Confidencialidad)
* **Offboarding:** Proceso de desvinculación de personal
* **VPN:** Virtual Private Network (Red Privada Virtual)
* **2FA:** Two-Factor Authentication (Autenticación de Dos Factores)
* **BYOD:** Bring Your Own Device (Traiga Su Propio Dispositivo)
* **ISO 27001:** Norma internacional de sistemas de gestión de seguridad de la información

## ANEXO: CONTACTOS CLAVE

**Coordinador del Proyecto SchoolMe:**  
Jesus Fernando Carvajal  
Correo: [olpierjesusfernud@gmail.com](mailto:olpierjesusfernud@gmail.com)

Teléfono: 311 5906033

**Responsable RRHH (Aprendices SENA):**  
Santiago Chaparro Riaño  
Correo: alfasan1481@gmail.com  
Teléfono: 3186577820

**Responsable TI**   
Juan Felipe Guerrero  
Correo: jfguerrero0411@gmail.com  
Teléfono: 315 3686037

## CONTROL DE VERSIONES

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Versión | Fecha | Descripción de Cambios | Autor | Aprobado por |
| 1.0 | Enero 2025 | Versión inicial | Equipo SENA | [Coordinador] |
|  |  |  |  |  |

## APROBACIÓN

**Elaborado por:**  
Equipo de Aprendices SENA - SchoolMe  
Fecha: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Revisado por:**  
Jesus Fernando Carvajal  
Cargo: Líder de Desarrollo  
Fecha: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Firma: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Aprobado por:**  
Carlos Julio Cadena

Cargo: Coordinador del Proyecto SchoolMe  
Fecha: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Firma: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**NOTA:** Este documento es propiedad de SchoolMe y contiene información confidencial. Su distribución está restringida solo a personal autorizado del proyecto. Queda prohibida su reproducción total o parcial sin autorización expresa.

*Fin del documento. Para consultas o sugerencias sobre estas políticas, contactar a: [correo responsable de políticas]*