



BACHILLERATO  
TECNICO  
AUTODIRIGIDO

Sistema de Gestión de Calidad

Gestión de comunicación a la comunidad

Política de seguridad de la información





# **POLÍTICA**

# DE SEGURIDAD DE LA **INFORMACIÓN**



BACHILLERATO  
TECNICO  
AUTODIRIGIDO

|                                                                                   |                                                |                                                                                     |
|-----------------------------------------------------------------------------------|------------------------------------------------|-------------------------------------------------------------------------------------|
|  | <b>SISTEMA DE GESTION DE LA CALIDAD</b>        |  |
|                                                                                   | <b>GESTIÓN DE COMUNICACIÓN A LA COMUNIDAD</b>  |                                                                                     |
|                                                                                   | <b>POLITICA DE SEGURIDAD DE LA INFORMACIÓN</b> |                                                                                     |

## MARCO DE SEGURIDAD DE LA INFORMACIÓN

**1. Resumen de la política:** La información, en todas sus formas de compartirse, comunicarse o almacenarse, debe ser siempre protegida.

### 2. Introducción:

Todos los activos de información y los datos almacenados son propiedad del **BACHILLERATO TECNICO AUTODIRIGIDO**. La información, independientemente de su ubicación física o electrónica, es un activo valioso que debe manejarse con responsabilidad. La seguridad de la información busca garantizar la disponibilidad, integridad y confidencialidad de los datos, asegurando la continuidad del negocio, minimizando riesgos y maximizando el retorno de inversiones.

### 3. Alcance:



- a. La información es crucial para todos los procesos y áreas del **BACHILLERATO TECNICO AUTODIRIGIDO**.
- b. Esta política se aplica a todos los miembros de la institución.

### 4. Objetivos de seguridad de la información:

- a. Comprender y tratar los riesgos operativos y estratégicos en seguridad de la información para mantenerlos en niveles aceptables.
- b. Proteger la confidencialidad de la información de estudiantes, autorizaciones de tratamiento de datos personales, datos académicos, contratos de matrícula, entre otros.
- c. Conservar la integridad de los registros contables.
- d. Garantizar que los servicios web de acceso público y las redes internas cumplan con las especificaciones de disponibilidad requeridas.

### 5. Riesgos Específicos:

Abordar los riesgos potenciales, como la pérdida de información por accesos no autorizados, ataques de ciberdelincuentes y posibles amenazas internas. Establecer medidas preventivas y correctivas para mitigar estos riesgos.

|                                                                                   |                                                |                                                                                     |
|-----------------------------------------------------------------------------------|------------------------------------------------|-------------------------------------------------------------------------------------|
|  | <b>SISTEMA DE GESTION DE LA CALIDAD</b>        |  |
|                                                                                   | <b>GESTIÓN DE COMUNICACIÓN A LA COMUNIDAD</b>  |                                                                                     |
|                                                                                   | <b>POLITICA DE SEGURIDAD DE LA INFORMACIÓN</b> |                                                                                     |

## 6. Formación en Seguridad de la Información:

**Capacitaciones Periódicas:** Realizar sesiones de capacitación periódicas para mantener actualizado al personal y a los estudiantes adultos sobre las últimas amenazas de seguridad, vulnerabilidades y medidas de protección. Estas capacitaciones pueden ser conducidas por expertos internos o externos en seguridad informática y adaptarse a la evolución del panorama de ciberseguridad.

**Boletines de Seguridad:** Complementar las capacitaciones con boletines regulares por correo electrónico o mediante otros canales internos que destaquen información relevante sobre amenazas de seguridad, casos de interés y mejores prácticas. Incluye consejos prácticos para aplicar en el día a día.

## 7. Responsabilidades:

Cada persona es individualmente responsable por la seguridad de la información del **BACHILLERATO TECNICO AUTODIRIGIDO**. Todos los empleados, estudiantes, contratistas o asociados con acceso a nuestros sistemas informáticos, deben cumplir el respectivo acuerdo de confidencialidad. Además, debemos tener conocimiento y apoyar a las siguientes funciones de seguridad:

- Los propietarios de la información y los sistemas: **BACHILLERATO TECNICO AUTODIRIGIDO** cuenta con responsables de la custodia de los datos y sistemas que ayuden con dicha finalidad. Funciones que permiten comprender los riesgos relacionados con los sistemas y sostener las tecnologías y los procesos necesarios para asegurar sus datos.
- Los equipos de TI: Muchos controles del marco de seguridad de la Información del **BACHILLERATO TECNICO AUTODIRIGIDO** están directamente configurados en nuestros sistemas de TI y procesos de apoyo.
- Otras funciones de control interno: Recursos Humanos, Auditoría Interna tienen conocimientos especializados y también trabajan con los equipos de TI para garantizar la seguridad de la información del **BACHILLERATO TECNICO AUTODIRIGIDO**.

- a. El comité de calidad es el responsable de asegurar que la seguridad de la información se gestiona adecuadamente en toda la organización.



## SISTEMA DE GESTION DE LA CALIDAD

## GESTIÓN DE COMUNICACIÓN A LA COMUNIDAD

## POLITICA DE SEGURIDAD DE LA INFORMACIÓN



- b. Cada líder de proceso es responsable de garantizar que las personas que trabajan en su equipo protejan la información de acuerdo con las normas establecidas por la organización.
- c. El responsable de seguridad (oficial de protección de datos) asesorara y proporcionara apoyo especializado al personal de la organización y garantiza que los informes sobre la situación de la seguridad de la información están disponibles.
- d. Cada miembro del **BACHILLERATO TECNICO AUTODIRIGIDO**. tiene la responsabilidad de mantener la seguridad de información dentro de las actividades relacionadas con su trabajo.

### 8. Políticas Específicas de Uso:

**Desarrollo de Políticas:** Crear políticas específicas de uso que aborden áreas clave, como el manejo de contraseñas, el uso de dispositivos personales, la navegación segura por internet y cualquier otra práctica relevante para la seguridad de la información en el **BACHILLERATO TECNICO AUTODIRIGIDO**.

Establecer requisitos claros para la creación y gestión de contraseñas seguras, incluyendo la periodicidad para cambiarlas y la prohibición de compartir contraseñas.

**Comunicación:** Comunicar las políticas de uso de manera clara y accesible a todos los miembros de la institución. Puedes utilizar varios canales, como correo electrónico, tabloneros de anuncios físicos o virtuales, y durante las sesiones de capacitación periódicas.

Destacar las razones detrás de cada política para que los empleados y estudiantes adultos comprendan la importancia de seguir las pautas establecidas.

**Capacitación Específica:** Integrar información sobre las políticas específicas de uso en las sesiones de capacitación periódicas para asegurar que todos estén al tanto de las expectativas y procedimientos.

**Revisión y Actualización:** Revisar y actualizar las políticas periódicamente para reflejar los cambios en las amenazas de seguridad y para garantizar que sigan siendo efectivas y relevantes.

**Registro de Aceptación:** Solicitar a los empleados y estudiantes adultos que confirmen su comprensión y aceptación de las políticas específicas de uso. Mantener un registro de estas aceptaciones para referencia futura.



SISTEMA DE GESTION DE LA CALIDAD

GESTIÓN DE COMUNICACIÓN A LA COMUNIDAD

POLITICA DE SEGURIDAD DE LA INFORMACIÓN



### Consecuencias del Incumplimiento:

El incumplimiento de esta política, puede dar lugar a sanciones disciplinarias como por ejemplo la rescisión del contrato de trabajo o de contratos con terceros y consecuencias personales, tales como acciones judiciales y/o investigaciones penales. Sin embargo, el apoyo activo de esta Política y su implementación en nuestro Marco de Seguridad de la Información puede reducir los riesgos colectivos de seguridad de información que enfrentamos; y garantizar el éxito continuo de la **BACHILLERATO TECNICO AUTODIRIGIDO**. La inadecuada protección afecta al rendimiento general de una empresa y puede afectar negativamente a la imagen, reputación y confianza de los clientes

### 9. Reporte de Incidentes:

**Proceso de Reporte:** Establecer un proceso claro y accesible para que los empleados y estudiantes adultos informen cualquier incidente de seguridad de la información. Proporcionar canales seguros, como un correo electrónico dedicado o un formulario en línea.

**Manejo de Incidentes:** Designar un equipo de respuesta a incidentes que sea responsable de evaluar, gestionar y mitigar cualquier incidente reportado. Este equipo debe contar con los recursos necesarios para abordar incidentes de manera efectiva.

**Comunicación Post-Incidente:** Desarrollar un protocolo de comunicación para informar a los afectados y a las partes interesadas sobre incidentes significativos. La transparencia en la comunicación es clave para mantener la confianza.

**Análisis Post-Incidente:** Realizar análisis post-incidente para entender las causas y las lecciones aprendidas. Utilizar estos análisis para mejorar continuamente los controles de seguridad.

### 10. Respaldo y Recuperación de Datos:

Establecer políticas y procedimientos para realizar respaldos periódicos de los datos críticos y garantizar la disponibilidad de mecanismos eficientes de recuperación en caso de pérdida de datos o desastres.

### 11. Políticas de Acceso:



**SISTEMA DE GESTION DE LA CALIDAD**

**GESTIÓN DE COMUNICACIÓN A LA COMUNIDAD**

**POLITICA DE SEGURIDAD DE LA INFORMACIÓN**



Detallar las políticas de acceso a sistemas y datos, incluyendo la gestión de permisos y la revisión periódica de los accesos para garantizar la mínima exposición necesaria.

**12. Política de Dispositivos Móviles:**

Establecer reglas para el uso seguro de dispositivos móviles dentro de la institución, tales como conexiones no seguras, cifrado de datos, acceso a redes sociales, gestión de contraseñas. incluyendo la seguridad de la información almacenada y la conexión a redes internas.

**13. Monitoreo y Auditoría:**

Definir políticas para el monitoreo continuo de los sistemas y la realización de auditorías de seguridad de forma regular, identificando y respondiendo a actividades sospechosas.

**14. Cumplimiento Legal y Normativo:**

La política de seguridad de la información debe cumplir con las leyes y regulaciones aplicables en materia de privacidad y protección de datos.

**15. Concientización Continua:**

Establecer programas de concientización continua sobre seguridad de la información para mantener a todos los miembros de la institución informados y comprometidos.

|           |                                                                |  |
|-----------|----------------------------------------------------------------|--|
| Realizado | <b>Jairo Pabón</b><br><i>Supervisor de desarrollo</i>          |  |
| Revisado  | <b>José Martínez</b><br><i>Administrador del sistema</i>       |  |
|           | <b>Gustavo Garrido</b><br><i>Revisor fiscal</i>                |  |
|           | <b>Liceth Achkar</b><br><i>Gerencia Control Interno</i>        |  |
| Aprobado  | <b>Álvaro Rodelo Sierra</b><br><i>Dirección Administrativo</i> |  |
|           | <b>Jairo Rodelo Sierra</b><br><i>Director General</i>          |  |