

# Política de **Seguridad de la Información**

hgi

## Objetivos Seguridad de la Información



Gestionar los riesgos de seguridad de la información y potencializar las amenazas del entorno.



Cumplir los requisitos legales y reglamentarios aplicables relacionados con la seguridad de la información.



Estructurar planes de capacitación y sensibilización para el logro de la seguridad de la información.



Promover mejores prácticas y controles en todos los niveles de la organización que conlleven a la mejora continua del Sistema.



- En **HGI** controlamos el acceso áreas e información.
- Sensibilizamos **al usuario** para el uso adecuado de claves y contraseñas.
- Buenas prácticas para uso del internet y el **correo electrónico**.
- Controlamos **la información** en los equipos desatendidos



Nuestra Política de **Seguridad de la información** esta comprometida con estos **tres aspectos**:



### **Confidencialidad**

Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.



### **Disponibilidad**

Propiedad de la información de estar accesible y utilizable cuando lo requiera nuestro cliente.



### **Integridad**

Propiedad de la información relativa a su exactitud y completitud.

## Objetivo del **Sistema de Gestión Seguridad de la Información**

Establecer los mecanismos y herramientas de gestión que permitan la disponibilidad, confidencialidad e integridad de los activos de información.

## Políticas de **Seguridad de la Información**

1

Generar atributos de confidencialidad de la información en actividades y procesos.

2

Establecer mecanismos de disponibilidad de la información y los sistemas y servicios de tecnología de la información.

3

Proteger la integridad de la información en los procesos del negocio.

4

Cumplir la legislación actual aplicable al ejercicio.

## Política de **Controles Criptográficos**

### **Cifrado**

La información que por petición del cliente deba ser codificada, será tratada por medios de la política de encriptación.

### **Autorización**

Solo al personal autorizado se le permite codificar y decodificar la información.



## Política de Seguridad Física

### Cámaras

Las instalaciones cuentan con circuito cerrado de información.

### Alarma

Control de detección a tiempo de una intrusión indeseada.

### Carné

El personal externo que accede a nuestras instalaciones debe de estar identificado y acompañado durante todo su recorrido.

### Visitantes

Los visitantes deben ser registrados, identificados y definidas las áreas a las que tendrá acceso.



## Política de **Controles de Código Malicioso**

### **Informar**

Es deber de todos los usuarios reportar señales de código malicioso e incidentes que afecten la seguridad en la información.

### **Eliminar**

Los mensajes de correo electrónico identificados como peligroso, debe ser eliminados en el mismo momento que sean identificados.

## Política de **Transferencia de Información**

### **Transferencia**

La transferencia de información clasificada como confidencial debe ser a través de medios seguros.

### **Cifrado**

La información sensible como bases de datos debe ser transmitida de manera cifrada.

### **Medios**

Para la transferencia de información solo se debe utilizar el correo corporativo.





## Política de Relaciones con Proveedores

HGI S.A.S define claramente la política de relación con los proveedores para el servicio de Facturación Electrónica.

## Política de Relaciones con Proveedores

- ✓ Acuerdos de custodia y confidencialidad de la información
- ✓ Seguridad en el intercambio de información con proveedores
- ✓ Certificación de seguridad de la Información de los proveedores
- ✓ Manejo de incidentes de seguridad asociados a los servicios
- ✓ Acuerdos de niveles de servicios y los planes de recuperación
- ✓ Entrega y difusión de las políticas de seguridad de los proveedores





hggi