

## POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

### INTERNAUTA S.A.S.

#### 1. INTRODUCCIÓN

La Dirección de **INTERNAUTA S.A.S.**, reconociendo la importancia de una adecuada gestión y protección de los activos de información, establece la presente Política General de Seguridad y Privacidad de la Información, en concordancia con la normativa aplicable al sector de telecomunicaciones y tomando como referencia los estándares de la familia **ISO/IEC 27000**.

INTERNAUTA S.A.S. busca fortalecer la protección de la información mediante la definición de políticas, procedimientos, controles y responsabilidades orientados a garantizar un manejo seguro de la información y de los recursos tecnológicos de la organización.

La presente política busca generar confianza entre la compañía, sus clientes, colaboradores, proveedores y demás partes interesadas, promoviendo el cumplimiento de las obligaciones legales, regulatorias y contractuales aplicables.

#### 2. OBJETO

La presente política tiene como propósito establecer los lineamientos generales para gestionar y reducir los riesgos asociados a la seguridad de la información, protegiéndola bajo los principios de:

- **Confidencialidad:** garantizar que la información sea conocida únicamente por personas autorizadas.
- **Integridad:** preservar la exactitud, consistencia y completitud de la información.
- **Disponibilidad:** asegurar que la información y los servicios se encuentren disponibles cuando sean requeridos.

Para ello, INTERNAUTA S.A.S. busca:

- Proteger sus activos de información y tecnológicos.
- Reducir los riesgos que puedan afectar sus procesos y servicios.
- Fortalecer la cultura de seguridad de la información.



Celular:  
(310) 886-3877



Correo:  
Oficina@internauta.com



Dirección:  
Cra 9B Este # 22D-20 Sur  
Barrio San Blas

- Establecer responsabilidades relacionadas con la protección de la información.
- Garantizar la continuidad de las operaciones ante incidentes.
- Cumplir las obligaciones legales, regulatorias y contractuales aplicables.
- Promover la mejora continua de sus controles y medidas de seguridad.

### 3. ALCANCE

Esta política aplica a todos los colaboradores, contratistas, proveedores y terceros que tengan acceso a información, sistemas, redes, equipos o recursos tecnológicos de **INTERNAUTA S.A.S.**

Todos los usuarios deberán cumplir los lineamientos establecidos y utilizar los recursos de información de manera responsable y segura.

### 4. GLOSARIO

**Sistema de Gestión de Seguridad de la Información (SGSI):** conjunto de políticas, procedimientos, controles y medidas destinados a proteger los activos de información de la organización.

**Confidencialidad:** propiedad que garantiza que la información no sea divulgada a personas no autorizadas.

**Integridad:** propiedad que permite conservar la exactitud y completitud de la información.

**Disponibilidad:** condición que permite que la información y los sistemas puedan ser utilizados por los usuarios autorizados cuando sean necesarios.

**Control:** medida implementada para prevenir, reducir o gestionar un riesgo de seguridad de la información.

### 5. POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Para proteger la confidencialidad, integridad y disponibilidad de la información, **INTERNAUTA S.A.S.** establece los siguientes lineamientos:

**5.1. Responsabilidades:** la compañía definirá y comunicará las responsabilidades relacionadas con la seguridad de la información a sus colaboradores, proveedores y terceros.



Celular:  
(310) 886-3877



Correo:  
Oficina@internauta.com



Dirección:  
Cra 9B Este # 22D-20 Sur  
Barrio San Blas

**5.2. Control de acceso:** el acceso a la información y a los sistemas estará limitado a personal autorizado de acuerdo con sus funciones y permisos.

**5.3. Protección frente a terceros:** se establecerán medidas para proteger la información cuando intervengan proveedores, contratistas o terceros.

**5.4. Uso adecuado de la información:** se implementarán controles para prevenir usos indebidos que puedan generar impactos operativos, financieros o legales.

**5.5. Protección frente a amenazas:** se aplicarán medidas para prevenir y gestionar amenazas internas y externas que puedan afectar la información.

**5.6. Seguridad de los equipos:** los colaboradores deberán adoptar buenas prácticas para proteger los equipos y evitar accesos no autorizados.

**5.7. Seguridad de redes y recursos tecnológicos:** INTERNAUTA S.A.S. implementará controles destinados a proteger sus redes, sistemas e infraestructura tecnológica.

**5.8. Seguridad en los sistemas:** la seguridad será considerada dentro de los procesos de implementación, mantenimiento y actualización de los sistemas de información.

**5.9. Gestión de eventos e incidentes:** los eventos de seguridad serán identificados, gestionados y documentados, buscando fortalecer continuamente los controles de la organización.

**5.10. Continuidad:** se implementarán medidas para contribuir a la continuidad de las operaciones y servicios ante incidentes que puedan afectar la infraestructura tecnológica.

**5.11. Cumplimiento:** INTERNAUTA S.A.S. cumplirá las obligaciones legales, regulatorias y contractuales relacionadas con la seguridad y privacidad de la información.

**5.12. Protección de información confidencial:** cuando corresponda, se aplicarán mecanismos de protección adecuados para la información confidencial.

**5.13. Dispositivos y recursos:** se establecerán medidas de seguridad de acuerdo con el tipo de dispositivo, recurso y clasificación de la información.

**5.14. Copias de respaldo:** se realizarán copias de respaldo de la información crítica de acuerdo con las necesidades de la organización, buscando garantizar su recuperación.



**Celular:**  
(310) 886-3877



**Correo:**  
Oficina@internauta.com



**Dirección:**  
Cra 9B Este # 22D-20 Sur  
Barrio San Blas

**5.15. Transferencia de información:** el intercambio de información deberá realizarse mediante mecanismos adecuados de seguridad y confidencialidad.

**5.16. Seguridad en aplicaciones:** los sistemas y aplicaciones utilizados por INTTERNAUTA deberán considerar medidas de seguridad durante su implementación y mantenimiento.

**5.17. Proveedores:** los acuerdos con proveedores y terceros que tengan acceso a información o recursos tecnológicos deberán contemplar las condiciones de seguridad correspondientes.

**5.18. Gestión y reporte de incidentes:** los incidentes de seguridad serán registrados y gestionados de acuerdo con los procedimientos internos y las obligaciones regulatorias aplicables.

El incumplimiento de las disposiciones establecidas en esta política podrá generar las acciones correspondientes de acuerdo con la normativa interna de la organización y la legislación colombiana vigente.

## 6. ROLES Y RESPONSABILIDADES

**Alta Dirección:** aprobar la política, proporcionar los recursos necesarios y promover su cumplimiento.

**Área técnica o tecnológica:** implementar y mantener los controles de seguridad, gestionar los riesgos tecnológicos y apoyar la atención de incidentes.

**Responsables de procesos:** aplicar los controles y procedimientos de seguridad relacionados con sus actividades.

**Colaboradores, contratistas y proveedores:** cumplir las políticas establecidas, proteger la información a la que tengan acceso y reportar oportunamente cualquier evento o incidente de seguridad.

## 7. SEGUIMIENTO Y MEJORA

INTTERNAUTA S.A.S. realizará revisiones periódicas de sus medidas de seguridad con el propósito de evaluar su efectividad, identificar riesgos y establecer oportunidades de mejora.

La política será revisada, entre otros casos, cuando:

- Se presenten cambios regulatorios.



**Celular:**  
(310) 886-3877



**Correo:**  
Oficina@intternauta.com



**Dirección:**  
Cra 9B Este # 22D-20 Sur  
Barrio San Blas

- Se produzcan modificaciones importantes en la organización o infraestructura tecnológica.
- Se presenten incidentes que requieran ajustes.
- Se identifiquen nuevos riesgos de seguridad.

## 8. APROBACIÓN Y CONTROL DEL DOCUMENTO

La presente política entrará en vigencia una vez sea aprobada por la Dirección de **INTERNAUTA S.A.S.**

Deberá ser revisada periódicamente y actualizada cuando las condiciones legales, tecnológicas, operativas o de seguridad de la organización así lo requieran.

## 9. ANEXOS

Como parte de la gestión de seguridad de la información, INTERNAUTA S.A.S. podrá contar con formatos para el registro y seguimiento de incidentes de seguridad, así como con los demás documentos, procedimientos e instructivos necesarios para la aplicación de esta política.

## 1. INFORMACIÓN GENERAL DEL INCIDENTE

| Campo            | Información     |
|------------------|-----------------|
| Número incidente | de INC-2026-001 |
| Fecha detección  | de DD/MM/AAAA   |
| Hora detección   | de HH           |
| Fecha de reporte | DD/MM/AAAA      |



Celular:  
(310) 886-3877



Correo:  
Oficina@internauta.com



Dirección:  
Cra 9B Este # 22D-20 Sur  
Barrio San Blas



**Persona que reporta** Nombre completo

**Cargo / área** Cargo o área responsable

**Medio de reporte** Correo / teléfono / sistema / otro

**Tipo de incidente** Malware / phishing / acceso no autorizado / falla de sistema / ataque / pérdida de información / otro

**Nivel de impacto** Bajo / Medio / Alto / Crítico

**Estado** Abierto / En investigación / Contenido / Cerrado



**Celular:**  
(310) 886-3877



**Correo:**  
Oficina@internauta.com



**Dirección:**  
Cra 9B Este # 22D-20 Sur  
Barrio San Blas