

# **PRESENTACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y CONTRATO DE SERVICIOS TECNOLÓGICOS**

## **1. Bienvenida y Objetivo de la Reunión**

Buen día, **Sr. Irving Bernal Arango**, como Representante Legal de **PROMOTORA PALMERA DE ANTIOQUIA S.A.S.**, queremos presentarle las **Políticas de Seguridad de la Información**, junto con los procedimientos de trazabilidad necesarios para garantizar su cumplimiento. Además, abordaremos la relación entre estas políticas y el **Contrato de Prestación de Servicios Tecnológicos**, asegurando que las medidas de seguridad se implementen en cada etapa del servicio.

Esta reunión tiene como propósito concientizar sobre la importancia de la seguridad de la información y definir los lineamientos estratégicos que debemos adoptar para minimizar riesgos y garantizar la continuidad operativa.

## **2. Importancia de la Seguridad de la Información**

**¿Por qué es un tema clave para la empresa?**

La seguridad de la información es crucial porque:

- Protege nuestros datos contra accesos no autorizados y ciberataques.
- Asegura la integridad y disponibilidad de la información.
- Cumple con normativas internacionales y mejores prácticas.
- Garantiza la continuidad del negocio y evita pérdidas económicas.

## **3. Políticas de Seguridad de la Información**

### **3.1. Políticas Generales**

- Todos los empleados deben firmar un acuerdo de confidencialidad.
- Se realizarán capacitaciones periódicas en seguridad.
- Implementación de controles estrictos en el acceso a información sensible.

### **3.2. Control de Accesos**

- Uso obligatorio de credenciales seguras.
- Implementación de autenticación multifactorial (MFA) para accesos críticos.

- Auditoría y supervisión de accesos a sistemas y archivos sensibles.

### **3.3. Gestión de Riesgos**

- Identificación de amenazas y vulnerabilidades en nuestros sistemas.
- Medidas de mitigación y planes de respuesta ante incidentes.
- Evaluaciones y auditorías de seguridad regulares.

### **3.4. Seguridad en la Gestión de Proyectos Tecnológicos**

- Incorporación de seguridad desde la planificación de proyectos.
- Pruebas de vulnerabilidad en nuevos sistemas.
- Documentación clara de las medidas de seguridad implementadas.

## **4. Seguridad Física del Área de Servidores y Control de Accesos**

### **4.1. Medidas de Protección para el Área de Servidores**

- Acceso restringido solo al personal autorizado.
- Implementación de controles biométricos o tarjetas de acceso.
- Cámaras de seguridad activas las 24 horas.
- Sistemas de refrigeración y protección contra incendios.

### **4.2. Control de Accesos a las Áreas Sensibles**

- Registro detallado de ingresos y salidas.
- Inspección periódica de accesos y cámaras de seguridad.
- Prohibición del uso de dispositivos externos sin autorización.
- 

## **5. Relación con el Contrato de Servicios Tecnológicos**

Las políticas de seguridad de la información están directamente relacionadas con el **Contrato de Prestación de Servicios Tecnológicos**, asegurando que:

- Todo proveedor cumpla con los estándares de seguridad de la empresa.
- Se establezcan cláusulas de confidencialidad y manejo seguro de la información.
- Se exijan pólizas de cumplimiento y garantía en los servicios contratados.
- Los pagos se realicen solo después de validar los resultados en reuniones semanales de gestión.
- Se mantenga una trazabilidad detallada del cumplimiento del SLA (Acuerdo de Nivel de Servicio).

**Puntos clave en el contrato:**

- Definición de responsabilidades de los proveedores en términos de seguridad.
- Procedimientos de monitoreo y auditoría de los servicios tecnológicos.
- Protocolos de respuesta ante incidentes de seguridad.
- Evaluación del desempeño y continuidad operativa en función del SLA.

## **6. Procedimientos de Trazabilidad y Cumplimiento**

### **6.1. Registro y Monitoreo de Actividades**

- Todos los accesos a los sistemas deben ser registrados en logs de auditoría.
- Implementación de alertas ante accesos no autorizados o intentos de intrusión.
- Revisión mensual de los registros por el área de TI.

### **6.2. Capacitación y Concientización**

- Programación de capacitaciones semestrales sobre seguridad de la información.
- Simulaciones de incidentes de seguridad para medir tiempos de respuesta.
- Encuestas anuales para evaluar el conocimiento de los empleados sobre las políticas.

### **6.3. Evaluación y Mejoramiento Continuo**

- Auditorías internas anuales para revisar el cumplimiento de las políticas.
- Identificación de mejoras y actualización de protocolos según nuevas amenazas.
- Reporte de incidentes de seguridad con análisis de causa raíz y plan de mitigación.
- 

## **7 Responsabilidades del Representante Legal y del Equipo Directivo**

Como Representante Legal, su liderazgo en la implementación de estas políticas es clave. Sus responsabilidades incluyen:

- Aprobar y supervisar la ejecución de estas políticas.
- Garantizar que todos los empleados cumplan con las normativas de seguridad.
- Apoyar la inversión en tecnologías y recursos necesarios para la protección de la información.
- Fomentar una cultura organizacional basada en la seguridad y la prevención de riesgos.

## 8. Conclusión y Espacio para Preguntas

La seguridad de la información es responsabilidad de toda la empresa, con un liderazgo fuerte desde la dirección.

- Las políticas establecidas protegen a la empresa y a cada uno de sus colaboradores.
- Implementar buenas prácticas fortalece nuestra seguridad y operación.
- La trazabilidad nos permite garantizar el cumplimiento de estas medidas de seguridad.
- La alineación con el contrato de servicios tecnológicos asegura la ejecución efectiva de estas políticas.

**¡Es importante el compromiso de la gerencia con la seguridad de la información!**

### **Espacio para Preguntas y Discusión:**

Ahora abrimos el espacio para dudas y comentarios. **Sr. Irving Bernal Arango, ¿tiene alguna inquietud o sugerencia sobre estas políticas y procedimientos?**

# **Procedimientos y Trazabilidad de las Políticas de Seguridad de la Información**

## **1. Procedimientos y Trazabilidad de las Políticas Generales**

### **Procedimientos:**

- Todo nuevo empleado debe firmar un acuerdo de confidencialidad antes de acceder a cualquier información de la empresa.
- Se realizarán capacitaciones periódicas sobre seguridad de la información.
- Se implementará un control de acceso a la información mediante roles y permisos específicos según las funciones del empleado.

### **Trazabilidad:**

- Registro de firmas de acuerdos de confidencialidad almacenado en la base de datos de RRHH.
- Registro de asistencia a capacitaciones y evaluaciones periódicas.
- Reporte de cambios en roles y permisos dentro del sistema de gestión de accesos.

## **2. Procedimientos y Trazabilidad del Control de Accesos**

### **Procedimientos:**

- Implementación de credenciales seguras con autenticación multifactorial (MFA) para accesos críticos.
- Revisión periódica de los accesos otorgados a cada empleado y revocación de permisos innecesarios.
- Monitoreo en tiempo real de accesos a sistemas críticos mediante herramientas de seguridad.

### **Trazabilidad:**

- Registro de accesos exitosos y fallidos en logs de auditoría.
- Reportes semanales de revisión de accesos.
- Historial de modificaciones de permisos y revocaciones.

## **3. Procedimientos y Trazabilidad de la Gestión de Riesgos**

**Procedimientos:**

- Identificación y clasificación de activos de información.
- Análisis de vulnerabilidades y amenazas a los sistemas de información.
- Elaboración y ejecución de planes de mitigación de riesgos.

**Trazabilidad:**

- Registro de evaluaciones de riesgos realizadas trimestralmente.
- Historial de incidentes de seguridad y medidas correctivas aplicadas.
- Reportes de auditorías internas y externas.

## **4. Procedimientos y Trazabilidad en Seguridad en la Gestión de Proyectos Tecnológicos**

**Procedimientos:**

- Incorporación de pruebas de seguridad en cada fase del ciclo de vida de desarrollo de software.
- Implementación de controles de acceso y encriptación en nuevas soluciones tecnológicas.
- Validación de cumplimiento de estándares de seguridad antes del despliegue de un nuevo sistema.

**Trazabilidad:**

- Registro de pruebas de seguridad realizadas y resultados obtenidos.
- Documentación de requisitos de seguridad en cada proyecto.
- Historial de auditorías de cumplimiento de estándares.

## **5. Procedimientos y Trazabilidad en la Seguridad Física del Área de Servidores y Control de Accesos**

**Procedimientos:**

- Acceso restringido únicamente a personal autorizado mediante credenciales biométricas o tarjetas de acceso.
- Implementación de cámaras de seguridad y monitoreo en tiempo real.
- Revisión y mantenimiento periódico de los sistemas de seguridad física.

**Trazabilidad:**

- Registro de ingresos y salidas del área de servidores.
- Historial de grabaciones de cámaras de seguridad.

- Reportes de mantenimiento de sistemas de seguridad.

## **6. Procedimientos y Trazabilidad en Capacitación y Concientización**

### **Procedimientos:**

- Planificación de capacitaciones semestrales sobre seguridad de la información.
- Aplicación de pruebas de conocimiento antes y después de cada capacitación.
- Simulaciones de incidentes de seguridad para medir tiempos de respuesta.

### **Trazabilidad:**

- Registro de asistencia a capacitaciones y resultados de pruebas.
- Reportes de desempeño en simulaciones de seguridad.
- Encuestas de percepción sobre la cultura de seguridad dentro de la empresa.

## **7. Procedimientos y Trazabilidad en Evaluación y Mejoramiento Continuo**

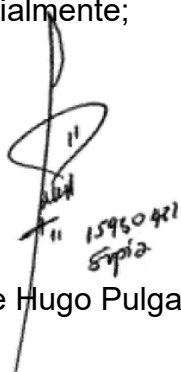
### **Procedimientos:**

- Auditorías internas anuales para verificar el cumplimiento de las políticas.
- Análisis de incidentes de seguridad y definición de planes de mejora.
- Revisión y actualización periódica de las políticas de seguridad.

### **Trazabilidad:**

- Registro de auditorías y hallazgos detectados.
- Historial de incidentes de seguridad y acciones correctivas aplicadas.
- Control de versiones y actualizaciones de las políticas de seguridad.

Cordialmente;



Jorge Hugo Pulgarin B.