# Protocolo de Seguridad para Proteger la Información Sensible de SANOFI

Tiene como objetivo establecer una serie de medidas en busca de garantizar que la información sensible de nuestra compañía esté protegida en todo momento. Mantener estos estándares es responsabilidad de todos, y su cumplimiento es vital para la seguridad de nuestra organización y sus colaboradores.

## 1. Políticas de Escritorio Limpio.

**Clean Desk:**

- Todos los empleados deben asegurarse de que sus escritorios estén libres de documentos sensibles al final del día. Los documentos importantes deben ser guardados en cajones con llave.

**Máquinas de Destrucción de Papel**:

- Utilizar máquinas pica papel para destruir cualquier documento que contenga información sensible antes de desecharlo.

## 2. Control de Áreas Restringidas.

**Acceso Restringido:**

- No se debe permitir el acceso a áreas restringidas a personas no autorizadas.

**Supervisión de Visitantes:**

- Los visitantes deben ser siempre acompañados por un empleado de la compañía cuando se encuentren en áreas restringidas.

## 3. Gestión de Visitantes.

**Acompañamiento:**

- Los visitantes solo pueden ingresar en compañía de un empleado autorizado.

**Carnets de Visitantes:**

- Asignar un carnet temporal a los empleados de otras filiales para controlar su acceso durante el tiempo de su visita.

## 4. Reuniones y Presentaciones

**Tableros y Documentos:**

- Al finalizar una reunión, asegúrese de borrar los tableros y recoger todos los documentos. Los documentos deben ser destruidos adecuadamente si contienen información sensible.

**Suspensión de Reuniones con información sensible:**

- Si una persona desconocida ingresa a una reunión, se debe suspender inmediatamente hasta que se verifique su identidad.

## 5. *Seguridad Digital.*

**Bloqueo de Computadoras:**

- Los empleados deben bloquear sus computadoras cada vez que se ausenten de su estación de trabajo.

**Sistemas de Protección:**

- La compañía cuenta con un sistema de protección de información que debe ser seguido rigurosamente.

## 6. *Reporte de Actividades Sospechosas.*

**Estudio de Seguridad:**

- Todos los empleados pasan por un estudio de seguridad al ingresar a la organización.

**Alertas:**

- Si se nota alguna actividad sospechosa, debe comunicarse de inmediato al gerente de seguridad.

## 7. *Inducción de Nuevos Empleados y Terceros.*

**Incorporación de Recomendaciones:**

- Durante la inducción de nuevos empleados y terceros, se incluirán estas recomendaciones de seguridad para garantizar que todos estén informados y comprometidos con la protección de la información sensible.

## 8. *Sensibilización Continua:*

**Comunicación Regular:**

- Enviar comunicados periódicos a todos los empleados reforzando los puntos más relevantes de este protocolo.

**Capacitaciones:**

- Realizar capacitaciones periódicas para actualizar y recordar a los empleados sobre las mejores prácticas de seguridad.