¡Desafía tu historia
y hagámosla
extraordinaria!

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

DOBLEUESE ATELIER, S.A.P.I DE C.V.

1. Objeto.

La presente Política tiene como objetivo establecer las directrices y lineamientos para garantizar la protección de la información generada, utilizada, almacenada o compartida por Dobleuese Atelier, S.A.P.I. de C.V., incluyendo información creativa, estratégica, técnica, comercial y personal.

Dada la naturaleza de nuestros servicios —que involucran campañas confidenciales, bases de datos de clientes, activos creativos y relaciones con proveedores y medios—, la seguridad de la información representa un pilar crítico para el cumplimiento de los compromisos contractuales, normativos y éticos de la agencia.

2. Alcance.

Esta política aplica a:

- Todo el personal interno de la agencia: empleados, socios, becarios y directivos.
- Personal externo: freelancers, consultores, proveedores, y otros terceros que tengan acceso a información de la agencia o sus clientes.
- Toda la información generada o recibida en el marco de nuestras actividades, sin importar su formato (físico o digital) ni el medio a través del cual se almacene o transmita.

3. Principios Rectores.

- **Confidencialidad:** Proteger la información estratégica y sensible (campañas, presupuestos, briefings, propuestas creativas, contratos, datos personales) de accesos no autorizados.
- **Integridad:** Asegurar que la información no sea alterada sin autorización y se mantenga precisa y completa.
- **Disponibilidad:** Garantizar el acceso oportuno a la información por parte de quienes la requieran para su función.
- **Legalidad y ética:** Cumplir con la legislación aplicable (como la LFPDPPP) y con los más altos estándares éticos en el uso de la información.

4. Clasificación de la Información.

La información será clasificada conforme a su nivel de sensibilidad:

Nivel	Descripción	Ejemplos
Pública	Información que puede divulgarse sin restricción.	Portafolio público, contenido publicado en redes, promociones.
Interna	Uso exclusivo del personal de la agencia.	Manuales internos, formatos operativos.
Confidencial	Información sensible que puede afectar a la agencia o sus clientes si se divulga.	Estrategias creativas, presupuestos, campañas en desarrollo, contratos.
Información de terceros	Información de clientes y proveedores que debe tratarse con el mismo o mayor cuidado que la confidencial.	Bases de datos, briefings, NDAs, especificaciones técnicas.

5. Responsabilidades.

- **Dirección General:** Aprobar esta política y asignar los recursos necesarios para su ejecución.
- **Responsable de Seguridad de la Información / Data Privacy Officer (DPO):** Supervisar el cumplimiento, coordinar auditorías, responder a incidentes y capacitar al personal.
- **Líderes de área (cuentas, creativo, digital, producción, administración):** Promover el cumplimiento entre sus equipos.
- **Colaboradores y proveedores:** Cumplir con esta política y reportar cualquier vulnerabilidad, sospecha o incidente.

6. Medidas Generales de Seguridad.

- **Físicas:** Control de accesos a oficinas; credenciales, cámaras de vigilancia, áreas restringidas para documentación sensible.
- **Digitales:**

a. Contraseñas robustas actualizadas cada 90 días.
b. Autenticación multifactor en plataformas sensibles (correo, CRM, drives).
c. Encriptación de archivos con datos personales o de campañas en desarrollo.
d. Antivirus actualizado y firewall en todos los equipos.
e. Control de acceso por roles en carpetas compartidas.
f. Políticas de bloqueo automático de pantalla y de sesión.
g. Prohibición del uso de equipos personales para información sensible salvo autorización expresa.

7. Seguridad en el Uso de Equipos y Dispositivos.

- Todo equipo proporcionado por la agencia (computadoras, cámaras, tablets, discos duros) es de uso exclusivo para fines laborales.
- En caso de teletrabajo, se deberán seguir las políticas de acceso seguro (VPN, escritorio remoto).
- En caso de pérdida, robo o daño del equipo, se deberá reportar inmediatamente al DPO o al área de IT.
- Está prohibido conectar dispositivos externos (USB, discos) sin validación previa del área responsable.

8. Seguridad en Comunicaciones.

- La información estratégica o confidencial se debe compartir exclusivamente por canales oficiales (correo corporativo, herramientas con cifrado).
- Está prohibido enviar información de campañas en desarrollo o información de clientes por WhatsApp personal o correos personales.
- Toda presentación o contenido enviado a medios o terceros debe estar validado previamente por las áreas responsables.
- En los contratos con terceros deberá incluirse cláusulas de confidencialidad y seguridad de la información.

9. Manejo de Incidentes de Seguridad.

- Todo incidente deberá ser reportado inmediatamente al DPO o al área legal: filtraciones, accesos no autorizados, hackeos, robo de dispositivos, suplantaciones de identidad.
- Se aplicará un procedimiento de respuesta que incluirá:

a. Evaluación del impacto.
b. Notificación a las partes afectadas.
c. Corrección de la vulnerabilidad.
d. Medidas preventivas y revisión de controles.

- Cuando aplique, se notificará al INAI o a la autoridad correspondiente.

10. Capacitación y Concientización.

- Todo el personal recibirá inducción sobre seguridad de la información al integrarse a la agencia.
- Se impartirán capacitaciones periódicas (mínimo una vez al año) sobre temas como protección de datos, seguridad digital, buenas prácticas y manejo ético de la información.
- Se enviarán boletines con recordatorios y alertas sobre posibles riesgos (phishing, fraudes, etc.).

11. Sanciones El incumplimiento de esta política puede derivar en:

- Sanciones administrativas internas.
- Terminación del vínculo laboral o contractual.
- Reclamaciones por daños y perjuicios.
- Denuncias ante autoridades competentes cuando proceda conforme a la legislación penal o de protección de datos.

12. Revisión y Actualización Esta política será revisada de manera anual por el DPO, o cuando exista:

- Cambio significativo en procesos internos.
- Incidentes que lo ameriten.
- Reformas legales en materia de protección de datos o seguridad informática. Las versiones actualizadas deberán ser comunicadas y firmadas por todo el personal.

Entiendo y acepto la presente Política.
Nombre o Razón Social:
Fecha:
Firma