



Política de Privacidad



Política de Privacidad

Código	PP-DS-01
Versión	1
Fecha de la Versión	01-03-2021
Creado por:	
Aprobado por:	Camilo Fernández

Historial de Modificaciones

Fecha	Versión	Creado por	Descripción de la modificación

Contenido

Objetivo, alcance y usuarios.....	3
Clasificación de información.....	3
Criterios de clasificación.....	3
Niveles de confidencialidad.....	4
Uso de información solicitada a usuarios.....	4
Actualización de datos de usuarios.....	5
Transparencia	5
Eliminación de información de usuarios	6
Etiquetado de la información	6
Manejo de información clasificada.....	7
Divulgación de información.....	8

Objetivo, alcance y usuarios

El propósito de esta política es definir el objetivo, la dirección, los principios y las reglas básicas para la protección y manejo de privacidad de la información de DSIGNER, S. A. y la del usuario.

Los usuarios de este documento son todos los empleados de DSIGNER, S. A. así como también todos los participantes externos que cumplan funciones sensibles y de carácter privado.

Clasificación de información

DSIGNER, S. A. es una empresa que maneja información de carácter confidencial de sus usuarios y clientes, adicionalmente utiliza información de carácter pública sobre los servicios que presta y el funcionamiento de su infraestructura de generación de llaves para generación de Certificados Digitales y Firma Electrónica. Así como la información interna y comunicación propia de sus empleados para la realización de sus procesos y funcionamiento en general.

Criterios de clasificación

El nivel de confidencialidad se determina de acuerdo con los siguientes criterios:

- **Publica:**
 - Información que puede ser divulgada por cualquier índole.
- **Uso Interno:**
 - Información utilizada dentro de la organización para el día a día.
- **Confidencial:**
 - Información que contenga datos sensibles de clientes.
 - Obligaciones legales y contractuales, según contratos y regulaciones legales.

Niveles de confidencialidad

Toda la información debe ser clasificada en los siguientes niveles de confidencialidad.

Nivel de confidencialidad	Etiquetado	Criterios de clasificación	Restricción de acceso
Pública	(sin etiquetar)	Hacer pública la información no puede dañar a la organización de ninguna forma	La información está disponible para todo el público
Uso interno	USO INTERNO	El acceso no autorizado a la información podría ocasionar daños y/o inconvenientes menores a la organización	La información está disponible para todos los empleados y terceros seleccionados
Confidencial	CONFIDENCIAL	El acceso no autorizado a la información podría dañar considerablemente el negocio y/o la reputación de la organización	La información está disponible solamente para un grupo específico de empleados y de terceros autorizados

La regla básica es utilizar el nivel de confidencialidad más bajo garantizando un adecuado nivel de protección para evitar gastos de protección innecesarios.

Uso de información solicitada a usuarios

Toda información solicitada a los usuarios de DSIGNER, S.A., es clasificada como Confidencial, en cualquiera de los servicios a contratar es únicamente utilizada para el propósito del servicio brindado; la organización no utiliza dichos datos e información para otro propósito más que el contratado por el cliente. Dicha información es únicamente utilizada para la identificación apropiada del usuario siendo esta para la generación de su acceso al sistema, así como la generación de su certificado digital.



El uso de la información es estrictamente para los servicios contratados por el solicitante y esta se cataloga de uso interno confidencial la cual no es divulgada a terceros y se encuentra suscrita bajo los acuerdos de confidencialidad previstos por la corporación.

La información general provista por el cliente es la colocada en su certificado digital al momento de su generación y publicación. Es de entera responsabilidad del cliente que dicha información se encuentre actualizada y sea completamente correcta en la entrega de su certificado.

Actualización de datos de usuarios

Es responsabilidad estrictamente del usuario realizar la actualización de datos y de brindar información fidedigna cada vez que DSIGNER, S. A. le solicite sus datos para la actualización de su perfil dentro de la plataforma digital; la actualización de datos tendrá un plazo anual, así como la actualización de sus datos dentro del certificado digital emitido previamente. Dicha actualización no conlleva ningún costo asociado al cliente dentro de la plataforma, el proceso de certificado para firma electrónica tendrá sus propios costos para los usuarios.

Transparencia

DSIGNER, S. A. Como entidad prestadora de servicios de certificación está comprometida con la transparencia y el uso de la información solicitada, el usuario tiene acceso a la información proporcionada, el manejo, edición o eliminación de la misma está disponible para el cliente, y será el que proporcione los datos respecto de la actualización que se encuentran sujetas a verificación y/o validación por parte de la organización.

Eliminación de información de usuarios

El cliente puede solicitar la completa eliminación de su información dentro de los sistemas de DSIGNER, S. A., esto lo puede realizar por medio de los canales de soporte previamente publicados en los sitios web (correo electrónico, chat electrónico y teléfonos).

Adicionalmente DSIGNER, S.A. elimina la información del usuario cuando este solicita la eliminación de su cuenta por medio de la plataforma en línea, así como la eliminación de los datos cuando el usuario ha dejado de utilizar los servicios por más de dos años dentro de la plataforma.

Etiquetado de la información

Los niveles de confidencialidad son etiquetados de la siguiente forma:

- **Documentos en papel:** se indica el nivel de confidencialidad en el pie de página de cada página del documento; también se indica en la portada del documento.
- **Documentos electrónicos:** se indica el nivel de confidencialidad en el pie de página de cada página del documento.
- **Correo electrónico:** se indica el nivel de confidencialidad en el cuerpo del correo electrónico.
- **Información transmitida oralmente:** el nivel de confidencialidad de la información confidencial que se transmite a través de una comunicación cara a cara, por teléfono o por alguna otra vía de comunicación debe ser comunicado antes que la información propiamente dicha.

Manejo de información clasificada

Todas las personas que tienen acceso a información clasificada deben seguir los controles del siguiente cuadro. El área de administración debe activar acciones disciplinarias cada vez que no se cumplan las reglas o si la información se transmite a personas no autorizadas. Cada incidente relacionado con el manejo de información clasificada debe ser reportado de acuerdo con el procedimiento existente.

Uso interno	Confidencial*
<ul style="list-style-type: none">• Sólo las personas autorizadas pueden tener acceso.• Los documentos sólo pueden ser guardados en habitaciones sin acceso público.• El remitente debe verificar cuidadosamente el destinatario.	<ul style="list-style-type: none">• El documento debe ser almacenado en un gabinete con llave.• Los documentos pueden ser transferidos dentro y fuera de la organización solamente en un sobre cerrado.• Si es enviado fuera de la organización, el documento debe ser enviado con acuse de recibo.• Los documentos deben ser retirados inmediatamente de impresoras y máquinas de fax.• Solamente el propietario del documento puede destruirlo y/o eliminarlo.• Los almacenamientos móviles electrónicos deben estar cifrados.• Las conversaciones no deben ser grabadas o enviadas como notas de voz.• La información confidencial de clientes debe ser trasladada a través la consola administrativa utilizada por DSIGNER, S. A. (MSS.develsecurity.com) y cuando no sea posible hacerlo de esta manera, se utilizará el correo electrónico, empaquetando la información mediante archivo ZIP o RAR con contraseña que será transmitida al cliente por otro medio.

Divulgación de información

TIPO DE INFORMACIÓN		
Medio	Interna	Confidencial
Por teléfono	Se debe verificar la ausencia de personal no autorizado a escuchar la información previa a comunicarla.	No se debe utilizar el modo <i>altavoz</i> para esta información. La comunicación debe darse en un área cerrada. Se debe verificar la ausencia de personal no autorizado a escuchar la información previa a comunicarla.
Verbal	En caso de presentaciones o capacitaciones, se debe omitir cualquier referencia que permita identificar el caso, los participantes o información que pueda poner en duda el adecuado tratamiento de la información.	Dicha información solo puede ser tratada dentro de las instalaciones o por medios seguros, sin la compañía de personal no autorizado. La información confidencial, solo puede ser utilizada como parte presentaciones con el dueño de la misma (sin otros involucrados). En estos casos, es responsabilidad del emisor contar con las autorizaciones necesarias del dueño de la información.