

### Manual de Tratamiento de Datos del Sistema de Circuito Cerrado de Televisión ("CCTV")

#### 1. Introducción

El presente manual establece los procedimientos y políticas para el tratamiento de datos personales, capturados por el sistema de Circuito Cerrado de Televisión (en adelante "CCTV") implementado en Empresa Distribuidora Sur S.A. (en adelante EDESUR o la Compañía"), con el propósito de garantizar la seguridad de nuestras instalaciones, proteger a nuestro personal, clientes y activos, así como prevenir pérdidas y actos delictivos.

El presente manual es emitido conforme a los requerimientos exigidos por la Ley Nro. 25.326, respecto de Protección de los Datos y su Decreto reglamentario N° 1558/01 y toda la normativa vigente dictada por la Agencia de Acceso a la Información Pública (A.A.I.P.) en su carácter de Autoridad de Aplicación de la Ley mencionada, en especial con lo previsto en la Disposición 10/2015, la Resolución 38/2024 y otras disposiciones aplicables, siendo su finalidad proteger los datos de los titulares de los mismos.

#### 2. Responsable del Tratamiento de Datos

El responsable del tratamiento de datos en relación con el sistema de CCTV es EDESUR S.A.

La Compañía a su vez ha nombrado un Oficial de Protección de Datos Personales (en adelante "DPO"), a quien puede dirigírsele todas las consultas sobre el ejercicio de los derechos del Titular conforme a lo previsto en el sitio web:

https://www.edesur.com.ar/acerca-de-edesur/legales/proteccion-datos/.

Asimismo, el DPO, ha dispuesto una casilla donde pueden enviarse consultas: <u>dpo.argentina@enel.com</u>.

### 2.1 Tratamiento de datos de CCTV

Las consultas y solicitudes relacionadas con el tratamiento de datos de CCTV o bien las solicitudes relativas a fragmentos de videos obtenidos por medio de las cámaras de videovigilancia, conforme a lo previsto en el artículo 14 de la Ley 25.326, deben dirigirse al Responsable de Seguridad de la Información vía correo electrónico a la casilla: <u>seguinformacion.argentina@enel.com</u> quien deberá tratarlo conforme a lo previsto en el apartado 8 del presente Manual.

#### 3. Finalidad del Tratamiento de Datos

Los datos capturados por el sistema de CCTV se tratan con las siguientes finalidades:

- <u>Seguridad y Prevención de Delitos:</u> Monitoreo para prevenir y detectar actividades delictivas como robos, vandalismo y violaciones de seguridad.
- <u>Control de Acceso</u>: Verificación de acceso autorizado a áreas restringidas y protección de la integridad física de las instalaciones.
- Investigación y Resolución de Incidentes: Utilización de imágenes como evidencia en la investigación y resolución de incidentes como accidentes o conflictos.
- <u>Prevención de Pérdidas</u>: Detección y prevención de pérdidas económicas debido a hurtos internos o externos y mal uso de recursos.

Las imágenes registradas no podrán ser utilizadas para una finalidad distinta o incompatible a las que motivaron su captación.

### 4. Datos Recopilados

El sistema de CCTV puede capturar imágenes, videos y otros datos relacionados con la seguridad de nuestras instalaciones. Esto incluye, pero no se limita a, la grabación de imágenes de personas físicas presentes en áreas monitoreadas, así como información sobre la fecha, hora y duración de las grabaciones.

### 5. Base Legal para el Tratamiento de Datos

El tratamiento de datos de CCTV se basa en el interés legítimo de la empresa en garantizar la seguridad de sus instalaciones y proteger sus activos. Cuando sea necesario, obtendremos el consentimiento de las personas afectadas antes de utilizar sus datos para fines adicionales.

### 6. Seguridad y Confidencialidad

Se implementarán medidas técnicas y organizativas apropiadas para garantizar la seguridad y confidencialidad de los datos capturados por el sistema de CCTV. Esto incluye la encriptación de datos, la restricción de acceso, el monitoreo de accesos y la capacitación del personal en materia de protección de datos.

Por otra parte, el deber de confidencialidad resulta aplicable a todos aquellos colaboradores que tengan acceso a los mismos para el desarrollo de su función o en ocasión de su trabajo. Este deber abarcará también a los colaboradores que puedan realizar el tratamiento en calidad de Encargados.

Tal obligación subsistirá aun después de finalizada su relación con el Responsable del archivo de datos y solo podrá ser relevado del deber de secreto por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública.



Las imágenes obtenidas mediate el sistema de CCTV serán considerados como información confidencial o estrictamente confidencial -según el caso- y deberá ser tratada como tal.

El incumplimiento de los deberes aquí previstos por parte de los colaboradores, dará lugar a las actuaciones correspondientes por parte del Responsable, que pueden tener como consecuencia la imposición de sanciones disciplinarias.

#### 7. Retención de Datos – Plazo de Conservación:

Los datos capturados mediante el sistema de CCTV se conservarán por un período de tiempo de 20 a 30 días, dependiendo de la capacidad de las NVR (grabadoras de video en red), utilizadas para almacenar las imágenes y videos. Esta retención de datos se considera apropiada para cumplir con la finalidad de seguridad y prevención de delitos del sistema de CCTV.

Después del período de retención, los datos serán automáticamente sobrescritos por nuevas grabaciones, a menos que sean necesarios para fines legales, como evidencia en investigaciones o litigios. En tales casos, se implementarán medidas adicionales para preservar la integridad de los datos pertinentes y cumplir con los requisitos legales aplicables.

#### 8. Derechos de los Titulares de Datos:

Se refiere al conjunto de facultades mediante los cuales se garantiza a los Titulares la disposición y control sobre los datos de carácter personal contenidos en bases de datos que reposen en los sistemas de información de las Empresas. Estos derechos se desprenden del derecho fundamental a la protección de datos personales reconocido en el artículo 43 de la Constitución Nacional de la República Argentina.

Las personas cuyos datos son capturados por el sistema de CCTV, en cumplimiento a lo dispuesto en los previsto en los artículos 14 y 15 de la Ley de Protección de Datos Personales (N° 25.326), el Titular del dato tiene derecho de acceso respecto de solicitar fragmentos de videos obtenidos por medio de las cámaras de videovigilancia. Para ejercerlos deberá llenar el presente formulario obrante en el sitio web de la compañía y que obra en el presente como Anexo II. Posteriormente deberá remitirlo en formato PDF y acreditando identidad (sin excepción), debidamente suscripto al Responsable de Seguridad de la Información vía correo electrónico a la siguiente dirección: <u>seguinformacion.argentina@enel.com</u>.

El derecho de acceso sólo podrá ser ejercido en forma gratuita a intervalos no inferiores a seis meses, salvo que se acredite un interés legítimo al efecto (art. 14 inciso 3), ley 25.326.



En caso de que la información enviada se encuentre incompleta, insuficiente o no acredite identidad, un representante de la compañía se pondrá en contacto con el Titular del dato y le requerirá que la complemente o aclare en un plazo máximo de 5 (cinco)días hábiles; de lo contrario, se tendrá por no presentada la solicitud.

Asimismo, si resulta necesaria información o documentación adicional para atender correctamente su solicitud y poder identificar las imágenes solicitadas, le requeriremos que envíe tal información en un término de 5 (cinco) días hábiles; de lo contrario, se tendrá por no presentada la solicitud.

Ahora bien, en el supuesto que el formulario de solicitud se ingrese en una dependencia de EDESUR o bien en una Oficina Comercial, la persona que lo reciba -y teniendo en cuenta lo escueto de los plazos establecidos para responder al solicitante-, deberá remitir el mismo inmediatamente después de haberlo recibido el mismo a la Unidad de Seguridad, mediante correo electrónico a la casilla: seguinformacion.argentina@enel.com para su procedencia, evaluación y tratamiento por el área.

#### 8.1 Plazos de respuesta:

Los plazos de respuesta variaran de acuerdo con el derecho ejercido por el cliente o titular de los datos personales y son los siguientes:

 Derecho de acceso: La Unidad de Seguridad Argentina deberá proporcionar la información solicitada dentro de los diez días corridos de haber sido intimado fehacientemente (art. 14 inciso 2, Ley 25.326).
 Vencido el plazo sin que se satisfaga el pedido, o si evacuado el informe, éste se estimara insuficiente, quedará expedita la acción de protección de los

datos personales o de hábeas data prevista la Ley 25.326.

Téngase presente que, en base a las imágenes ofrecidas al Titular por parte de la Unidad de Seguridad Argentina- éste puede a su vez solicitar la supresión de las imágenes conforme a los previsto en el artículo 16 de la Ley 25.326, teniendo en cuenta las excepciones previstas en el artículo 17 que podrá interponer la Compañía. Ahora bien:

II. Tratándose del ejercicio de los otros derechos como en este caso el de supresión, el plazo máximo de respuesta será de diez (5) días hábiles contados desde el día siguiente de recibido el reclamo del titular de los datos o advertido el error o falsedad. Transcurrido ese tiempo sin respuesta, el afectado quedará habilitado a promover sin más la acción de protección de los datos personales o de hábeas data prevista en la ley 25.326.

La supresión no procederá cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, o cuando existiera obligación legal de conservar los datos.

### 8.2 Plazo de ejercicio de los derechos:

El derecho de acceso puede ser ejercido a intervalos no inferiores a seis meses, salvo que se acredite un interés legítimo al efecto.

#### 8.3 Gratuidad:

El ejercicio de los derechos en todos los casos será gratuito.

#### 8.4 Política de protección de datos personales:

Lo aquí previsto debe complementarse con lo previsto en el artículo 9 y concordantes de la Política N° 1227 "Política de protección de datos personales para las sociedades del Grupo Enel en Argentina"

#### 9. Transferencias Internacionales de Datos

El Responsable no podrá realizar la transmisión y transferencia internacionales de datos capturados por el sistema de CCTV, a menos que sea necesario y se cumplan los requisitos legales aplicables por las autoridades y reglamentaciones pertinentes que determinan los países con nivel adecuado de protección de datos<sup>1</sup>.

En los eventos de transmisión de datos solicitados en ejercicio de un poder de policía del estado, la Empresa adoptará las medidas necesarias para que las personas que tengan acceso a los datos y/o imágenes cumplan con la presente política y con los principios de protección de datos personales establecidos en la Ley.

Lo aquí previsto debe complementarse con lo previsto en el artículo 4.8 y concordantes de la Política N° 1227, Política de protección de datos personales para las sociedades del Grupo Enel

en Argentina y lo previsto en la Resolución N° 34/2019 de la Agencia de Acceso a la Información Pública y sus modificatorias posteriores.

En vista de lo anterior, cuándo se requiera transmitir y/o transferir Datos Personales a otros países, incluyendo aquellos en los cuales tenga presencia el Grupo Empresarial al que pertenece la Empresa, se debe consultar con el Oficial de Protección de datos (DPO) quien debe dar su conformidad previa a realizar la transferencia.

### 10. Modificaciones y Actualizaciones

Este manual se revisará y actualizará periódicamente para garantizar su conformidad con cualquier cambio en la normativa de protección de datos o en los procedimientos internos de la empresa.

<sup>&</sup>lt;sup>1</sup> Se entiende que un país ofrece un nivel adecuado de protección de datos cuando cumpla con los estándares fijados por la Agencia de Acceso a la Información Púbica y a lo establecido en la Política de Protección de datos de Argentina N° 1227, la Resolución N° 34/2019 de la AAIP y sus modificatorias.



Este manual forma parte integral de las políticas de protección de datos de la empresa y debe ser seguido por todo el personal involucrado en el tratamiento de datos capturados por el sistema de CCTV.



#### Anexo I

### Manual de USO del Circuito Cerrado de Televisión ("CCTV")

#### Información General

SmartPSS Lite es un software cliente desarrollado para soluciones pequeñas y medianas. Puede descargar varias soluciones según sea necesario. Este manual presenta las funciones y operaciones generales.

#### Instalación e inicio de sesión

#### Instalación:

Póngase en contacto con el soporte técnico o descargue ToolBox para obtener SmartPSS Lite. Si obtiene el paquete de software de SmartPSS Lite, instale y ejecute el software de acuerdo con instrucciones de la página.

#### Inicialización:

Inicialice SmartPSS Lite cuando inicie sesión por primera vez, incluida la configuración de una contraseña para iniciar sesión y preguntas de seguridad para restablecer la contraseña.

Para la configuración de la contraseña se tendrán en cuenta los siguientes parámetros:

- La contraseña debe constar de 8 a 32 caracteres que no estén en blanco y contener al menos dos tipos de caracteres entre mayúsculas, minúsculas, números y caracteres especiales (excluyendo ' "; : &).
- Establezca una contraseña de alto nivel de seguridad de acuerdo con la solicitud de seguridad de la contraseña.

#### Restablecimiento de contraseña:

Puede reestablecer la contraseña respondiendo las preguntas de seguridad previamente configuradas.



- 1. Pestaña de Función: Muestra la página de inicio de forma predeterminada.
- 2. Sonido de alarma: Se puede activar y desactivar el sonido.
- 3. Gestión de usuario: Se puede cambiar de usuario o verificar el usuario que está conectado en ese momento.
- 4. Configuración del sistema: Configure la configuración básica, la configuración de monitoreo y otros parámetros.
- 5. Estado del sistema: Se puede visualizar el estado del CPU y la RAM. Si el uso del CPU es elevado el icono se vuelve rojo.
- 6. Módulo de funciones: Nos dirige a la página de funciones.
- 7. Manual de usuario: Nos dirige al manual de usuario.
- 8. Gestión: Se puede agregar, eliminara o modificar dispositivos. Se puede realizar configuración de forma remota, modificar IP, etc.
- 9. Módulo de solución: Se puede seleccionar la solución necesaria.

#### Configuración del sistema:

🗹 Auto check time	Every day 8:00 🗘 or	Che	eck Time
Auto Start			
Language	English	٠	
Log save time	30		Days Active after Restart
Date Format	yyyy/MM/dd	۳	
Time Format	24-H	•	
Network Ability	High	۳	
Skin	Grayish White	•	Active after Restart
Minimum Behaviour	Show Floating Window		
Initial Page	Home	•	
Close Prompt	Minimize the window to the s	v	Don't show again

- Momento: Habilite la hora de verificación automática todos los dias y configure la hora de verificación para que los dispositivos verifiquen la hora automáticamente en el momento establecido.
- Autoencendido: La plataforma se inicia automáticamente después de encender la computadora.
- Idioma: Muestra el idioma que se activa después del reinicio.
- Registrar tiempo de ahorro: Configure la hora par guardar el registro y luego se guardarán los registros desde hoy hasta la hora establecida. Esta función se activa después del reinicio.
- Formato de datos: Seleccione el formato de visualización de datos.
- Formato de tiempo: Seleccione el formato de visualización de la hora.
- Capacidad de la red: Seleccione la capacidad de la red según la condición de la red.
- Skin: Se puede seleccionar el color de la interfaz luego del reinicio.
- Página principal: Seleccione la pestaña de función que se abre de forma predeterminada cuando se inicia la plataforma.
- Cerrar mensaje: Aparecerá un mensaje automáticamente cuando se cierre la plataforma.

#### **Ruta local:**

Se puede establecer la ruta donde se guardarán las imágenes y los videos.

#### Gestión de datos:

Se puede extraer periódicamente los datos de asistencia de los dispositivos y borrar periódicamente los datos, imágenes y videos guardados en la computadora.

#### Copia de seguridad y restauración:

La plataforma admite realizar copias de seguridad de forma automática y manual.

d Extraction of Access Control Records		
]+		
30	Days	
30	Days	
	d Extraction of Access Control Records ] + 30	d Extraction of Access Control Records ] + 30 Days

- Extracción de registro con regularidad: La plataforma extrae automáticamente registros e imágenes de control de acceso y asistencia según lo establecido.
- Extracción programada: Se puede configurar el tiempo de extracción regular como todos los dias, puede seleccionar cinco puntos de tiempo.
- Extracción automática: Habilite la función de extracción automáticamente y luego la plataforma extraerá automáticamente registros de asistencia o los registros de control de acceso.
- Proporción de sobreescritura: Habilite la función de proporción de sobreescritura y luego configure la proporción. Cuando el disco este lleno, el sistema sobrescribirá automáticamente las imágenes y videos más antiguos según la proporción.
- Borrar datos: Configure el tiempo de guardado de bases de datos, imágenes y videos de acuerdo con los requisitos reales. La plataforma borra automáticamente los datos y las imágenes que superan el tiempo de ahorro.

#### Gestión de dispositivos

#### Agregar dispositivo:

Existen varios métodos para agregar un dispositivo. Se puede seleccionar el método adecuado según la situación, como la dirección IP, el segmento de red, etc.

#### Agregar dispositivo mediante búsqueda automática:

La recomendación es agregar dispositivos mediante búsqueda automática cuando necesite agregar dispositivos en lotes dentro del mismo segmento de red o cuando el segmento de red está claro pero la dirección IP del dispositivo no está clara.

- Paso 1: Haga clic en Búsqueda automática en la página Administrador de dispositivos.
- Paso 2: Configure el rango del segmento de red y luego haga clic en Buscar.
- Paso 3 Haga clic en los dispositivos necesarios y luego haga clic en Agregar.



• Paso 4 Ingrese el nombre de usuario y la contraseña de inicio de sesión y luego haga clic en Aceptar para confirmar.

#### Agregar dispositivo manualmente:

Le recomendamos agregar dispositivos manualmente cuando necesite agregar un solo dispositivo con cierta dirección IP o nombre de dominio

- Paso 1: Seleccione Agregar en la página Administrador de dispositivos.
- Paso 2 Configure los parámetros del dispositivo. Agregar dispositivos a través de IP-

dd Device		×
Device Name:	Method to	add:
* Device	IP	•
IP:	Port:	
*	* 37777	
User Name:	Password:	
* admin	* •••••	

 Paso 3: Haga clic en Agregar para agregar el dispositivo y luego cierre la página Agregar dispositivo, o haga clic en Agregar y Continúe agregando el dispositivo y permanezca en la página Agregar dispositivo para que pueda agregar otro dispositivo cómodamente.

#### Eliminación del dispositivo:

- Paso 1: Seleccione Administrador de dispositivos en la página de inicio.
- Paso 2 Seleccione el dispositivo que ya no necesita y luego haga clic en Eliminar o lado del dispositivo.
- Paso 3 (Opcional) seleccione Al mismo tiempo, elimine la instantánea y el video del dispositivo si no necesita esas instantáneas y videos; de lo contrario, no lo seleccione.



• Paso 4 Haga clic en Aceptar.

#### Dispositivo de edición

#### Edición de información del dispositivo:

Puede modificar la información del dispositivo agregado, como el nombre, el nombre de usuario de inicio de sesión y la contraseña

- Paso 1: Seleccione Administrador de dispositivos en la página de inicio.
- Paso 2: Haga clic en el lápiz del lado derecho del dispositivo seleccionado o haga doble clic en el dispositivo en el dispositivo lista.
- Paso 3 Edite la información del dispositivo
- Paso 4 Haga clic en Guardar.

#### Configuración del dispositivo:

Para algunos dispositivos de control de acceso, puede realizar configuraciones, incluida la configuración de hora, actualización de firmware, reinicio del dispositivo, extracción de personal y extracción de registros de asistencia.

#### Procedimiento:

• Paso 1: Seleccione Administrador de dispositivos y luego haga clic en el icono de configuración.

No.	Name 🔺	1P	Device Type	De	evice Model	Port	Channel Numbe	Online Status	SN	Operation
1	10010-001	-112.01.001	Access Standald	ine As	RIR214Y-V3	37777	0/0/2/2	<ul> <li>Online</li> </ul>	1.000-0.0000000000000000000000000000000	0000
	Time Softin	a.c.				~				
	Time Seturi	ys				^				
	Date F	Format yyyy-MM-dd	*							
	Time F	Format 24-H	*							
	Time	e Zone GMT+08:00	•							
	System	n Time 2022-04-14	\$ 10:55:24	¢	Sync PC					
	DST E	nable								
	Star	rt Time 🔹	Last Wee 🔻	Thursday 🕶	00:00	\$				
	En	d Time 🔹	Last Wee •	Thursday •	00:00	\$				
	NTP	Server 255.255.255	.255							
		Port 65535	(1-6553	(5)						
	Update	Period 65535	Min(0-6	5535)						
				Sava	Cance	ol				
				Save	Cano	-				

#### Consulta de registro:

Puede consultar eventos de alarma, registros de clientes y registros de dispositivos.

- Paso 1 Seleccione Consulta de registro.
- Paso 2 Seleccione el tipo de registro y la hora del registro y luego ingrese las palabras clave si es necesario.



- Paso 3 Haga clic en Buscar.
- Paso 4 (opcional) Haga clic en Exportar para exportar registros al dispositivo local.

Lap Type:	1 Equi						
System Log *	144	Tite 1	UserName .	Elevel Type	DeviceTrans	Chaire Name	Kenada
Al •	- 10 L	2029-84-00 18 04:00	22	University			
Time	2	2029-04-26 19 83:31	22	Usercedar			
64/30 00:00 04/30 23:53	3	2019-01-30 10:30:22	3.2	Unstages			
Key work:		2029-04-30 14 30:04	1	UnirLoge			
	8	2009-84-00 18:29:43	atmid 1	UnterLagen			
-	. 4	2019-04-16 16:25:22	ettie	UserLogod			
Papo.	1	20/9-04-30 18:22:51	10718	tawtage			
	8	2029-04-30 16:21.47	42709	UserLepad			
		2020-34-30 1152/23	atria	Linetage			
	-	2009-04-36 11 44 63	1010	GeerLegent			
		2026-04-30 11 33 (98	40%	UserLeph			
	12	2029-04-32-08-49-01	atrois	UserLapout			
	18	2029-0-00 10 44 42	42101	Unitaria			

#### **Configuración de Eventos:**

Al configurar el evento, puede establecer vínculos de eventos, como sonido de alarma, envío de correo electrónico y vínculos de alarma.

• Configurar enlaces de alarma externos conectados a los controladores de acceso (como alarma de humo), cámaras y dispositivos de almacenamiento.

• Diferentes dispositivos admiten diferentes enlaces de alarma y la página real puede variar dependiendo de diferentes dispositivos.

• Configurar enlaces de eventos del controlador de acceso. (Evento de alarma, Evento anormal, Evento normal)

#### Centro de Eventos Introducción a la página:



- 1. Estadísticas del evento. Eventos totales/ tasa de procesamiento, muestra una grafico circular del total de eventos y la tasa de procesamiento. Tendencias de eventos de los últimos 7 dias.
- 2. Ver video en vivo: Vista previa del video del canal configurado.



• 3. Eventos en Tiempo real: Ver eventos de alarma en tiempo real. Puede buscar información de eventos según tipos de alarmas y dispositivos.

#### Configuración de visualización de video en directo:

Configure canales de video para visualización en vivo y capture imágenes, videos y charlas en video del canal.

- Paso 1: Haga click en la parte superior izquierda para seleccionar el número de pantalla en la página del Centro de eventos.
- Paso 2: Haga clic derecho en la pantalla, haga clic en Tipo de transmisión y luego seleccione el canal de video que desee para ver en vivo.
- Paso 3 Haga clic en Configuración y luego seleccione la configuración según las necesidades reales.



#### Formulario de Solicitud Fragmento de Video

(Solicitud de información de datos personales contenidos en el Banco de datos (Ley Nro. 25326 Art. 14)

#### EMPRESA DISTRIBUIDORA SUR S.A.

Domicilio social: San José 140, Ciudad Autónoma de Buenos Aires -(C1076AAD).

En cumplimiento a lo dispuesto en los artículos 14, 15, 16 y 17 de la Ley de Protección de Datos Personales (N° 25.326), usted tiene derecho de acceso, es decir, podrá solicitar fragmentos de videos obtenidos por medio de las cámaras de videovigilancia captadas mediante el Circuito Cerrado de Televisión (en adelante "CCTV") implementado en Empresa Distribuidora Sur S.A., con el propósito de garantizar la seguridad de nuestras instalaciones, proteger a nuestro personal, clientes y activos, así como prevenir pérdidas y actos delictivos.

Para ejercer este derecho deberá llenar el presente formulario y remitirlo en formato PDF y acreditando identidad (sin excepción), debidamente suscripto al Responsable de Seguridad de la Información vía correo electrónico a la siguiente dirección: seguinformacion.argentina@enel.com.

En caso que la información enviada se encuentre incompleta, insuficiente o no acredite identidad, un representante de la compañía se pondrá en contacto con el Titular del dato y le requerirá que la complemente o aclare en un plazo máximo de 5 días hábiles; de lo contrario, se tendrá por no presentada la solicitud.

Asimismo, si resulta necesaria información o documentación adicional para atender su solicitud, le requeriremos que envíe tal información en un término de 5 días hábiles; de lo contrario, se tendrá por no presentada la solicitud.

١.	DATOS DEL SOLICITANTE (TITULAR DE LOS DATOS PERSONALES) Y/O REPRESENTANTE LEGAL O APODERADO (en
	caso de tratarse de personas de existencia ideal):

CUIT: Número:

Código Postal:

Piso:

Dpto:

Nombre y Apellido / Razón Social de quien solicita el fragmento del video:

Representante Legal y/o Apoderado (en su caso): DNI / CI / LE / Pasaporte:

CUIL:

Domicilio:

Localidad:

Número de Cliente:

Teléfono de contacto: Correo electrónico de contacto:

En caso de haberse producido la toma de imágenes en alguna de las dependencias de EDESUR u Oficinas Comerciales, los efectos de la mejor identificación del registro se servirá indicar:

• Dirección completa del establecimiento/Oficina Comercial en donde se presentó

Información solicitada, "Fragmento de video" correspondiente a:

•	Fecha (DD/MM/AAA	echa (DD/MM/AAAA) de presentación en el establecimiento: _		_/	
•	Hora desde:	Minutos desde:	(am_	_/pm)	

Hora hasta: \_\_\_\_\_ Minutos hasta: \_\_\_\_\_ (am\_/pm\_)

•	Breve descripción de vestimenta del día de presentación en el establecimiento y toda aquella información que
	permita identificar o ubicar la grabación solicitada y/o el fragmento. (esta información es fundamental ya que
	permite establecer patrón de búsqueda):

• Asimismo, se servirá indicar las razones que justifiquen la solicitud efectuac	da:
Por medio de este formulario, manifiesto el deseo de ejercer el derecho de acceso, del a Ley Nro. 25326, y los artículos 14 y 15 de la Reglamentación de la Ley Nro. 2532 1558/01.	de conformidad con el artículo 14 26 aprobada por el Decreto Nro.
A completar por la Mesa de Entradas/Recepción del Establecimient	to/Oficina Comercial
Establecimiento/oficina comercial:	Fecha (DD/MM/AAAA):
//	
Recibió:	(*)
*) Téngase presente que de ser recibido en la Oficina Comercial este formulario deberá se naberla recibido a la Unidad de Seguridad, mediante correo electrónico a la casilla: seguinf	r remitida inmediatamente después de formacion.argentina@enel.com para su
evaluación y tratamiento.	