RES - 2024 - 152 - CS # UNNE
Sesión 06/03/2024

VISTO:

El Expte. Nº 01-2023-06788, por el cual el Secretario General Legal y Técnico eleva el proyecto de Reglamento sobre Video Vigilancia en el ámbito de la Universidad Nacional del Nordeste; y

CONSIDERANDO:

Que la propuesta de referencia busca incrementar el nivel de protección de la comunidad universitaria, la prevención de faltas, delitos y preservación de la seguridad de los bienes de propiedad, como así también los accidentes relacionados con la salud, entre otros;

Que a fs. 02/09, obra proyecto de Reglamento con su anexo y a fs. 10 se adjunta imagen de aviso de zona video vigilada;

Que el proyecto tiene en cuenta las previsiones de la Ley 25.326, de protección de datos personales, y su uso va a ser válido en la medida en que su necesidad se encuentre justificada, se informe a la comunidad en forma previa a su colocación y no se utilice en sectores privados (como baños, vestuarios, lugares de descanso o en ámbitos en que se desarrollen actividades gremiales);

Que la propuesta queda comprendida en las competencias reglamentarias que la Universidad ostenta en el marco de la autonomía y autarquía universitaria consagrada en el art. 75 inc. 19 de la Constitución Nacional y receptada legislativamente en los art. 29º y 59º de la ley 24.521 y estatutariamente en el art. 3º del Estatuto Universitario y, además, se adecúa al gobierno digital, uno de los ejes centrales del Plan de Acción institucional 2022-2026. Igualmente, el proyecto se enmarca dentro de los objetivos prioritarios de la Secretaría General Legal y Técnica previstos para la gestión 2022-2026 relativa a la innovación estratégica, modernización y transparencia de la gestión institucional y en consonancia con el Plan Estratégico de Desarrollo Institucional (PEDI 2020-2030, Eje 3 de Fortalecimiento e Innovación del Desarrollo institucional, cuyos objetivos son "modernizar la gestión institucional, promover un Sistema de Innovación Estratégica y vigorizar los principios de una organización transparente y sostenible";

Que obra Dictamen de la Dirección General de Asuntos Jurídicos que expresa: "…en relación a la observación formulada a fs. 13/14 por la Auditoria Legal de la

RES - 2024 - 152 - CS # UNNE
Sesión 06/03/2024

Unidad de Auditoría Interna en orden a la instalación de Cámara con sonido y con independencia de hacer notar que la objeción manifestada en la opinión citada no reposa en normativa alguna que fuera individualizada por los auditores, sin embargo la misma no se compadece con el tenor del proyecto el cual prevé, en su art 4º, como principio general la no instalación de cámaras con sonidos a excepción que la autoridad fundamentadamente justifique la razonabilidad de su uso evitándose especialmente cualquier afectación del derecho a la privacidad. En función de lo señalado, el proyecto aborda la cuestión apropiadamente a partir de los límites que hacen a la razonabilidad de la medida respecto la utilización de las videocámaras, fundadamente y con preservación de las garantías debidas, por lo que no existen objeciones jurídicas al respecto.";

Que el art. 19º del Estatuto de la UNNE establece: "El Consejo Superior tiene las siguientes atribuciones: 1.- La dirección de la Universidad y el desarrollo de funciones normativas generales, de definición de políticas y de control;…";

Que en atención a lo expuesto la Comisión de Interpretación y Reglamento aconseja aprobar el Reglamento sobre Video Vigilancia en el ámbito de la Universidad Nacional del Nordeste;

Lo aprobado en sesión de fecha 6 de marzo de 2024;

EL CONSEJO SUPERIOR
DE LA UNIVERSIDAD NACIONAL DEL NORDESTE
RESUELVE:

ARTICULO 1º- Aprobar el Reglamento sobre Video Vigilancia en el ámbito de la Universidad Nacional del Nordeste, cuyo texto se agrega como parte integrante de la presente.

ARTICULO 2º- Regístrese, comuníquese y archívese.

PROF. PATRICIA B. DEMUTH MERCADO
SEC. GRAL. ACADÉMICA

PROF. GERARDO OMAR LARROZA
RECTOR

# REGLAMENTO SOBRE VIDEO VIGILANCIA

## INTRODUCCIÓN

La necesidad de incorporación en el ámbito de la Universidad de un sistema de video vigilancia, se ve fundada en la intención de incrementar el nivel de protección de su comunidad, la prevención de faltas, delitos y preservación de la seguridad de los bienes de propiedad de la Universidad, como así también los accidentes relacionados con la salud, alertas de tipo social, entre otros. -

Desde nuestra perspectiva el uso de cámaras de seguridad va a ser válido en la medida en que la necesidad de su colocación se encuentre justificada, se informe a la comunidad universitaria en forma previa a su colocación y no se las utilicen en baños, vestuarios, lugares de descanso o donde se realicen las actividades gremiales. -

La licitud de las cámaras de seguridad va a depender de las razones que se esgriman para su colocación. Por ejemplo, serán válidas si se las utiliza para garantizar la seguridad de las instalaciones, lo justifica el tipo de actividad o por la seguridad de las personas. En tal sentido, la ley 25.326, de Protección de Datos Personales, estipula la necesidad de contar con el consentimiento del titular de la información a fin de obtener la legitimidad para su obtención, a menos que ésta derive de una relación contractual o profesional y siempre que resulte necesaria para su desarrollo o cumplimiento. -

Este tipo de control se debe implementar siempre de forma razonable, equilibrada y de buena fe de modo de causar el menor daño posible a la intimidad de las personas titulares de la información. -

## MARCO DE ACTUACION. PRINCIPIOS DE LEGALIDAD Y DERECHO DE PRIVACIDAD

El derecho a la supervisión, monitoreo y uso de videocámaras de seguridad se limita exclusivamente a las autoridades y personal designado, que resultan responsables en términos funcionales y normativos del sistema que supervisan, debiendo garantizar un funcionamiento sustentado en principios de legalidad y respeto de la privacidad de las personas (art. 19 de la Constitución Nacional, art. 5 Declaración Americana de los Derechos y Deberes del Hombre, art. 12
Declaración Universal de Derechos Humanos, art. 11, incs. 2 y 3, de la Convención Americana de
Derechos Humanos – Pacto de San José de Costa Rica -, Normas Supranacionales de Jerarquía
Constitucional en los términos del art. 75, inc. 22, de la Constitución Nacional). -

Hay que tener presente que la Dirección Nacional de Protección de Datos Personales – en el entendimiento que la imagen de una persona debe ser considerada un dato personal en tanto la persona pueda ser identificada o identificable a través de esa imagen – dictó

en febrero del año 2015 la Disposición Nº 10/2015. Esta Disposición contiene una serie de principios que se aplican a los sistemas de video vigilancia. Estos principios son:

**CONSENTIMIENTO:** La normativa exige el consentimiento previo e informado del titular del dato; la información al titular del dato de la captación de la imagen puede realizarse a través de un cartel que indique que la zona cuenta con cámaras de video vigilancia pero sin necesidad que se establezca su ubicación específica, por otro lado, no se requerirá el consentimiento bajo tres excepciones: cuando la recolección del dato la realiza la Institución ya sea un espacio público o privado, cuando quién recolecta el dato sea el Estado en ejercicio de sus funciones (respetando el art. 6 de la ley 25.326) y, por último, cuando la recolección del dato se hace en un espacio de uso propio.-

**RESPETO DE LA FINALIDAD:** Las imágenes captadas no podrán utilizarse con un fin distinto o diferente de los que motivaron su captación. Por ejemplo, si las imágenes se obtuvieron con motivo de seguridad no podría utilizarse después para otros fines. -

**CALIDAD DEL DATO:** Esto es que las imágenes obtenidas deben tener relación con la finalidad para la que fueron tomadas debiendo eliminarse todas aquellas imágenes que puedan vulnerar los derechos de las personas. Deberá evitarse especialmente entre las razones de seguridad que motivan la toma de las imágenes y la intromisión efectuada en la intimidad de las personas. -

**SEGURIDAD Y CONFIDENCIALIDAD:** El responsable de las bases de datos deberá garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado a su vez el responsable de los datos deberá garantizar la confidencialidad de los datos recabados. -

**EJERCICIO DE LOS DERECHOS DEL TITULAR DEL DATO:** Garantiza a los titulares de datos los derechos de supresión y rectificación. -

**INSCRIPCIÓN:** En caso que la Institución grave y conserve las imágenes obtenidas a través de la cámara de vigilancia debe registrar dicha base de dato en el Registro Nacional de Bases de Datos dependiente de la DNPDP (**D**irección **N**acional de **P**rotección de **D**atos **P**ersonales). -

**MANUAL DE TRATAMIENTO DE DATOS:** Los responsables de las actividades de recolección y posterior tratamiento de imágenes digitales de personal con fines de seguridad deberán contar con un manual o política de tratamiento de datos personales y privacidad. -

En conclusión, la utilización de cámaras de seguridad en todo el ámbito universitario es válida en la medida en que su utilización se encuentre debidamente justificada en los hechos (por razones de seguridad), y se informe en forma previa a su colocación, y no se las utilicen en baños, vestuarios, lugares de descanso o donde se realicen actividades

gremiales y se cumplan con los requisitos establecidos por la Disposición Nº 10/2015 de la Dirección Nacional de Protección de Datos Personales. -

Las recomendaciones hacen hincapié en la Ley 25.326 de Protección de Datos Personales y en el
Convenio 108+ para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, aprobado en nuestro país por la Ley 27.483. (Siendo el único instrumento multilateral jurídicamente vinculante adoptado en el ámbito de la protección de datos personales y vida privada). -

**¿POR QUÉ HAY QUE REGISTRAR BASES DE DATOS DE VIDEOVIGILANCIA?**

Según lo establecido en la Disposición 10/2015, "… una imagen o registro fílmico constituyen, a los efectos de la Ley N° 25.326, un dato de carácter personal, en tanto que una persona pueda ser determinada o determinable...".
Una imagen con formato digital permite su tratamiento a través de sistemas informáticos y conformar un sistema organizado de fácil consulta.

La base de datos de videovigilancia debe ser declarada (al igual que se declaran, por ejemplo, los empleados, clientes y proveedores). En ese momento, al presentar el formulario, debe presentarse también el "manual de tratamiento de datos personales" cuyos requisitos mínimos están indicados en el artículo 7° de la disposición 10/2015.

Por tanto, el manual de videovigilancia debe contener al menos la siguiente información:

- Forma de la recolección.
- Referencia de los lugares, fechas y horarios en los que se prevé que operarán.
- Plazo de conservación de los datos.
- Mecanismos técnicos de seguridad y confidencialidad previstos.
- Medidas dispuestas para el cumplimiento de los derechos del titular del dato contemplados en los artículos 14, 15 y 16 de la Ley 25326.
- Los argumentos que justifiquen la toma de fotografías para el ingreso al predio, en caso de disponerse dicha medida de seguridad.

A su vez, en el caso de actividades de videovigilancia se debe informar previamente al público:

- La existencia de cámaras de seguridad (sin que sea necesario precisar su ubicación puntual).
- Los fines para los que se captan las imágenes.
- Los datos de contacto del responsable de la base de datos, para que las personas puedan ejercer sus derechos como titulares de datos personales.

## DEFINICIONES

A los efectos del presente Reglamento, se entiende por:

a. Sistema de video vigilancia: circuito cerrado de cámara/videocámara u otro tipo de dispositivo electrónico, digital, óptico o electro-óptico que permite captar y enviar imágenes con o sin sonido desde la zona de vigilada a puestos de visualización, monitoreo y/o tratamiento de datos con el objetivo de controlar y proteger un espacio definido. Está compuesto por medios de captación y transmisión de imágenes, equipos para la visualización y monitoreo de imágenes en forma local o remota, equipos para la grabación y almacenamiento de imágenes, equipos de conmutación, medios de control de videos, equipos de alarmas, y todo tipo de complemento necesario para su normal funcionamiento.
b. Cámara/Videocámara: dispositivo que permite la captura de imágenes, con o sin sonido, que pueden ser reproducidas y/o almacenadas por un aparato determinado.
c. Cámara fija: cámara que no posee movimiento de rotación automáticos.
d. Cámara móvil (Domo o PTZ): cámara que puede rotar alrededor de DOS (2) ejes, uno horizontal y otro vertical, así como acercarse o alejarse (zoom) para enfocar un área u objeto específico de forma manual o automática.
e. Datos personales: información de cualquier tipo (incluso imágenes) referida a persona físicas o jurídicas, públicas o privadas.
f. Responsable de archivo, registro, base o banco de imágenes: personal física o jurídica, pública o privada, que es titular de un archivo, registro, base y/o banco de imágenes.
g. Archivo, registro, base o banco de imágenes: conjunto organizado de imágenes que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera fuere la modalidad de su obtención, almacenamiento, grabación, acceso y reproducción.
h. Tratamiento de imágenes: operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenamiento. Almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de imágenes con o sin sonido, así como también su reproducción por cualquier medio y/o cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.
i. Almacenamiento de imágenes: archivo generado en los equipos de grabación por las imágenes capturadas. El tiempo de almacenamiento va desde el instante de captura de la imagen hasta su eliminación por parte del propio sistema. -
j. Resguardo de imágenes: acción de extraer determinadas imágenes del archivo, a los efectos de que el propio sistema no las elimine.

# REGLAMENTO DE USO DE VIDEO VIGILANCIA EN LA UNIVERSIDAD

**Artículo 1°. - Objeto.** El presente reglamento regula la utilización por parte de la Universidad de videocámaras para grabar imágenes en el ámbito comprendido por el predio de uso propio y/o su perímetro, así como su posterior tratamiento, estableciendo específicamente el régimen de garantías de los derechos fundamentales y libertades públicas de la comunidad universitaria que habrá de respetarse ineludiblemente en las sucesivas fases de grabación y uso de las imágenes.

**Artículo 2°. - Principios generales para la utilización de videocámaras.** La utilización de videocámaras está regida por el principio de proporcionalidad y razonabilidad, en su doble versión de procedencia y de intervención mínima. La procedencia determina que sólo podrá emplearse la videocámara cuando resulte adecuado, en una situación concreta, para asegurar la convivencia universitaria, la utilización segura de los espacios públicos dentro de su predio, así como para la prevención de faltas e infracciones relacionadas con la seguridad pública. La intervención mínima exige la ponderación en cada caso, entre la finalidad pretendida y la posible afectación por utilización de la videocámara al derecho a la propia imagen, a la intimidad y a la privacidad de las personas, de conformidad con los principios consagrados en nuestra Constitución Nacional. -

**Artículo 3°. - Principios para la disposición de videocámaras.** La instalación de videocámaras por parte de la Universidad será procedente en la medida en que resulten de utilidad concreta a fin de proporcionar información necesaria para adoptar eventuales medidas de seguridad. Las imágenes registradas no podrán ser utilizadas para una finalidad distinta o incompatible a la que motivó su captación. -

**Artículo 4°. - Límites a la utilización de videocámaras.**

a) La información que se recabe debe ser adecuada, pertinente y no excesiva en relación a la finalidad para la que se hubiera obtenido, y por tales motivos deberá cuidarse que las imágenes obtenidas se relacionen estrictamente con los fines perseguidos evitándose mediante esfuerzos razonables la captación de detalles que no sean relevantes para la consecución de los objetivos que justifican la recolección del material fotográfico o fílmico.
b) Deberá evitarse especialmente cualquier afectación del derecho a la privacidad, cuidando de no instalar dispositivos de captación de imágenes en ámbitos inapropiados que no permitan verificar la debida proporcionalidad entre las razones de seguridad que motivan la toma de las imágenes y la intromisión efectuada en la intimidad de las personas.
c) Como norma general no se podrán instalar cámaras con sonido, a excepción de que la autoridad fundadamente justifique la razonabilidad de su uso, evitándose especialmente cualquier afectación del derecho a la privacidad.
d) En el supuesto que en forma accidental se obtuviesen imágenes cuya captación resulte violatoria del presente reglamento, las mismas deberán

ser destruidas inmediatamente por quién tenga la responsabilidad de su custodia. -

**Artículo 5°. - Alcance analógico.** Las referencias a videocámaras contenidas en el presente reglamento, se entenderán hechas a cualquier medio técnico análogo y, en general, a cualquier sistema que permita las grabaciones previstas en este reglamento. -

**Artículo 6°. - Efectos jurídicos.** La captación y almacenamiento de imágenes en los términos previstos en este reglamento, así como las actividades preparatorias, no se considerarán intromisiones ilegítimas en el derecho a la intimidad personal y familiar y a la propia imagen, siempre y cuando no contradigan lo establecido en la Constitución Nacional y la Ley N° 25.326.-

**Artículo 7°. - Comunicación a los (Consejos Directivos o autoridad) de las distintas Unidades Académicas e Institutos para la instalación de videocámaras**. En ocasión de cada instalación de videocámaras, la autoridad de aplicación remitirá un informe preliminar al (Consejo Directivo o autoridad) de dicha instalación. -

El informe deberá precisar el ámbito físico susceptible de ser grabado, el tipo de cámara y sus especificaciones técnicas. -

**Artículo 8°. - Informe (anual) a los Consejos Directivos**. El organismo de implementación, (antes del 31 de marzo), debe presentar un informe de gestión a cada una de los correspondientes Consejos Directivos en el que detalle:

a) La cantidad de cámaras instaladas bajo su jurisdicción precisando la ubicación geográfica de cada dispositivo. -
b) Información referente a la calificación técnica de las personas encargadas de la operación del sistema de captación de imágenes y las medidas adoptadas para garantizar el respeto a las disposiciones legales vigentes. -
c) Las modificaciones técnicas que hubiera en las características de los dispositivos respecto a las descriptas en el informe del (año) anterior. -
d) La justificación de la continuidad de la medida. -

**Artículo 9°. - Utilización de las grabaciones.** La obtención de imágenes según lo establecido en el presente reglamento no tendrá por objetivo la formulación de denuncias judiciales por parte de la autoridad de aplicación. Sin perjuicio de esto, la autoridad de aplicación pondrá la cinta o soporte original de las imágenes en su integridad a disposición judicial con la mayor celeridad posible si fuese solicitado. -

Si la grabación captara hechos que pudieran ser constitutivos de infracciones administrativas, se remitirán al área competente, igualmente de inmediato, para el inicio del oportuno procedimiento administrativo sancionatorio. -

**Artículo 10°. - Límites en la utilización de las grabaciones.** El acceso a toda información obtenida como consecuencia de las grabaciones será restrictivo a aquellos funcionarios que la autoridad individualmente determine, por razón de su función específica. Debiéndose adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

El responsable del tratamiento debe también tomar los recaudos necesarios para garantizar la confidencialidad de dicha información. Esta obligación alcanza a las personas que intervengan en cualquier fase del tratamiento de datos como usuarios o empleados del responsable. Tal obligación subsistirá aun después de finalizada su relación con el titular de la base de datos.
Se prohíbe la cesión o copia de las imágenes salvo en los supuestos previstos en el presente reglamento. Cualquier persona que por razón del ejercicio de sus funciones tenga acceso a las grabaciones deberá observar la debida reserva, confidencialidad y sigilo en relación con las mismas, siéndole de aplicación, en caso contrario, lo dispuesto en la legislación penal y convenios colectivos. Cuando no haya lugar a exigir responsabilidades penales, las infracciones a lo dispuesto en el presente reglamento serán sancionadas con arreglo al régimen disciplinario correspondiente a los infractores (docente o no docente) y, en su defecto, con sujeción al régimen de sanciones en materia de protección de datos de carácter personal. -

**Artículo 11°. - Destrucción de las grabaciones**. Las grabaciones son destruidas una vez transcurridos (120) días corridos desde su captación, mientras que no deberán destruirse las grabaciones que estén relacionadas con infracciones penales o administrativas en materia de seguridad pública, con una investigación policial en curso o con un procedimiento judicial o administrativo abierto. -

**Artículo 12°. - Autoridad de aplicación**. La autoridad (Consejo Directivo o Consejo Superior o Decanos y/o Rector) determinará el área (TIC) que se desempeñará como autoridad de aplicación, el que tendrá a su cargo la custodia de las imágenes obtenidas y la responsabilidad sobre su ulterior destino, incluida su inutilización o destrucción. -

**Artículo 13°. - Registro**. (Manual de tratamiento de datos). Los responsables de las actividades de recolección y posterior tratamiento de imágenes digitales de personas con fines de seguridad deberán contar con un manual o política de tratamiento de datos personales y privacidad, que ponga en práctica las condiciones de licitud previstas en la Ley N° 25.326 para el caso concreto. Éste deberá contener al menos la siguiente información: forma de la recolección; referencia de los lugares, fechas y horarios en los que se prevé que operarán; plazo de conservación de los datos; mecanismos técnicos de seguridad y confidencialidad previstos; medidas dispuestas para el cumplimiento de los derechos del titular del dato contemplados en los artículos 14, 15 y 16 de la Ley N° 25.326 y los argumentos que justifiquen la toma de fotografías para el ingreso al predio, en caso de disponerse dicha medida de seguridad.

**Artículo 14°. - Garantías**.

a) La existencia de videocámaras, así como la autoridad responsable de su aplicación, deben informarse mediante un cartel indicativo de manera clara y permanente. -
b) Toda persona interesada podrá ejercer, ante la autoridad o en su defecto ante autoridad judicial competente, los derechos de acceso y cancelación de las grabaciones en que razonablemente considere que figura, acreditando los extremos alegados. -
c) La autoridad de aplicación deberá publicar en la página web de la Universidad los puntos en los cuales se instalen videocámaras. -

**ANEXO**

**"Medidas de seguridad recomendadas para el tratamiento y conservación de los Datos Personales en medios informatizados". -**

De modo referencial y con el objetivo de facilitar el cumplimiento de la Ley Nº 25.326 de Protección de los Datos Personales, se establecen las medidas de seguridad recomendada para la administración, planificación, control y mejora continua de la seguridad de la información. -

La Ley Nº 25.326 en su artículo 2º define: **D**atos **P**ersonales (en adelante **DP**) a "Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables". **D**atos **S**ensibles (en adelante **DS**) a "Datos personales que revelan origen racial étnico, opiniones políticas, convecciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual".

A – Recolección de datos

Relacionado con los procesos necesarios para asegurar la completitud e integridad de los datos, minimizar los errores e implementar las medidas técnicas con el objeto de asegurar la confidencialidad y limitar el acceso durante la recolección. -

DP

| | | |
|---|---|---|
| A | RECOLECCIÓN DE DATOS | |
| | | |
| A.1. | Integridad | |
| A.1.1. | Asegurar la completitud | Verificar que los campos que componen el formulario de recolección de datos permitan el ingreso completo de los datos requeridos. |
| A.1.2. | Minimizar los errores de ingreso | Indicar en forma clara y concreta el tipo de información a ingresar y el formato de la misma. |
| A.1.3. | Asegurar la integridad | Verificar la exactitud del dato ingresado en caso de que el tipo de registro lo permita (ej. Fecha formato: DD/MM/AAAA). |
| A.2. | Confidencialidad | |

| | | |
|---|---|---|
| A.2.1. | Asegurar la confidencialidad durante el proceso de recolección | Cifrar la comunicación cliente-servidor durante la recolección. |
| A.2.2. | Limitar el acceso a la recolección de los datos | Limitar cache del formulario en el cliente únicamente al momento de la carga de datos. |
| | | Limitar la carga de datos en el cliente a una sola sesión de usuario. |
| A.2.3. | Limitar el acceso no autorizado durante la recopilación | Utilizar certificados digitales seguros y validados por entidad autorizada. |

DS

| | | |
|---|---|---|
| A.2.3. | Limitar el acceso no autorizado durante la recopilación | Cifrar la comunicación durante el traslado desde el servidor de aplicación hacia la base de datos. |

B – Control de acceso

Relacionado con la implementación de medidas de seguridad, mecanismos de autenticación, segregación de roles y funciones, y demás características del acceso a los sistemas para la protección de la identidad y la privacidad. -

DP

| | | |
|---|---|---|
| B | CONTROL DE ACCESO | |
| | | |
| B.1. | Identificación de activos | |
| B.1.1. | Identificar los activos | Elaborar un inventario de activos informáticos que almacenen o gestionen datos personales. |
| B.1.2. | Definir responsables y responsabilidades | Definir propietarios de activos informáticos que almacenen o gestionen datos personales. |
| | | Notificar a los propietarios de activos informáticos que almacenen o gestionen datos personales. |
| | | Especificar a los propietarios de activos informáticos autorizaciones de acceso (tipo de acceso y validez). |
| B.1.3. | Verificar la aplicación de controles | Elaborar un procedimiento de actualización periódica del inventario. |

| | | |
|---|---|---|
| | | Elaborar un procedimiento de verificación de autorizaciones. |
| | | Elaborar un procedimiento para nuevos activos informáticos, definiendo responsable asignado y autorizaciones. |
| B.2. | Acceso a los datos | |
| B.2.1. | Gestionar los accesos a los sistemas | Elaborar un documento interno que defina los controles de acceso a cada sistema. |
| | | Definir e identificar aquellos usuarios que por su rol de superusuarios (administradores) puedan evadir los controles de acceso definidos para el propietario. |
| | | Controlar y monitorear a los superusuarios (registrando accesos y actividad) |
| B.2.2. | Asignar los permisos | Disponer de una notificación concreta y formal de las responsabilidades asumidas por cada usuario que acceda internamente a los sistemas (notificación fehaciente). |
| B.2.3. | Verificar la identificación y autorización | Disponer de un sistema que identifique inequívocamente a cada usuario. |
| | | Establecer una política de contraseñas seguras. |
| | | Disponer de un registro de acceso a los sistemas. |
| | | Disponer de un registro de uso de los sistemas. |
| | | Disponer de un procedimiento de Alta, Baja, Modificación de usuarios. |
| | | Limitar el acceso de los superusuarios a los datos personales o establecer un seguimiento de su actividad. |
| | | Asegurar la implementación de la política de contraseñas seguras en todos los sistemas. |
| | | Evitar el uso de usuarios genéricos. |
| B.2.4. | Controlar el acceso físico al centro de datos | Disponer de un control de acceso físico al centro de datos. |
| | | Elaborar un procedimiento de control de acceso físico. |
| | | Disponer de un registro de los accesos físicos (identificando día, hora. Ingresantes y motivo). |
| | | Asegurar el sistema de registro del control de acceso. |

| | | |
|---|---|---|
| B.2.5. | Monitorear la actividad | Definir un procedimiento de limpieza de cuentas inactivas con privilegios de acceso. |

DS

| | | |
|---|---|---|
| B.2.5. | Monitorear la actividad | Limitar el acceso interno a los sistemas con un mismo usuario a una sola sesión concurrente. |
| | | Monitorear y controlar las cuentas de usuario que dispongan de privilegios especiales, identificarlas en forma diferencial. |
| | | Identificar y analizar intentos de autenticación fallidos. |

C- Control de cambios

Relacionado con la implementación de los procesos para identificar fehacientemente a toda persona que acceda a realizar cambios en los entornos productivos que contengan datos personales, garantizando su identificación, autenticación y autorización correspondiente. -

DP

| | | |
|---|---|---|
| D | RESPALDO Y RECUPERACIÓN | |
| | | |
| D.1. | Copias de respaldo y proceso de recuperación | |
| D.1.1. | Asegurar un proceso formal de respaldo y recuperación | Disponer de un procedimiento de resguardo de información donde se identifique:<br>a) Qué tipo de información se resguardará.<br>b) Qué medio físico se utilizará.<br>c) Cantidad de copias de resguardo que se realizaran.<br>d) Periodicidad de las ejecuciones de copias de resguardo.<br>e) Descripción del proceso de la realización de copias de resguardo.<br>f) Tiempo de almacenamiento de copias de resguardo.<br>g) Responsable de la realización de copias de resguardo. |
| | | Definir y verificar procedimiento de pruebas de recuperación. |

| | | |
|---|---|---|
| | | Disponer de un registro de pruebas de recuperación realizadas identificando:<br>a) Tipo de información recuperada.<br>b) Lugar y fecha donde se realizaron las pruebas de recuperación.<br>c) Resultado de las pruebas de recuperación.<br>d) Responsable de la realización de las pruebas de recuperación.<br>e) Personal interviniente en las pruebas de recuperación.<br>f) Notificación al responsable de datos. |
| | | Disponer de un inventario que identifique las copias de seguridad, su ubicación real y el medio físico en donde se encuentran. |
| D.1.2. | Asegurar control de acceso en los medios | Aplicar las medidas de Control de acceso (B) a las copias de resguardo. |
| | | Cifrar las copias de resguardo utilizando herramientas seguras. |
| | | Asegurar los entornos de prueba de recuperación utilizando las mismas medidas de seguridad que un entorno productivo. |
| | | Eliminar en forma segura la información recuperada durante las pruebas una vez verificada su exactitud. |

DS

| | | |
|---|---|---|
| D.1.2. | Asegurar control acceso en los medios | Disponer medidas de protección contra incendios o inundaciones en el sitio de almacenamiento de los medios físicos que contienen las copias de resguardo. |
| | | Almacenar las copias de resguardo en una locación física diferente a la del sistema productivo. |
| | | En caso de traslado de copias de resguardo, disponer de un procedimiento de registro y control de tránsito. |
| | | Asegurar los entornos de prueba de recuperación utilizando las mismas medidas de seguridad que un entorno productivo. |

E – Gestión de vulnerabilidades

Destinado a la implementación de procesos continuos de revisión que permitan identificar, analizar, evaluar y corregir todas las vulnerabilidades posibles de los sistemas informatizados que traten información, aplicando técnicas de control de integridad, registro, trazabilidad y verificación.

DP

| | | |
|---|---|---|
| E | GESTION DE VULNERABILIDADES | |
| | | |
| E.1. | Gestión de vulnerabilidades | |
| E.1.1. | Prevenir incidentes de seguridad desde el diseño | Considerar y analizar las posibles amenazas a la que estarán expuestos los sistemas informatizados. |
| | | Disponer de un mapa conceptual que permita conocer el flujo de la información entre los distintos sistemas informatizados. |
| | | Establecer un documento de seguridad que indique las medidas de seguridad adoptadas para los sistemas de información. |
| E.1.2. | Asegurar una protección adecuada | Establecer controles de seguridad para las aplicaciones que procesen datos personales, entre ellas:<br>a) Segmentación de roles y perfiles.<br>b) Autenticación segura.<br>c) Gestión de sesiones (cumpliendo apartado de control de acceso (B)<br>d) Gestión de mensajes de error en aplicaciones.<br>e) Implementar reglas y controles de seguridad en los servidores que estén conectados a una red externa y almacenen o gestionen datos personales, programando alertas ante posibles ataques.<br>f) Segmentar en forma física o lógica la red de la entidad, separando las áreas públicas de las privadas.<br>g) Separar los ambientes de Producción, QA, Prueba y Desarrollo.<br>h) Implementar controles para la prevención de virus informáticos en los servidores |

| | | |
|---|---|---|
| | | que almacenen o gestionen datos personales.<br>i) Establecer y ejecutar un procedimiento de actualización periódica de software/hardware de todo el equipamiento.<br>j) Definir a una persona responsable del cumplimiento de las medidas de seguridad. |
| E.1.3. | Detectar posibles incidentes seguridad | Disponer de un sistema de auditoria de incidentes implementando un sistema de registro que permita realizar un seguimiento ante eventos o acciones de un posible incidente (sistema de logs). |
| | | Sincronizar todos los servidores/equipamiento con un servidor de horario público para asegurar una correcta trazabilidad en caso de realizar una auditoría. |
| | | Implementar un proceso de denuncia que permita que los usuarios alerten eventos de seguridad. |
| | | Disponer de un sistema de gestión de incidentes capaz de mostrar fecha de registro, documentación relevante, personas involucradas, activos afectados. |

DS

| | | |
|---|---|---|
| E.1.2. | Asegurar una protección adecuada | Establecer controles de seguridad para las aplicaciones que procesen datos personales, entre ellas: Implementar controles para la detección de intrusos y/o fuga de información en las estaciones de trabajo que tengan acceso al tratamiento de datos personales |
| E.1.4. | Garantizar medidas eficaces perdurables | Implementar periódicamente procesos de auditoria interna para |
| | | verificar el cumplimiento de lo mencionado con anterioridad, exportando informes y resguardándolos. |
| | | Realizar auditorías externas a fin de evaluar la seguridad de los sistemas internos. |

F – Destrucción de la información

Relacionado con la implementación de los procesos de eliminación de datos, asegurando que el contenido confidencial sea debidamente destruido, utilizando métodos de borrado seguro y aplicando un control eficaz del proceso.

DP

| | | |
|---|---|---|
| F | DESTRUCCIÓN DE LA INFORMACIÓN | |
| | | |
| F.1. | Asegurar la destrucción de la información | |
| F.1.1. | Establecer modelo/formato de destrucción | Establecer un procedimiento de destrucción de datos en donde se identifique:<br>a) Tipo de información a destruir.<br>b) Medio que contiene la información.<br>c) Responsable de la destrucción.<br>d) Descripción del proceso y método de destrucción utilizado. |
| F.1.2. | Establecer mecanismos seguros de eliminación | Implementar un proceso de destrucción físico o lógico de la información que asegure el borrado total de la información sin posibilidad de recuperación de la misma cumpliendo tres premisas:<br>a) Irreversibilidad<br>b) Seguridad<br>c) Confidencialidad |
| F.1.3. | Designar responsable de destrucción | Establecer una persona autorizada para la destrucción y documentar su autorización. |
| F.1.4. | Monitorear el proceso | Disponer de un inventario que identifique los medios destruidos. |

DS

| | | |
|---|---|---|
| F.1.2. | Descarte de medios magnéticos | Implementar un proceso de destrucción lógico de reescritura continua, de modo que los datos originales no puedan ser recuperados, pudiendo reutilizar el medio magnético. |
| | | En caso de no poder realizar el proceso de destrucción lógica, implementar un proceso de destrucción física utilizando técnicas de desmagnetización, desintegración, incineración, pulverización, trituración o fundición. |

G – Incidentes de seguridad

Relativo al tratamiento de los eventos y consecuentes incidentes de seguridad que puedan afectar los datos personales, su detección, evaluación, contención y respuesta, como así también las actividades de escalamiento y corrección del entorno técnico y operativo.

DP

| | | |
|---|---|---|
| G | INCIDENTES DE SEGURIDAD | |
| | | |
| G.I. | Notificación ante incidentes de seguridad | |
| G.1.1. | Establecer responsabilidades y procedimientos | Elaborar un procedimiento de gestión ante incidentes de seguridad. |
| | | Establecer una persona responsable de la comunicación. |
| G.1.2. | Elaborar informe | Elaborar un informe del incidente de seguridad que tengo de contenido mínimo:<br>a) La naturaleza de la violación.<br>b) Categoría de datos personales afectados.<br>c) Identificación de usuarios afectados. |

# ZONA VIDEOVIGILADA

## LEY 25.326
## PROTECCIÓN DE DATOS PERSONALES

**Puede ejercer sus derechos ante:**

(Nombre del responsable del tratamiento)

(Dirección, Ciudad, C.P.)

(Teléfono)

(Página Web - correo electrónico)

**Para denunciar incumplimientos:** PDP
Dirección Nacional de Protección de Datos Personales
www.jus.gob.ar/datospersonales

Ministerio de Justicia y Derechos Humanos
Presidencia de la Nación

# Hoja de firmas

**Sistema: sudocu**
**Fecha: 15/03/2024 10:41:19**
**Cargado por: CECILIA INES VIEYRA**

**Sistema: sudocu**
**Fecha: 18/03/2024 15:52:20**
**Autorizado por: PATRICIA BEL DEMUTH MERCADO**

**Sistema: sudocu**
**Fecha: 18/03/2024 16:58:09**
**Autorizado por: GERARDO OMAR LARROZA**