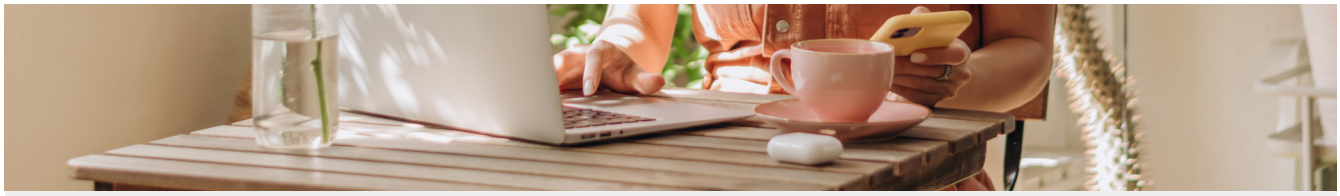
Confianza Digital y Protección de Datos Personales en el Reglamento de la Ley del Teletrabajo

(Decreto Supremo 002-2023-TR)

El pasado 26 de febrero se publicó el Decreto Supremo N° 002-2023-TR que aprueba el Reglamento de la Ley N° 31572 (Ley del Teletrabajo). Éste regula el teletrabajo en el sector público y privado, con la finalidad que dicha modalidad de trabajo se sujete a las necesidades del empleador y el teletrabajador.

Con respecto al ámbito de **confianza digital, protección de datos personales y seguridad de la información,** el Reglamento ha dispuesto las siguientes disposiciones:

CON RESPECTO AL TELETRABAJADOR



Sobre los derechos del teletrabajador

Los medios y herramientas que utilice **el empleador para la disposición, coordinación, control y supervisión del teletrabajo deben respetar la intimidad, privacidad** e inviolabilidad de las comunicaciones y documentos privados del teletrabajador.

Por lo tanto, el empleador está impedido de:

- Acceder, por medios digitales, a los documentos y comunicaciones originados con motivo del trabajo o de otra índole, **sin previa autorización de teletrabajador.** El documento informativo deberá cumplir con lo establecido en el artículo 18 de la Ley de Protección de Datos Personales, con relación al cumplimiento del deber de informar.

- Realizar captaciones y/o grabaciones de la imagen o la voz del teletrabajador, **sin consentimiento previo y expreso.** No es exigible el consentimiento si es necesario por la naturaleza de las funciones. En este caso, el cumplimiento del deber de informar también es obligatorio.

Sobre las obligaciones del teletrabajador

El teletrabajador tiene la obligación de **cumplir con la normativa vigente sobre seguridad de la información, confianza digital y protección de datos personales.**

Asimismo, debe guardar confidencialidad de la información proporcionada por el empleador.

Por lo tanto, el teletrabajador debe:

- Cumplir con las disposiciones señaladas en la Ley Marco de Confianza Digital (D.U 007-2020), Ley de Gobierno Digital (DL. 1412), para el caso de instituciones públicas, y todo el marco normativo relativo a la protección de datos personales.

- El mencionado marco normativo dispone obligaciones relativas al cumplimiento del deber de confidencialidad de los datos personales a los cual se tiene acceso, aún después de finalizada la relación laboral. Asimismo, establece la obligación por parte del teletrabajador de cumplir con las medidas de seguridad establecidas por el empleador a razón de proteger los datos personales del teletrabajador, de la empresa, y de terceros.

Ejemplos de medidas de seguridad

- No almacenar información personal y familiar en los equipos electrónicos brindados por el empleador.
- Evitar la conexión de internet de redes públicas
- No abrir links de procedencia desconocida en los correos electrónicos corporativos.

CON RESPECTO AL EMPLEADOR

Contenido mínimo del contrato o del acuerdo de cambio de modalidad:

Se debe establecer los conceptos relativos a las medidas de seguridad y confianza digital, en el marco previsto en **el artículo 24° de la Ley 31572.**

El mencionado artículo señala que las **condiciones específicas de seguridad y confianza digital** para el desarrollo del teletrabajo **se sujetan a lo establecido en el Decreto Legislativo 1412** (Ley de Gobierno Digital), y en el **Decreto de Urgencia 007-2020** (Ley Marco de Confianza Digital).

Para el sector privado aplican las disposiciones señaladas en la Ley Marco de Confianza Digital.

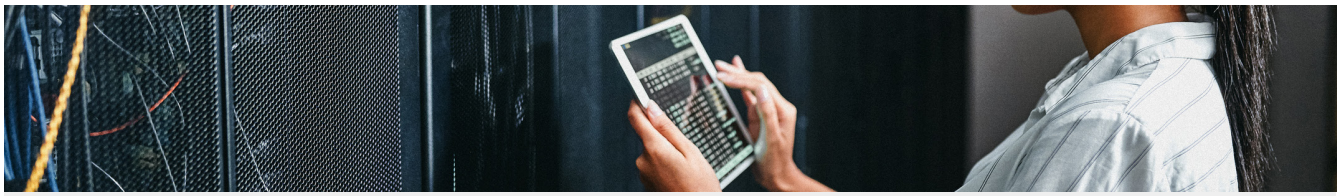
Para el sector público aplican tanto la Ley de Confianza Digital como la Ley Marco de Confianza Digital.

Entre las obligaciones estipuladas en la Ley Marco de Confianza Digital tenemos:

1. Notificar al Centro Nacional de Seguridad Digital todo incidente de seguridad digital.
2. Implementar medidas de seguridad físicas, técnicas, organizativas y legales.
3. Gestionar los riesgos de seguridad digital.
4. Establecer mecanismos para verificar la identidad de las personas que acceden a un servicio digital, conforme al nivel de riesgo del mismo y de acuerdo a la **normativa de protección de datos personales.**
5. Reportar y colaborar con la Autoridad Nacional de Protección de Datos Personales cuando verifiquen un incidente de seguridad digital que involucre datos personales.
6. Mantener una infraestructura segura, escalable e interoperable.

Asimismo, la Ley Marco de Confianza digital señala que el marco de la misma debe realizarse **observando la normativa vigente en materia de protección de Datos Personales.**

La Ley de Teletrabajo y su Reglamento se remiten, de forma expresa, al cumplimiento de las obligaciones contenidas en el Decreto Urgencia No. 007-2020, que establece los lineamientos de confianza digital.



El marco normativo vigente en materia de protección de datos personales, en lo relativo a seguridad de la información, está conformado por:

1. **Ley de Protección de Datos Personales (Ley 29733), y su Reglamento.**

2. **Directiva de Seguridad emitida por la Autoridad Nacional de Protección de Datos Personales (ANPD),** la cual brinda lineamientos para determinar las medidas de seguridad organizativas, legales y técnicas apropiadas en función de las características de la organización.

3. **Las opiniones consultivas emitidas por la ANPD relativas a seguridad de la infomación:**

    a. Opinión Consultiva N° 13-2021-JUS/DGTAIPD (sobre el tratamiento de los datos de los trabajadores en materia de seguridad y salud en el trabajo).

    b. Opinión Consultiva N° 24-2021-JUS/DGTAIPD (Sobre las medidas de seguridad, datos sensibles y flujo transfronterizo).

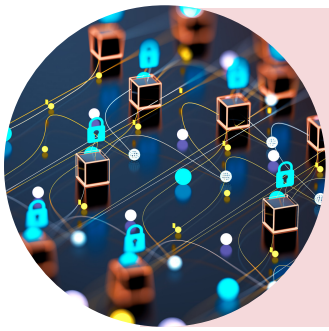
    c. Opinión Consultiva N° 17-2018-JUS/DGTAIPD (Sobre el cumplimiento de las medidas de seguridad aplicables al tratamiento de datos por medios informáticos y su concordancia con el derecho constitucional al trabajo.

CAPACITACIONES PRESENCIALES Y/O DIGITALES

El empleador tiene la obligación de brindar capacitaciones sobre **el uso de medios digitales en materia de protección de datos personales, seguridad y confianza digital.**

Las capacitaciones son relevantes a razón que la organización pueda cumplir con el principio de seguridad y el deber de confidencialidad, establecidos en la Ley de Protección de Datos Personales.

Las capacitaciones pueden reducir las contingencias relativas a un riesgo de exposición de la información de la organización, del trabajador o de terceros, respecto de las brechas de datos personales, accesos o usos no autorizados, entre otras amenazas que pueden afectar el la integridad, accesibilidad y disponibilidad de los datos personales.

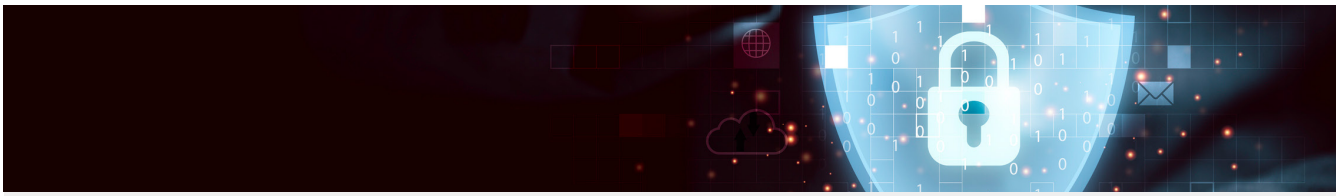


Resolución Directoral N° 655-2022-JUS/DGTAIPD-DPDP

La ANPD multó con 39.01 UITs a una organización, por la infracción al principio de seguridad y obligación de confidencialidad, dado que los colaboradores no cumplieron con las medidas de seguridad. Asimismo, se estableció como una de las medidas correctivas la capacitación al personal en lo relativo a seguridad y confidencialidad de la información.

En la misma línea, **las capacitaciones ayudan a cumplir con la obligación de confidencialidad.**

Se debe velar porque los trabajadores que tengan acceso a los datos personales de la organización, guarden la confidencialidad de la información. Por lo tanto, a razón de cumplir con la mencionada obligación, se debe capacitar al teletrabajador sobre las implicancias y contingencias que tiene divulgar la información considerada confidencial, así como las implicancias civiles, administrativas y penales que corresponda.



Las multas que puede imponer la ANPD ante las infracciones al principio de seguridad y el deber de confidencialidad son las siguientes:

- El no cumplir con las medidas de seguridad establecidas en la normativa de datos personales es considerada una infracción leve pasible a ser sancionada desde 0.5 UIT hasta 5 UIT.
- El realizar el tratamiento de datos sensibles sin cumplir con las medidas de seguridad establecidas en la normativa de datos personales es considerada una infracción grave pasible a ser sancionada desde 5 UIT hasta 50 UIT.
- El no cumplir con la obligación de confidencialidad es considerada una infracción grave pasible a ser sancionada desde 5 UIT hasta 50 UIT.

Para poder implementar con exactitud las medidas de seguridad aplicables es necesario realizar un análisis más complejo y exhaustivo sobre el flujo de los datos personales a razón de determinar la complejidad del tratamiento de los datos personales de la organización.

Para más información, escríbenos a:

Martin Serkovic
Socio
martinserkovic@esola.com.pe

Carol Quiroz
Asociada Senior
carolquiroz@esola.com.pe

Andrea Zanusso
Asociada Senior
andreazanusso@esola.com.pe