Teletrabajo y Seguridad de la Información

Webinar
Octubre 2021

Agenda

- Teletrabajo en Uruguay
- Seguridad de la Información en Uruguay, con especial foco en datos personales
- Ciberdelitos - Casos prácticos
- Preguntas

Teletrabajo en Uruguay

Teletrabajo en Uruguay

Normativa:

- **Ley de Teletrabajo Nº 19.978 :** aprobación Parlamentaria de 10 de agosto de 2021;
- **Ley de Rendición de Cuentas**: aprobada con fecha 14 de octubre de 2021.

> … entiéndase por “teletrabajo” la prestación del trabajo, total o parcial, fuera del ámbito físico proporcionado por el empleador, utilizando preponderantemente las tecnología de la información y de la comunicación, ya sea en forma interactiva o no (online-offline).

Teletrabajo en Uruguay - Ley de Teletrabajo N°19.978

Ámbito de aplicación

Lugar de trabajo

Principios

- Voluntariedad
- Reversibilidad
- Igualdad
- No discriminación
- Fomento del empleo

Jornada Laboral

Contrato de trabajo

Registro de asistencia

Teletrabajo en Uruguay - Ley de Teletrabajo N°19.978

- Derecho a la desconexión
- Herramientas y equipos para el teletrabajo
- Seguridad e higiene laboral
- Accidentes de trabajo

Los empleadores que utilicen la modalidad de teletrabajo, deberán ajustarse a las disposiciones de esta norma en el plazo de 6 meses a contar desde su promulgación.

Teletrabajo – Zonas Francas

2020: Área de Zonas Francas autorizó a realizar actividades en forma remota, hasta que la situación sanitaria permitiera el retorno a la presencialidad.

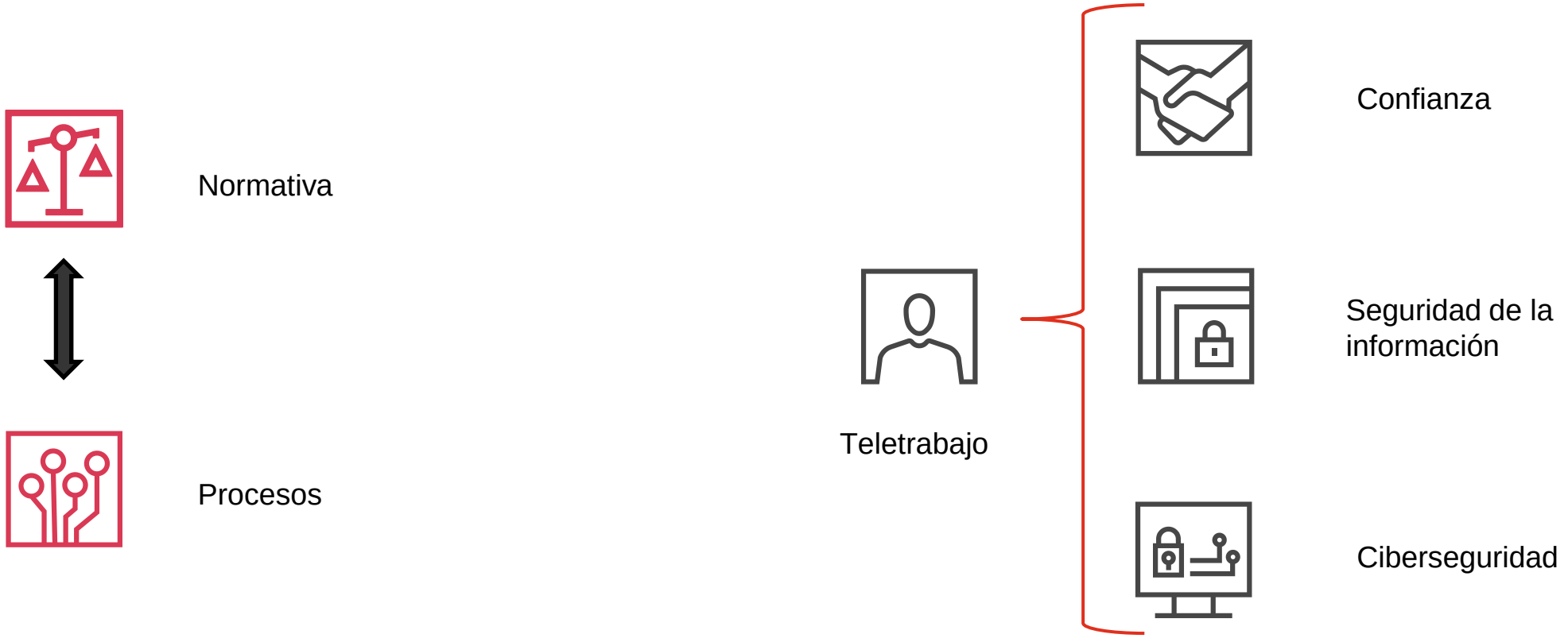
Ley de Rendición de cuentas:

- Usuarios ZF podrán celebrar acuerdos con personal dependiente para teletrabajar exclusivamente desde su domicilio particular en territorio nacional.
- PE establecerá condiciones y límites para la celebración de dichos acuerdos.
- Usuario ZF deberá asegurar el control de los recursos humanos que teletrabajen (días y horarios), información que podrá ser solicitada por la Dirección Nacional de Zonas Francas.
- No quedan comprendidos trabajadores que desarrollen actividades operativas de producción o fabriles, de distribución, o logísticas, ni actividades comerciales sustantivas.
- Habilitación para teletrabajo no implicará autorización para instalar oficinas administrativas fuera de ZF.

Seguridad de la Información

con especial foco en datos personales

Teletrabajo - Seguridad de la Información Protección de Datos



Datos personales: Cualquier tipo de información sobre un individuo que lo identifique o lo haga identificable.

Ej.: nombre, dirección, teléfono, CI, RUT, huella digital, número de socio, de estudiante, fotografía, ADN, etc.

Teletrabajo - Seguridad de la Información Protección de Datos

Recomendaciones (1 de 2)

Herramientas y dispositivos previamente definidos

Medios para informar o capacitar sobre alcance de herramientas empleadas, posibles amenazas a datos personales y procesos de informe de incidentes

Políticas internas

Contratos con terceros que determinen las obligaciones y derechos de las partes

Guías funcionales sobre tratamiento de datos personales, más aún si se utilizan equipos o redes domésticas

Mecanismos y plazos para el almacenamiento de la información transmitida y verificar la transferencia

Teletrabajo - Seguridad de la Información Protección de Datos

Recomendaciones (2 de 2)

Configurar técnicamente equipos informáticos para asegurar la privacidad de las comunicaciones

Medios para hacer efectivos los derechos ARCO

Informar si se utilizan sistemas de monitoreo y tratamiento de la información

Evaluación de impacto de la protección de datos

Recomendaciones técnicas para implementar el teletrabajo de AGESIC
Uso seguro – Escritorio remoto – Cuidado de la información
- Canales de comunicación

Ciberseguridad

Ciberseguridad – casos de estudio

Desvío exitoso de pago al exterior

A principios del 2021, un cliente recibió un **reclamo por un pago adeudado** a un proveedor del exterior. Nuestro cliente declaró que el pago había sido realizado, enviando los comprobantes de transferencia.

El proveedor detectó que **el pago se había realizado a una cuenta que no era de su propiedad.**

A partir de ese **momento se inicio una investigación**, para determinar lo ocurrido y ver la posibilidad de recuperar el dinero (USD 2M).

Cadena de correos intervenida por un atacante, quien reemplazo las direcciones de correo del proveedor por **cuentas falsificadas** y realizo la **solicitud del cambio de destino de la cuenta de pago a un banco en US**.

Fallas en **los controles y procesos** en las áreas de comerciales y de Pago a proveedores, que permitieron al estafador conseguir su cometido.

También se detectaron **fallas en los niveles de concientización** de **los empleados en niveles de seguridad**

Ciberseguridad – casos de estudio

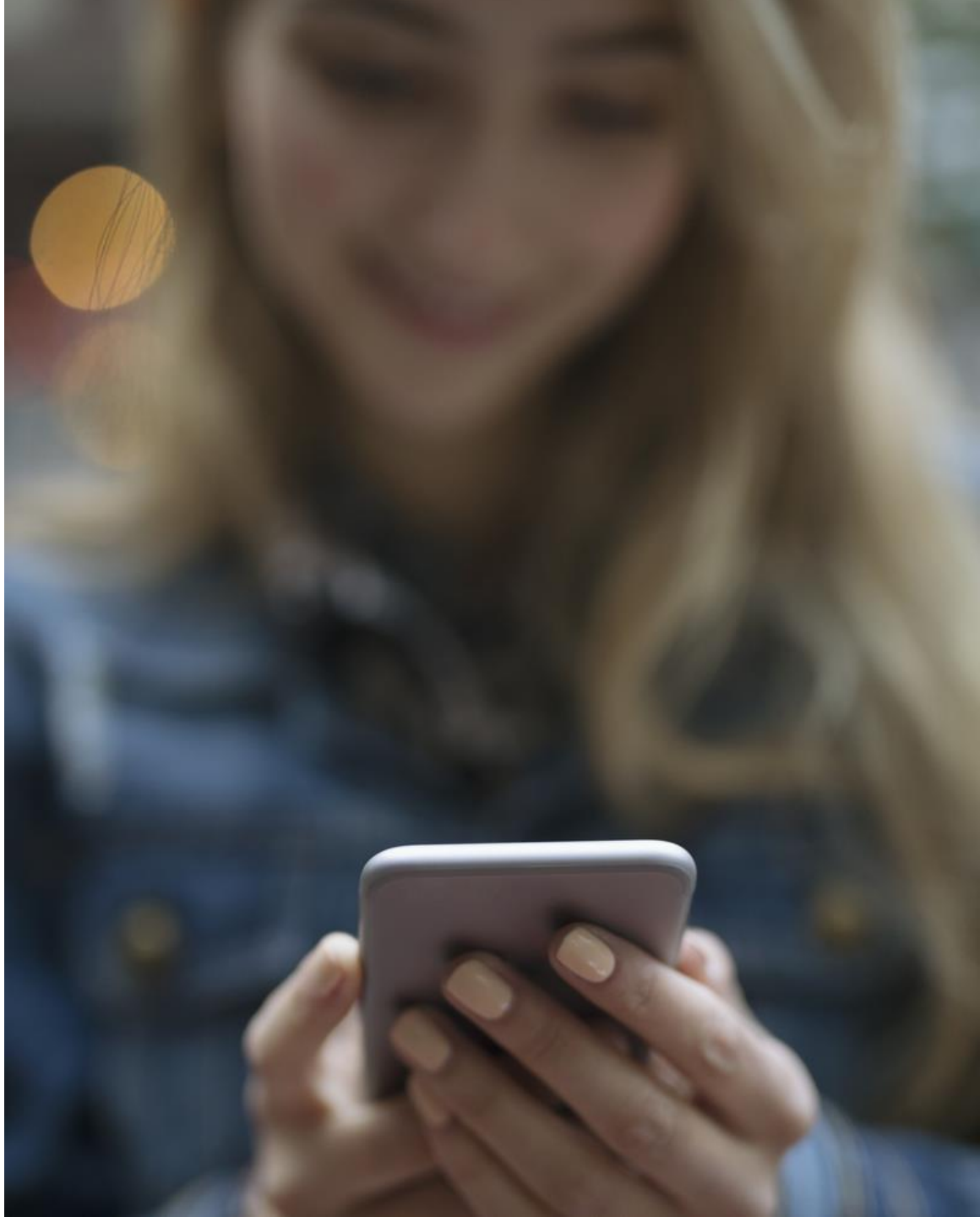
Intento de desvío de pago a proveedor del exterior

A mediados de Abril de 2020, uno de nuestros clientes detectó un intento de **fraude** al descubrir que una **cadena de emails entre su organización y uno de sus proveedores había sido intervenida, reemplazando a los destinatarios del proveedor por cuentas falsas**, con la intención de desviar un pago a una cuenta distinta de la del proveedor, hacia un banco de México.

El hecho fue detectado apenas hecha la transferencia para el pago y la misma se pudo revertir.

Pudimos detectar las **faltas de control y procesos** que permitieron al estafador casi a conseguir su cometido.

También pudimos identificar al titular de la cuenta bancaria en México y poner a disposición del cliente la información para llevar a cabo las medidas pertinentes.



Ciberseguridad – casos de estudio

Ataque de ransonware a Industria Argentina

A principios de septiembre de 2020, una empresa Argentina dedicada a la manufactura de tecnología sufrió un **ataque de ransonware**.

Mas de 20 servidores fueron encriptados en un periodo relativamente corto de tiempo (1-2hs).

Después del ataque, la empresa descubrió que gran parte de sus backups eran irrecuperables

También se detectaron problemas con los servicios de monitoreo que estaban funcionando.

Se perdieron 5 años de información sensible.

Aprecia a los CONTROLES INTERNOS

Como dicen, dos pares de ojos ven mas que uno!

Las organizaciones dependen de sus procesos de control interno para garantizar que las operaciones internas se realizan de la forma acordada y que sean revisadas por los responsables adecuados.

Los empleados en posiciones clave SON un objetivo mas que interesante para ciertos tipos de atacantes.

Aplicar debidamente los controles internos permite a las empresas detectar acciones que podrían llevar a la empresa a caer víctimas de ataques puntuales, como fraude financiero, entre otros.

Ante un requerimiento de realizar excepciones a los controles, es importante informar de estas situaciones.

Las situaciones excepcionales NO DEBEN continuarse en el tiempo.

Los procesos de control interno deben ser sometidos a revisión periódicamente, en lo posible, por terceros independientes.

Atención!!

Los atacantes intentarán invalidar los controles internos de esta forma:

- Explotan la predisposición a ayudar.
- Manipulan la confianza hacia el interlocutor (falso), distrayéndonos de comprobaciones básicas.
- Nos esforzamos en no decir NO (nos lleva a saltear controles).
- Nos gusta ser alabados y no presionados, lo cual también es utilizado por los atacantes habilidosos.

¡Gracias!

¿Seguimos en contacto?

Andrea Chanquet
andrea.chanquet@pwc.com

Milagros Eiroa
milagros.eiroa@pwc.com