Circular 37-2020. MEDIDAS DE SEGURIDAD.

Distinguido cliente:

El motivo de la presente circular, es realizar una serie de recomendaciones de medidas de seguridad a efectos de proteger la información que utilizamos.

1.- Medidas de protección para los dispositivos móviles: ordenadores portátiles, teléfonos inteligentes o smartphones, tabletas.

La globalización y la deslocalización de los procesos productivos de las empresas, hace que necesitemos trabajar y **acceder a la información de trabajo desde cualquier lugar**; de manera inmediata, rápida y ágil.

Por ello, para ser más productivos, hace que cada vez más utilizamos nuestros dispositivos móviles, ya sean de uso corporativo o personal, para acceder y compartir la información de trabajo con otros compañeros, clientes, proveedores, etc. desde cualquier lugar o dispositivo autorizado, ya sea desde dentro de la empresa o desde fuera de ella.

Esta "movilidad" nos aporta grandes ventajas, pero hay que tener muy presente también los riesgos que conlleva y cómo gestionarlos.

Riesgos como:

- pérdida o robo de información confidencial,
- el mal uso que se pueda hacer de los dispositivos,
- robo de dispositivos,
- robo de credenciales,
- utilización de sistemas de conexión no seguros, etc.

Todo esto hace que establezcamos los mecanismos necesarios para asegurar la seguridad en movilidad de estos dispositivos y de las redes de comunicación utilizadas para acceder a la información corporativa.

Para la protección de la información almacenada en estos dispositivos, debemos aplicar una serie de **medidas básicas** como las siguientes:

a) **Contemplar el uso de los dispositivos móviles, teletrabajo e información almacenada** fuera de las instalaciones de la empresa, **dentro de la política de seguridad de la empresa.**

** Recordad insertar los dispositivos de los empleados en el ANEXO 14, para que vuestra documentación este actualizada.

b) **No dejar los dispositivos móviles desatendidos en lugares públicos**, coche, etc.

c) **Evitar utilizar redes wifi ajenas, especialmente aquellas que no llevan contraseña**. Cuando sea posible, utiliza tu propia conexión 3G/4G.

d) **Utilizar siempre una conexión VPN** para enviar o recibir información sensible desde una red poco confiable.

e) **Tener siempre el antivirus y el dispositivo actualizado**, especialmente fuera de las redes corporativas.

f) **Utilizar siempre herramientas de cifrado de datos y comunicaciones** para proteger la información sensible de los dispositivos.
g) Salvaguardar la información periódicamente según su criticidad, mediante la **realización de copias de seguridad periódicas**.

2.- BYOD (por sus iniciales en inglés, Bring Your Own Device)

Especial atención hay que tener en cuenta al modo de trabajar denominado BYOD (por sus iniciales en inglés, Bring Your Own Device), caracterizado por el hecho de **permitir a los empleados la incorporación de sus dispositivos móviles personales (portátiles, smartphones y tabletas) a las redes corporativas desde su casa, la propia oficina o cualquier otro lugar, aceptando su uso compartido**, tanto para las tareas profesionales de uso corporativo como para las personales de los empleados.

Una buena parte de los riesgos que conlleva el BYOD estriba en el uso que haga de los dispositivos el usuario.

Para minimizar los riesgos derivados del uso de dispositivos BYOD a la hora de integrarlos dentro de la organización y obtener el mayor rendimiento posible de los mismos, seguiremos estos **consejos**:

- **Involucrar a los usuarios** en la protección de sus propios dispositivos, mediante su formación. Debemos incentivar, concienciar y formar al usuario para que tome medidas destinadas a proteger los datos corporativos y personales.
- **Mantener una base de datos de usuarios y dispositivos. Es conveniente mantener una base de datos con:**
  - la relación de dispositivos que acceden a los recursos de la empresa,
  - los usuarios que los manejan
  - los privilegios de seguridad que nos permitan autenticar y autorizar estos usuarios y dispositivos.
- **Tomar precauciones con el almacenamiento de datos de trabajo**. Hay que tener especial cuidado con las herramientas que utilizamos para el almacenamiento de datos corporativos, especialmente a la hora de utilizar aplicaciones de intercambio de archivos en la nube.
- Las aplicaciones públicas instaladas por los usuarios no son tan seguras como las corporativas para proteger los datos sensibles de nuestra empresa. A la hora de trabajar con los datos de la empresa, es más seguro **tener los datos almacenados en la nube y consultarlos,** que realizar un intercambio de archivos real.
- **Implementar medidas para el acceso seguro a la información**. Desde la empresa se deben implementar en los dispositivos mecanismos adicionales de seguridad:
  - Cifrado de la información
  - Correcta autenticación de usuarios. Se puede optar por sistemas de autenticación mediante contraseñas, utilizando aplicaciones gestores de contraseñas, que facilita el uso de contraseñas fuertes personalizadas para cada aplicación, o sistemas mixtos de utilización de contraseña y medios biométricos como huellas digitales.
- **Actualizar las políticas de seguridad para incluir el uso de BYOD**, reforzando el apartado referente a la política de protección de datos corporativa. También debemos concienciar a los usuarios de la importancia y la necesidad de la aplicación de esta política de protección de datos.

  ** Recordad insertar los dispositivos de los empleados en el ANEXO 14, para que vuestra documentación este actualizada.

3.- Comunicaciones inalámbricas

En la mayoría de las redes inalámbricas que utilizan los trabajadores fuera del entorno empresarial debemos asumir que no existe protección de datos alguna. A menudo, información confidencial de nuestra empresa puede transmitirse a través de redes inalámbricas que no están bajo nuestro control, por lo que debemos asegurarnos de que los datos viajan convenientemente protegidos.

La **manera de evaluar la seguridad de una solución inalámbrica es a través de su capacidad para mantener la confidencialidad, la integridad y la autenticidad** de los datos a través de la red inalámbrica, desde el dispositivo móvil hasta la red corporativa.

4.- Redes wifi de terceros

Es habitual que un empleado utilice con frecuencia redes públicas abiertas o poco seguras para el intercambio de correo electrónico corporativo o para acceder a aplicaciones de la empresa.

Este tipo de redes podemos encontrarlas como servicio de cortesía en restaurantes, hoteles, aeropuertos, etc. Los motivos habituales para el uso de estas redes inseguras suelen ser la velocidad de la red, no disponer de conexión de datos (3G, 4G,…) en el portátil, ahorrar tarifa de datos o por el tipo y calidad de la cobertura.

Sin embargo, a menudo su uso se realiza sin pensar en las posibles consecuencias. Es primordial utilizar este tipo de redes con algún tipo de seguridadadicional.

Utilizar este tipo de redes con algún tipo de cifrado punto a punto como los sitios web con SSL (que son los que empiezan con HTTPS y tienen un candado junto a la dirección) o como la posibilidad que ofrece VPN. A modo orientativo se podría decirque:

Wifi	A dónde te conectas	¿Qué puedes hacer?:
Pública y no segura	A un sitio web no seguro	Sólo actividades de bajo riesgo: • Navegar • Leer noticias
Pública y no segura	A un sitio web cifrado (https://) y con candado	Actividades de riesgo moderado: • Login (inicio de sesión) en sitios en los que estás suscrito
Pública pero segura (WPA)	A un sitio web cifrado (https://) y con candado	Actividades de alto riesgo • Email • Trabajar con documentos online • Redes sociales

Pública y segura	A sitios web cifrados o no	Actividades de muy alto riesgo • Banca online • PayPal o tarjetas de crédito

No obstante algunas aplicaciones, como las de correo electrónico o archivo de documentos en la nube, redes sociales, tienen la posibilidad de configurar cuándo se sincronizan. En la sincronización intercambian credenciales de acceso. **Desactiva la sincronización automática cuando utilices redes en las que no confíes**.

A veces el usuario piensa que conectarse a este tipo de redes para tareas que no necesitan una seguridad considerable (como leer el periódico) no conlleva riegos. Sin embargo, en los dispositivos móviles las aplicaciones como el correo siguen funcionando aunque la aplicación no esté en pantalla. Por tanto, no es posible asegurar que los datos que atraviesan la red segura son de poca importancia.

5.- Redes inalámbricas de corta distancia.

Hoy en día disponemos de otro tipo de **redes inalámbricas de corta distancia como Bluetooth y Zigbee**, que nos permiten conectar varios dispositivos cercanos entre sí.

Las **redes Bluetooth** se utilizan para conectar ratones y teclados con el ordenador, o los relojes (smartwatches), pulseras de actividad con el ordenador de a bordo del coche con el Smartphone.

Las **redes Zigbee** se utilizan en dispositivos demóticos y en automatización de edificios. En general, si se usa en dispositivos corporativos o personales, se han de tomar las siguientes medidas de seguridad:

- Activarlos sólo cuando se vayan a utilizar.
- No aceptar ninguna conexión desconocida y requerir siempre autenticación.
- Configurar los dispositivos para que no resulten visibles a terceros y revisar periódicamente la lista de dispositivos de confianza registrados.
- Asignar nombres a los dispositivos que no reflejen marcas ni modelos.
- Mantener actualizado el software del Smartphone.

6.- Acceso remoto

El mejor sistema para la conexión remota a los equipos de nuestra organización es mediante la utilización de una **red privada virtual, también llamada VPN**.

Esta tecnología de red proporciona un acceso seguro a las aplicaciones y sistemas corporativos a empleados dispersos geográficamente, de una manera equivalente al tipo de acceso que tendrían en los locales de nuestra empresa.

Una red privada virtual **se basa en la técnica de tunneling**, en la que haciendo uso de ciertos protocolos (IPSEC, SSTP, etc.) permite a los datos transferidos de un extremo a otro de la VPN, (por ejemplo, nuestro dispositivo y la red de la organización) ser asegurados por algoritmos de criptografía.

El término «túnel» se utiliza para simbolizar el hecho de **que los datos de entrada y salida se transmiten por un canal cifrado**, por tanto, incomprensibles para cualquier persona pueda interceptar el tráfico de la VPN.

Una conexión remota utilizando esta tecnología presenta las siguientes **ventajas**:

- **Permite al usuario conectarse a la organización de una manera totalmente segura**, incluso desde redes abiertas o poco seguras.
- **Funciona sobre conexiones 3G, 4G y wifi**, de modo que es una capa de seguridad extra sobre la red que estemos utilizando.

- **Limita el medio de acceso remoto a nuestra organización a un único punto con autenticación**, lo que permite un mayor control de los accesos.
- **Reduce los servicios expuestos a Internet**, disminuyendo la posibilidad de ser atacados. Sin embargo, si la contraseña de acceso a la VPN resulta comprometida por un atacante, éste dispone de un acceso a la red interna de nuestra empresa, por lo que puede resultar muy peligroso.
- **Reduce los servicios expuestos a Internet**, disminuyendo la posibilidad de ser atacados. Sin embargo, si la contraseña de acceso a la VPN resulta comprometida por un atacante, éste dispone de un acceso a la red interna de nuestra empresa, por lo que puede resultar muy peligroso.

7.- Medidas de seguridad para la instalación y utilización de software de escritorio remoto (ej.: AnyDesk, TeamViewer):

Actualización de equipos y dispositivos

- Los ordenadores, portátiles, tabletas, smartphones y demás dispositivos utilizados para el almacenamiento, tratamiento o transmisión de datos personales, deberán mantenerse actualizados en la medida de lo posible.
- Sistemas operativos: deben estar instaladas las últimas versiones estables, y las actualizaciones han de ser provistas directamente por el fabricante.
- Programas: deben estar instaladas las últimas versiones estables, y las actualizaciones han de ser provistas directamente por el fabricante.
- Dispositivos (routers, firewalls, videocámaras, etc.): se ha de mantener el firmware actualizado a la última versión estable proporcionada por el fabricante.

Copias de respaldo y recuperación

- La seguridad de los datos personales no solo supone la confidencialidad de los mismos, sino que también conlleva la integridad y la disponibilidad de esos datos.

- Para garantizar estos dos aspectos fundamentales de la seguridad es necesario que existan unos procesos de respaldo y recuperación, de forma, que ante un fallo informático, permitan reconstruir el fichero en el estado que se encontraba antes de la pérdida.
- Se realizarán copias de respaldo periódicamente, en función del volumen y de la frecuencia de actualización de los datos.
- Los procedimientos establecidos para las copias de respaldo y para su recuperación garantizarán su reconstrucción en el estado que se encontraban al tiempo de producirse la pérdida o destrucción.
- Únicamente, en el caso de que la pérdida o destrucción afectase a ficheros o tratamientos parcialmente automatizados, y siempre que la existencia de documentación permita alcanzar el objetivo al que se refiere el párrafo anterior, se deberá proceder a grabar manualmente los datos, quedando constancia motivada de este hecho en el Registro de Incidencias.
- Se verificará semestralmente los procedimientos de copias de respaldo y recuperación de los datos.
- Las pruebas anteriores a la implantación o modificación de sistemas de información que traten con datos de carácter personal no se realizarán con datos reales, salvo que se asegure la seguridad correspondiente al tratamiento realizado y se registre su realización. Si está previsto realizar pruebas con datos reales, previamente deberá haberse realizado una copia de seguridad.

Formación del personal

- Para que el tratamiento de los datos personales se realice en todo momento según los requisitos legales y de seguridad que marca la normativa, todo el personal involucrado en el tratamiento (recogida, registro, utilización, destrucción, etc.), sea externo o interno, debe recibir formación apropiada a las funciones realice, tanto en materia de protección de datos personales como en materia de seguridad y ciberseguridad.
- El personal que realice tareas de administración de sistemas debe recibir formación apropiada en relación a los sistemas que gestiona, de forma que no se produzcan omisiones o errores accidentales que afecten, o puedan afectar, a la confidencialidad, integridad y disponibilidad de los datos personales.
- Las personas (o persona) que actúe como Delegado de Protección de Datos y/o Responsable de Seguridad debe disponer de la formación y las competencias necesarias para desempeñar sus funciones con rigor y solvencia.

Limitación de intentos de acceso

- En aquellos sistemas que permitan acceder a datos especialmente sensibles, debe limitarse el número máximo de intentos de acceso no autorizado para evitar ataques de fuerza bruta que permitan obtener

las credenciales de acceso al sistema o las aplicaciones.

- Para ello, se deben configurar apropiadamente las políticas de seguridad del sistema de forma que se bloquee la cuenta del usuario al sobrepasar un número máximo definido de intentos de acceso no autorizado.

Registro de acceso

- Deberá existir un registro de accesos que permita conocer, de cada intento de acceso, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado. Si el acceso ha sido autorizado, será preciso guardar la información que permita identificar el registro accedido.
- Los mecanismos que permiten el registro de accesos estarán bajo el control directo del Responsable de Seguridad competente o del Delegado de Protección de Datos sin que deban permitir la desactivación ni la manipulación de los mismos.
- El periodo mínimo de conservación de los datos registrados será de dos años.
- El Responsable de Seguridad o el Delegado de Protección de Datos se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados.

Software anti-malware

- En los ordenadores y dispositivos donde se realice el tratamiento automatizado de los datos personales se dispondrá de un sistema anti-malware que evite, en la medida de lo posible, el robo y la destrucción de la información y datos personales. El sistema anti-malware deberá ser actualizado de forma periódica.

8.- Cumplimiento normativo

Les recordamos que deben efectuar el cumplimiento normativo en materia de Protección de Datos, bien implantando la norma aplicable para aquellas empresas, tanto personas físicas como jurídicas, que hasta la fecha no lo hayan efectuado, o bien realizando las actualizaciones y auditorias correspondientes para aquellos que ya tengan implantada la norma correspondiente.

9.- Recordatorio

Como consecuencia de la situación actual originada por el COVID-19, el ejercicio de nuestra actividad se desarrollará a puerta cerrada, prestando nuestros servicios mediante la opción telemática, hecho en ningún caso, verá mermado el servicio prestado.

Asimismo, les indicamos como ya se ha venido efectuando en circulares anteriores, los canales de los que dispone para contactar con nosotros:

- Atención Telefónica

1. Teléfonos móviles, tenemos habilitados los teléfonos

   - Recepción 665282734
   - Gonzalo 632948152
   - Sara 632860611
   - Inma 632860837
   - Iciar 632511626
   - Laura 632860743
   - Musa 609618228
   - Pedro 632860687
   - Paqui 609769854
   - Mª Cruz 632511885
   - Montse 608166909
   - Esther 632536156
   - Nacho 632511557

   Teléfonos fijos
   - 918811231
   - 918811211

- Atención telemática, para entrega y envío de documentación:
  - Portal del Cliente Net-Asesor https://cutt.ly/LtgBhju
  - Correo Electrónico @gtasl.es
  - Le rogamos eviten el uso del WhatsApp.

- Horario atención telefónica será de lunes a viernes mañanas de 09h a 14h

Desde GTA, reiteramos nuestro apoyo y les ofrecemos nuestra ayuda.

Sin otro particular, aprovechamos para saludarle atentamente, Alcalá de Henares 7 de abril de 2020.

Departamento de Gestión.

Móvil: +34 665 28 27 34
tlf: 918811231 - 918811211
fax: 918808303

VISITA NUESTRA WEB:
www.gtasl.es

**********Aviso**********
De acuerdo con lo establecido en el Reglamento UE 2016/679 (RGPD) le informamos que tratamos los datos que usted nos ha facilitado para realizar la gestión administrativa, mercantil, laboral, contable y/o fiscal, así como enviarle comunicaciones comerciales sobre nuestros productos y/o servicios. La causa que nos legitima es su consentimiento. No se cederán datos a terceros. Tiene derecho a acceder, rectificar y suprimir los datos, así como otros derechos, indicados en la información adicional. Aviso Legal
El "Cliente" autoriza expresamente en este acto, que la mercantil "Gestión Tributaria Alcalá, S.L." utilice como medio de comunicación tanto las aplicaciones móviles, como los correos electrónicos.
Si usted no desea recibir nuestra información, póngase en contacto con nosotros enviando un correo a la siguiente dirección de correo electrónico: info@gtasl.es o mediante correo ordinario dirigido a GESTION TRIBUTARIA ALCALA S.L. sito en C/ GALLEGOS 8 - 28807 ALCALA DE HENARES - MADRID