

Cód. Documento: 01 20 IT	TIPO DE DOCUMENTO: CIBERSEGURIDAD Y TELETRABAJO	
-----------------------------	--	---



CIBERSEGURIDAD Y TELETRABAJO

Debido a la situación actual que estamos viviendo como consecuencia del Covid-19, se ha puesto de manifiesto lo importante que es la **Transformación Digital**. La cual nos permite suavizar las consecuencias de esta crisis.

La pandemia ha situado a las empresas ante la cruda realidad de la **digitalización**, la **ciberseguridad** y el **teletrabajo** de los que tanto tiempo lleva hablándose.

El teletrabajo expone a la empresa a un mayor riesgo de ciberseguridad. Los ciberataques se están multiplicando mientras pasamos mucho más tiempo online utilizando dispositivos destinados para hacer nuestros pagos, compartirlos con los niños para que hagan los deberes del colegio, para ver una película en familia por la noche, para compartir redes sociales. No les dejamos un respiro y son una puerta abierta a los **ciber-atacantes** dispuestos a explorar cualquier oportunidad.

Los ataques por correo electrónico tipo **phishing** se han intensificado. Ingeniería social para suplantar la identidad de una cuenta reconocida y de confianza para los usuarios enviando correos ficticios que parecen reales, con el objetivo de hacerse con nuestro usuario y contraseña o con archivos adjuntos que contiene código malicioso que cifra los archivos (ransomware) a cambio de un rescate.

¿Cómo podemos reducir los riesgos de ciberseguridad y establecer las medidas necesarias para un teletrabajo eficaz y fiable?

1. Es necesario establecer los **procedimientos de seguridad** en los equipos de teletrabajo, garantizado así que se utilizan siguiendo la política de la empresa y las aplicaciones autorizados. Por eso es importante evitar que los trabajadores utilicen sus equipos personales.
2. Es importante **inventariar los activos de información**, y concretar por cada trabajador los permisos de uso de este, estas medidas de control permiten proteger a la empresa.

Fecha: 11/11/2020	DEPARTAMENTO: IT SERVICES	REALIZADO POR: RRT	REVISADO POR: DGP	Página:
----------------------	------------------------------	-----------------------	----------------------	---------

Cód. Documento: 01 20 IT	TIPO DE DOCUMENTO: CIBERSEGURIDAD Y TELETRABAJO	
-----------------------------	--	---

3. Firmar con el trabajador la entrega y los **compromisos de confidencialidad** que adquiere con la salida de ellos soportes de la empresa.
4. **Configuración de la comunicación** (routers, firewall, ...), contraseñas, privilegios, aplicaciones permitidas, y la conexión remota a los servidores mediante redes privadas virtuales (VPN), filtros de correo antispam, de contenidos y de autenticación, limitando el acceso a todo aquello que la empresa decida que no tiene nada que ver con el desempeño laboral.
5. Es recomendable contar con **seguridad Endpoint** y monitorizar de forma centralizada todos los activos IT que intervienen entre empleado y datos de empresa
6. Definir e implantar un **Plan de Contingencias**, respuesta ante incidentes y continuidad de negocio.
7. **Formar y concienciar a los trabajadores** para que estén familiarizados con los riesgos y amenazas más frecuentes y su forma de prevención.

Para todo ello es vital tener un buen equipo técnico informático que analice, defina implemente y dé continuidad a todas estas medidas.

Anticípate e implanta solución y control en tu negocio antes que llegue el problema.

Contacta con nosotros y te informamos.

Personal de contacto: **Silvia López y Silvia Martín**

Teléfono: **942 22 68 68** y **637898116**

E-mail: **administracion@glezco.com**

Aprovechamos también para informaros que actualmente están en vigor en Cantabria las ayudas de **SODERCAN** que financian este tipo de implantaciones, y que os ayudaremos a solicitar si estáis interesados.

Fecha: 11/11/2020	DEPARTAMENTO: IT SERVICES	REALIZADO POR: RRT	REVISADO POR: DGP	Página:
----------------------	------------------------------	-----------------------	----------------------	---------