TELETRABAJO
decálogo de ciberseguridad

BASQUE CYBERSECURITY CENTRE

Cada vez son más las empresas que están ofreciendo la posibilidad de teletrabajar. Para que todo funcione bien y garantizar la seguridad, debemos tomar algunas precauciones.

Factores a tener en cuenta

- Aspectos financieros
- Legislación aplicable
- Capacidad técnica de la organización
- Arquitectura admitida por las capacidades técnicas de la organización
- Modelos de propiedad permitidos en la organización (COBO, COPE, BYOD)

Recomendaciones

Uso de medios tecnológicos de la empresa
Establecer qué puede hacer y qué no el trabajador con los dispositivos y sistemas de propiedad de la empresa (móviles, portátiles...).

Medios propios del trabajador
Establecer una política de uso de medios propios que incluya requisitos de seguridad.

Usuarios individuales
Abandonar los usuarios genéricos por seguridad. Además, las contraseñas deben ser robustas y deben caducar. Y si es posible, implementar un sistema de doble factor.

Actualizaciones
Todos los sistemas operativos de servidores, portátiles y móviles deben estar actualizados para evitar vulnerabilidades de seguridad que pudiesen ser aprovechadas por un tercero malintencionado.

Herramientas colaborativas
Digitalización de la documentación para que esté disponible para todos los trabajadores y facilitar la comunicación y la gestión de proyectos.

Nube
Posibilidad de acceder a través de una página web y una autenticación fuerte o doble factor de autenticación (por ejemplo, token software en el teléfono móvil, un SMS, etc.) a portales tipo Citrix o VMware en la nube que les daría acceso a los sistemas corporativos.

GRUPO spri

EUSKO JAURLARITZA
GOBIERNO VASCO
EKONOMIAREN GARAPEN ETA AZPIEGITURA SAILA
DEPARTAMENTO DE DESARROLLO ECONÓMICO E INFRAESTRUCTURAS

TELETRABAJO
decálogo de ciberseguridad

BASQUE CYBERSECURITY CENTRE

Borrado seguro
Todos aquellos archivos que contengan información sensible deberán ser borrados de manera segura cuando finalice su uso utilizando una herramienta de borrado seguro.

Copias de seguridad
Implementar sistemas que permitan realizar copias de seguridad de la información de los usuarios.

Cortafuegos personal
Utilizar un cortafuegos personal que permita únicamente las comunicaciones autorizadas.

Cifrado en las comunicaciones
Conectarse al entorno corporativo a través de redes privadas virtuales (VPN).

Cifrado de dispositivos
Todos los dispositivos deben estar cifrados para dificultar el acceso a la información en caso de pérdida o robo.

En caso de incidente...
informar lo antes posible al responsable de sistemas de la organización.

GRUPO spri

EUSKO JAURLARITZA
GOBIERNO VASCO
EKONOMIAREN GARAPEN ETA AZPIEGITURA SAILA
DEPARTAMENTO DE DESARROLLO ECONÓMICO E INFRAESTRUCTURAS