Recomendacións en materia de ciberseguridade e privacidade para empresas e outro tipo de organizacións ante a crise do COVID-19

#EuQuedoNaCasa

amtega
Axencia para a Modernización Tecnolóxica

XUNTA DE GALICIA

No contexto da crise do COVID-19, indícanse unhas recomendacións xerais para as empresas e organizacións en xeral, sobre todo para aquelas que implanten o teletraballo.

FERRAMENTAS SEGURAS

Debe potenciarse o uso de ferramentas de traballo que eviten riscos técnicos e de incumprimento da normativa vixente, instando aos empregados a que utilicen as ferramentas corporativas evitando o uso de plataformas de terceiros non autorizadas.

ACCESOS

Recoméndase limitar os accesos aos sistemas de teletraballo desde as localizacións onde a empresa desenvolve a súa actividade (por exemplo, non permitir accesos desde fóra de España se non son necesarios).

IDENTIFICACIÓN SEGURA DAS PERSOAS USUARIAS

É necesario establecer un mecanismo seguro de identificación do usuarios, como mínimo usuario-contrasinal seguros, e a poder ser utilizando mecanismos de dobre factor (por exemplo, requirir a introdución dun código SMS recibido no teléfono móbil).

CONEXIÓN SEGURA

Para teletraballar é necesario utilizar unha conexión a internet de confianza, como pode ser a facilitada pola organización, de ser o caso, ou a do domicilio particular do empregado. É preciso evitar o uso de redes públicas como poden ser as wifis de locais abertos ao público, por exemplo, de aeroportos.

EQUIPOS ACTUALIZADOS

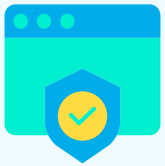
É necesario manter actualizados os equipos, tanto os da organización como os da casa no caso de teletraballo, especialmente no referente ás actualizacións de seguridade do fabricante, así coma o antivirus actualizado ou instálao en caso de non dispoñer del.

VIXILANCIA

É necesario monitorizar de xeito proactivo e continuo a seguridade dos sistemas de información.

COPIAS DE SEGURIDADE

É necesario revisar os plans de copia de seguridade existentes na organización na organización para evitar perdas de información.



NAVEGACIÓN SEGURA

É preciso realizar unha navegación segura por internet, evitando o acceso a páxinas dubidosas, especialmente nesta situación de crise do COVID-19, debido á proliferación de ciberataques e ciberestafas que utilizan como cebo temas relacionados con esta crise sanitaria.

CORREO ELECTRÓNICO

É preciso que se alerte aos membros da organización sobre a posibilidade de recibir correos fraudulentos, especialmente con ocasión da crise do COVID-19, dado que aumentou o número deste tipo de correos. É importante que se lembren os indicios de cando se está ante un correo sospeitoso: faltas de ortografía ou erros de redacción, remitentes non coñecidos, remitentes coñecidos pero contidos con textos, documentos adxuntos ou enlaces non esperados ou sospeitosos, etc. e que, no caso de recibir correos sospeitosos, non abran documentos adxuntos nin páxinas web sospeitosas.

COMUNICACIÓN DE DATOS

Non se deben facilitar datos persoais, bancarios ou outro tipo de dato sensibles cando existen dúbidas sobre a identidade do interlocutor, xa sexa por correo electrónico ou de xeito telefónico.

AUDITORÍA

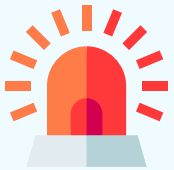
Recoméndanse activar os mecanismos de auditoría de seguridade dos sistemas, en particular dos de seguridade perimetral e dos de acceso ás plataformas de traballo máis sensibles para a organización.

CANLES DE COMUNICACIÓN

Deben definirse as canles de comunicación que se van empregar durante o teletraballo, para evitar riscos na confidencialidade ou o uso de sistemas de comunicación non recomendables. É recomendable contar cunha liña de contacto permanente na que os empregados poidan comunicar calquera incidente ou actividade sospeitosa durante o teletraballo, a fin de detectar posibles incidentes de seguridade ou violacións da seguridade dos datos persoais.

CAMPAÑAS DE CONCIENCIACIÓN E SENSIBILIZACIÓN A EMPREGADOS

É recomendable que de xeito periódico se remitan aos membros da organización recomendacións en materia de seguridade da información, tratamento de datos persoais e ciberseguridade.



PLAN DE CONTINXENCIA

É necesario que se apliquen os plans de continxencia e continuidade do negocio en caso de que estean definidos.

INCIDENTE DE SEGURIDADE E/OU VIOLACIÓN DA SEGURIDADE DOS DATOS PERSOAIS

Lémbrase que persiste a obriga de notificar ás autoridades competentes (Centro Criptolóxico Nacional (CCN) e/ou á Axencia Española de Protección de Datos (AEPD)) a existencia deste tipo de incidentes. Para máis información ao respecto recoméndase visitar as respectivas páxinas web https://www.ccn-cert.cni.es/ e https://www.aepd.es/es

RECOMENDACIÓNS ESPECÍFICAS RESPECTO AO COVID-19:

Teña especial coidado ante estes posibles intentos de engano:

- Preste especial atención aos correos electrónicos que recibe. A cura do coronavirus non a recibirá por correo electrónico.
- Evite abrir documentos e arquivos adxuntos sobre o COVID-19 nos correos electrónicos que reciba, salvo que estea absolutamente seguro de que son lexítimos.
- Non descargue aplicacións non oficiais para coñecer o alcance internacional do COVID-19.
- No relativo á desinformación, teña en conta o seguinte:
    - Evite difundir información que non proveña de medios e fontes oficiais.
    - Non contribúa á difusión de contido non contrastado.
    - Non comparta mensaxes que poidan xerar alarma na poboación.

amtega
Axencia para a Modernización Tecnolóxica

XUNTA DE GALICIA