agesic

Uruguay **Presidencia**

Recomendaciones para teletrabajo y continuidad operativa

Versión 1.1

Objetivo del documento

Este documento tiene por objetivo presentar recomendaciones y buenas prácticas para implementar opciones de teletrabajo en los organismos públicos. Ofrece un abordaje rápido para facilitar y mejorar las operaciones de las organizaciones que se estén viendo afectadas por la pandemia de coronavirus Covid-19.

Público al que se dirige

Está dirigido a perfiles técnicos y vinculados a áreas de TI de organismos públicos.

Introducción

Es importante distinguir entre el teletrabajo y una ocasión particular en la que se trabaja durante un período corto desde un lugar externo a la organización para realizar una tarea puntual.

La Organización Internacional del Trabajo (OIT) define el teletrabajo como una forma de trabajo que se realiza en una ubicación alejada de una oficina central o instalaciones de producción, separando al trabajador del contacto personal con colegas de trabajo que estén en esa oficina. Las nuevas tecnologías hacen posible esta separación, facilitando la comunicación. Una persona trabaja en esta modalidad cuando está por períodos prologados de tiempo trabajando desde un lugar fuera de su oficina.

El teletrabajo implica la necesidad de contar con mayor información, cuando por defecto esta no es gestionada dentro de un ambiente controlado. De esta forma, para que la persona pueda realizar su trabajo, deberá acceder continuamente a información y sistemas que muchas veces tienen un alto grado de sensibilidad y no están expuestos a Internet. Esto requiere el uso de determinadas tecnologías y prácticas que aseguren la confidencialidad, integridad y disponibilidad de la información.

Cuando una persona se lleva un breve trabajo corto para finalizar en un lugar externo a la oficina, la situación es diferente, asumiendo que no será necesario obtener información interna mientras se está trabajando fuera de la oficina. Este caso no es considerado teletrabajo y los riesgos disminuyen. Una de las principales características es que, por la naturaleza del trabajo, si la persona se lleva el material que necesita, no necesita acceder a información o sistemas internos a la organización para finalizar su trabajo. Es muy importante tener en cuenta de qué forma se llevará esta información.

En ambos casos siempre es importante tener en cuenta las políticas para la gestión de la Seguridad de la Información definidas en la organización, pero las necesidades y características pueden cambiar en función de cada situación.

Las recomendaciones y buenas prácticas mencionadas a continuación no pretenden ser exhaustivas, ni cubrir todas las aristas asociadas. Fueron pensadas para un abordaje rápido con el propósito de facilitar y mejorar rápidamente las operaciones de las organizaciones que se estén viendo afectadas por la pandemia de coronavirus Covid-19.

A continuación, se detallan algunas recomendaciones para tener en cuenta para cada una de estas situaciones:

1. Cuando una persona realiza un trabajo puntual desde fuera de la organización, por lo que no necesita acceder a información o sistemas internos.
2. Teletrabajo, es decir, cuando la modalidad de trabajo remoto es la modalidad por defecto de la persona y, por lo tanto, necesita acceder desde afuera a información y sistemas internos de la organización.

Recomendaciones para trabajos esporádicos desde un lugar externo a la organización

Antes de salir de la organización es importante tener en cuenta la información que se necesitará para terminar el trabajo. Asumiendo que esta información es reducida en cantidad y ocupa poco espacio, una opción es enviársela por correo, utilizando siempre la cuenta de la organización o algún repositorio en la nube que la organización tenga disponible.

Estas formas tienen ciertas limitaciones, sobre todo en capacidad, pero asumiendo que la solución de correo o repositorio en la nube utilizada por la organización sea segura, puede ser práctica para una ocasión como esta.

Otra posibilidad es almacenar la información en un medio físico como, por ejemplo, un pendrive. En ese caso, es importante cifrarla para evitar problemas en caso de que el medio físico sea extraviado.

En lo que respecta al equipo y la conexión que se utilizarán en el lugar externo a la oficina, es importante tener en cuenta lo siguiente:

- Mantener actualizados los dispositivos.
- Tener antivirus instalado.
- Preferentemente, no utilizar redes públicas.
- Habilitar el borrado remoto para poder eliminar la información ante pérdida de los dispositivos.

Teletrabajo

Algunas organizaciones ya están habituadas a esta forma de trabajo, mientras que otras quizás lo estén evaluando. Por ello, se plantean a continuación algunas pautas a considerar a la hora de implementar el teletrabajo en una organización.

Uso seguro

Debido a que se estará accediendo a los servicios e infraestructura de la organización desde lugares potencialmente inseguros y/o fuera de nuestro control, es recomendable implementar las siguientes buenas prácticas como mínimo:

- Utilizar VPN seguras.
- Utilizar contraseñas seguras y, en la medida de lo posible, con doble factor de autenticación.
- Mantener actualizados los dispositivos de teletrabajo.
- Instalar antivirus en los dispositivos de teletrabajo.
- Preferentemente, no utilizar redes públicas.

Ver documento “Anexo I – Uso de VPN”, para ampliar información.

Escritorio remoto

Pueden existir ocasiones en las que el acceso remoto por VPN no sea suficiente; de manera conjunta al uso de VPN, se puede utilizar el escritorio remoto.

El protocolo de escritorio remoto o RDP (por sus siglas en inglés), permite a un usuario acceder de forma remota a su estación de trabajo a través de la red. De esta forma, se puede utilizar un equipo corporativo desde cualquier equipo conectado remotamente a una red interna.

Es importante resaltar que RDP ha presentado múltiples vulnerabilidades conocidas, por lo que es se debe evitar exponerlo a internet. Se recomienda acceder a la organización por un canal seguro (por ejemplo VPN) y luego dentro de éste acceder al escritorio remoto. También es importante configurarlo con los permisos mínimos de acceso sobre el equipo servidor.

En cuanto a la experiencia de usuario, es válido mencionar que la calidad y la velocidad de visualización que haya en el escritorio remoto son una combinación entre la velocidad de internet de origen y la velocidad de internet del destino.

Cuidado de la información

Además de los requisitos anteriores, es importante tener en cuenta los siguientes:

- Cifrar la información que pueda ser sensible.
- Realizar respaldos periódicos.
- Habilitar el borrado remoto para poder borrar la información ante pérdida de los dispositivos.

Es importante tener en cuenta la sensibilidad de la información que se está gestionando para tomar las medidas mínimas necesarias.

Canales de comunicación

Es fundamental mantener una comunicación fluida entre los equipos de trabajo. Por ello, es recomendable:

- Definir los canales de comunicación entre el personal (incluir mensajería, chat, videoconferencia, otros.)
- Tener a disposición una lista de contactos claves dentro de la organización.
- Definir voceros oficiales para la comunicación interna.

Ver documento “Anexo II – Recomendaciones de plataformas” para ampliar información.

Recomendaciones para la continuidad de las operaciones

El plan de continuidad del negocio (BCP) no solo apunta a la continuidad de las operaciones tecnológicas, sino también a la continuidad de todos los procesos operativos de la organización.

Si tenés un BCP, es buen momento para probarlo y ver que se ajusta; de esta manera, si realmente se necesita utilizar, no habrá sorpresas.

Si aún no contás con un BCP, hacé algunas preguntas. ¿Qué pasa si falta el 10% del personal que atiende al público? ¿Cómo se continúa operando si el principal sistema informático de la organización se cae? ¿Cuál es la política de respaldos? ¿Se está respaldando bien?

Algunos otros aspectos que se deberán contemplar:

<u>Atención a usuarios</u>
a. Identificar todos los canales de atención a usuarios.
b. Si existen líneas telefónicas, establecer mecanismos de desvió para atención remota.
c. Determinar número mínimo de personas para cubrir el servicio.

<u>Operación interna de la organización</u>
a. Establecer los mecanismos para continuar brindado los servicios con los niveles de servicio habituales.

b. Conocer los planes de continuidad de servicios de los proveedores críticos.
c. Identificar personal clave y su contingente.
d. Comité de crisis. Establecer quiénes serán los responsables de la toma de decisiones (titulares y alternos).
e. Campaña antiphishing para personal. Se deben evitar la desinformación y los incidentes de ciberseguridad. Aquí se pueden encontrar materiales de concientización para utilizar libremente: https://www.gub.uy/centro-nacional-respuesta-incidentes-seguridad-informatica/campana-seguro-te-conectas

Documentación de interés

A continuación, se listan diversas fuentes que permitirán ampliar conocimiento, recursos e información en el abordaje del teletrabajo y las diversas medidas que se podrán adoptar para la continuidad de las operaciones.

Marco de ciberseguridad de Uruguay
Marco de Ciberseguridad
Enlace: https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/marco-ciberseguridad

Políticas
En particular, políticas para acceso remoto y dispositivos móviles
Enlace: https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/marco-de-ciberseguridad-anexo-i-politicas

Plantillas
En particular, Plan de Continuidad de Negocio (BCP) y Plan de Recuperación ante Desastres (DRP).
Enlace: https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/marco-de-ciberseguridad-anexo-ii-plantillas

NIST
SP 800-46 Rev. 2: Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security
Enlace: https://csrc.nist.gov/publications/detail/sp/800-46/rev-2/final

SANS

Tips to secure your organization in a work-from-home environment.

Enlace: https://www.sans.org/blog/tips-to-secure-your-organization-in-a-work-from-home-environment/

Modelos de políticas de seguridad.

Enlace: https://www.sans.org/security-resources/policies/

En particular, se puede consultar:

General - Pandemic Response Planning Policy

Enlace: https://www.sans.org/security-resources/policies/general#pandemic-response-planning-policy

Network security - Remote Access Policy

Enlace: https://www.sans.org/security-resources/policies/network-security#remote-access-policy

Microsoft

Microsoft Windows implementa el escritorio remoto, aquí unas guías de cómo se configura RDP

Enlaces:
https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/clients/remote-desktop-allow-access
https://support.microsoft.com/en-us/help/4028379/windows-10-how-to-use-remote-desktop
https://support.microsoft.com/en-us/help/17463/windows-7-connect-to-another-computer-remote-desktop-connection

Contacto

Por dudas, consultas o asesoramiento respecto a esta documentación: soporte@agesic.gub.uy