CONSIDERACIONES DE TECNOLOGÍA Y SEGURIDAD DE LA INFORMACIÓN AL MOMENTO DE IMPLEMENTAR TELETRABAJO EN LAS INSTITUCIONES GUBERNAMENTALES

ANTECEDENTE

Ante la situación de salud que vivimos actualmente por la presencia del virus COVID-19, una de las medidas preventivas para evitar el contagio es limitar la aglomeración de personas. En nuestras instituciones gubernamentales tenemos personal que puede estar expuesto al momento de la movilización de sus hogares al trabajo y viceversa, lo que podría aumentar la posibilidad de contagio en la sociedad.

Por ello en diversos países han aplicado la opción laborar bajo la modalidad de teletrabajo. En Panamá, el pasado 18 de febrero el Presidente de la República, sancionó la Ley 126 de 18 de febrero de 2020 que establece y regula el teletrabajo en la República de Panamá.

OBJETIVO

Proporcionar recomendaciones que sirvan como guía rápida y efectiva de herramientas y consejos de seguridad para la implementación del teletrabajo en las instituciones gubernamentales.

MEDIDAS DE SEGURIDAD PARA EL TELETRABAJO

1. CONEXIONES A REDES DE LA INSTITUCIÓN POR MEDIO DE VPN

De sus siglas en ingles *Virtual Private Network*, es una solución que nos permite acceder de forma remota a una red institucional como si estuviéramos físicamente en el sitio.

Se utiliza un canal de comunicación segura entre el equipo portátil corporativo y la red de la institución. Para el establecimiento de la comunicación será necesario validar la identidad del equipo, es decir, confirmar que se trata de un equipo informático de la institución, por ejemplo, estableciendo la comunicación VPN mediante autenticación con certificado de máquina. Puede ser la opción más habitual de conexión y conviene tener varias medidas para comprobar los requisitos de conexión. Las medidas de validación de acceso deben ser revisadas para que no se produzcan duplicidades de acceso o se conozca la dimensión de estos. Las medidas para registrar las actividades de los usuarios, así como el registro de las conexiones, son muy importantes para evitar posibles incidentes o facilitar su investigación.

Estas VPN deberán ser de punto a punto entre el firewall o Concentrador de VPN de la Institución y el equipo del cliente (celular/computador asignado al funcionario). Para el establecimiento de dichas VPN se utilizarán protocolos seguros como IPSec o TLS 1.2 o superior. Proveerán autenticación *extremo a extremo*, basada en la utilización de certificados digitales, protección de la integridad y, en el caso de que se maneje información sensible, protección de la confidencialidad.

Al finalizar de realizar las tareas requeridas, se debe desconectar de la sesión de VPN, con la finalidad de no mantener una conexión innecesaria, liberar recursos y mantener la disponibilidad del servicio.

Esta debe ser la única forma de acceder a recursos de la institución como servidores de archivos, SharePoint, sistemas o servicios institucionales, salvo aquellos definidos por la Dirección de Tecnología de la Institución. En ninguna circunstancia estos recursos deben ser publicados y accedidos directamente desde el Internet.

2. EQUIPO CLIENTE (CELULAR / COMPUTADOR)

El equipo *cliente* será el medio proporcionado por la Institución para ser utilizado en el teletrabajo, este equipo deberá cumplir con todas las medidas de seguridad estándar definida por la Institución.

Se recomienda que el equipo cliente cuente con un agente de "*endpoint security*" (Antivirus), preferiblemente administrado de forma centralizada por la Institución.

Estas herramientas deberán actualizarse con una periodicidad establecida por la política de seguridad de la Institución. El equipo cliente deberá contar con las medidas de seguridad establecidas por defecto para cualquier equipo de la Institución en caso de no ser el de uso habitual.

- **Medidas Hardware**
  - Se recomienda que el BIOS/UEFI sea protegido con contraseña fuerte y configurada de acuerdo al principio de mínima funcionalidad.
- **Medidas del sistema operativo**
  - Autenticación mediante Directorio Activo, aplicando políticas de contraseñas definidas por la Institución.
  - Utilización de doble factor de autenticación.
  - Se debe bloquear el equipo tras intentos fallidos de autenticación consecutivos o después de un período corto de inactividad.
  - El Sistema operativo debe contar con soporte y parches de seguridad actualizados.
  - Únicamente se podrá administrar el sistema desde un usuario administrador.
  - Se debe contar una configuración que restrinja y controle la ejecución de software de acuerdo con las políticas de la institución.
- **Herramientas de seguridad**
  - **Herramientas antimalware:** El software de detección de código dañino deberá configurarse para:
    - Analizar todo archivo procedente de fuentes externas antes de trabajar con este.
    - Revisar el sistema cada vez que arranque y realizar escaneos regulares para detectar software malicioso.
    - Actualizar periódicamente las firmas.

  - Implementar protección en tiempo real de acuerdo a las recomendaciones del fabricante.
- **Firewall personal:** Se utilizará un cortafuego personal que permita únicamente los flujos de comunicación autorizados conforme a las políticas de la institución y rechace el resto**.**
- **HIPS (Host Intrusion Prevention):** Se debe contar con un sistema para la prevención de intrusiones (HIPS) con el fin de detectar y bloquear en tiempo real cualquier intento de intrusión en éste. El conjunto de reglas predefinidas y patrones de firma utilizados para detectar posibles ataques deberán ser personalizados y actualizados periódicamente conforme a la Política de Seguridad de la Institución.
- **Gestión de eventos:** Se utilizarán mecanismos para el registro de bitácoras (*logs*) y eventos de seguridad generados por el sistema y/o los usuarios, que puedan ser almacenados y retenidos durante el período que establezca la Política de Seguridad establecida en la Institución.
- **Cifrado de datos:** Se recomienda aplicar mecanismos criptográficos para la protección de la confidencialidad e integridad de la información de los sistemas que almacenen información sensible. Concretamente, estos mecanismos serán:
  - Cifrado fuera de línea (offline): para la protección de la información sensible que vaya a ser enviada por o almacenada en un medio inseguro.
  - Cifrado en reposo (data almacenada): deberá utilizarse siempre que la solución de dispositivo final (*endpoint*), sea móvil o portátil, para sistemas que guarden información sensible.
  - Cifrado de Disco Duro de las estaciones de trabajo.
- **Prevención de Fuga de Datos (DLP):** siempre que sea posible, para sistemas que manejen información sensible, se aplicarán mecanismos que permitan monitorizar y controlar la salida de data desde el sistema, que haya sido previamente definida como sensible.
- **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 para el tipo de soporte en donde se encuentre almacenada. El mecanismo de borrado seguro utilizado podrá consistir en una o varias pasadas de sobrescrita o el cifrado de la información.

3. ESTRATEGIA DE COMUNICACIÓN

Si se plantea un escenario en el que los usuarios puedan acceder a salas de reuniones y conferencias de forma virtual desde equipos informáticos gestionados y no gestionados por la institución a través de Internet, se debería revisar las actualizaciones de seguridad correspondientes y aplicarse en caso de ser necesario. Algunos consejos importantes en relación a este punto son los siguientes:

1. Tener un listado de servicios acordados para mantener reuniones de forma virtual, conocer las licencias de las que se disponen o si se van a utilizar herramientas gratuitas.

2. Tener controlados los accesos a la red y sistemas de la Institución, además de tener la posibilidad en los dispositivos perimetrales de habilitar reglas con fecha y hora de inicio y finalización de la reunión.
3. Revisar que los asistentes son los invitados y no se tienen duplicados, personas no invitadas o desconocidas en la reunión.
4. Verificar si la reunión es grabada, que quede registro de las personas conectadas, donde se almacena y que personas pueden grabar la reunión dentro de la misma.
5. Tener listados telefónicos de fácil acceso para comunicarse con las diferentes personas.

Si en su institución no cuentan con herramientas propias para realizar este tipo de comunicación cómo MyUC, deberá evaluar herramientas que permitan colaborar con equipos de trabajo, y que se adecue a los requerimientos de las Institución.

4. RECOMENDACIONES GENÉRICAS PARA ADMINISTRADORES

Al aplicarse teletrabajo en su institución es importante que no bajen la guardia y sean más precavidos al momento realizar sus labores diarias. Algunos consejos o medidas genéricas de protección de seguridad que deben considerar:

- Tener instaladas las últimas actualizaciones del sistema operativo.
- Tener activados servicios de monitorización con alertas definidas.
- Revisar los registros y auditorías de las conexiones remotas.
- Restringir montar unidades mapeadas del organismo en equipos remotos inseguros.
- Evitar las opciones de “Split-Tunneling” en equipos inseguros o que no cumplan todas las medidas de seguridad.
- Asegurar que los sistemas de antivirus realicen la tarea de escaneo de los dispositivos USB conectados a los equipos remotos y si es necesario bloquear el acceso de USB en dichos equipos.
- Cumplir con las medidas de seguridad de la institución como políticas, normativas y procedimientos de seguridad.
- Tener listados de personas, direcciones IP, teléfonos, correos electrónicos corporativos y alternativos relacionados con el acceso a los sistemas de forma remota.
- Tener actualizado el listado de personas que pueden acceder remotamente a los equipos de la organización con la dirección IP de acceso y medio de conexión.

5. MEDIDAS DE SEGURIDAD PARA USUARIOS

Es importante que cuenten con mucha precaución y siempre colaborar con el equipo de soporte técnico, explicando de manera confiable y exacta las dudas e inconvenientes que puedan surgir en el proceso, algunas recomendaciones son:

- El usuario de la Institución es responsable de custodiar las credenciales de acceso a las distintas herramientas de tecnología a las que tenga acceso. Asegúrese de resguardar su nombre de usuario y contraseña de manera segura, evitando anotar esta información en un medio que pueda ser accedido por terceros.
- Si detectas cualquier actividad sospechosa o un funcionamiento anómalo de tu equipo avisa al departamento de tecnología de la Institución.
- Mantener la confidencialidad de la Institución, no debemos revelar información de carácter confidencial.
- Evitar acceder a sitios fraudulentos para descargar malware o sitio para efectuar el fraude mediante el robo de información.
- Notificar los incidentes de seguridad, ante situaciones como emails sospechosos o comportamientos anómalos del sistema a CSIRT Panamá mediante info@cert.pa.
- Sé cauto y asegúrate de compartir estos consejos con tus compañeros de trabajo.
- Promover la cultura en ciberseguridad en especial ante la medida del teletrabajo.

Consejos de seguridad para los usuarios en relación al manejo del correo electrónico:

- Utilizar el correo Institucional responsablemente. No debe ser utilizado para conversaciones que no estén asociada a sus actividades laborales. No utilice el correo Institucional para fines personales.
- Verificar la veracidad de la identidad remitente.
- No proporcionar información personal o de la Institución a desconocidos por ningún medio que produzca desconfianza, recuerde verificar el remitente.
- Si no esta seguro del remitente del correo, no abras o descargues sus adjuntos. Comuníquese con el departamento de tecnología de su Institución.
- Precaución ante correos de mensajes de urgencia, o aprovechándose de la situación actual de salud, consultando información por medio telefónico, por mensaje de texto, por mensajería instantánea de redes sociales, o por su correo personal o de la organización

ÚLTIMAS CONSIDERACIONES

La modalidad de teletrabajo abarca muchos departamentos y procesos. La Autoridad Nacional para la Innovación Gubernamental recomienda tomar en consideraciones las siguientes acciones al momento de iniciar la modalidad de teletrabajo en su Institución:

1. Determine la elegibilidad de los funcionarios que puedan realizar teletrabajo. Entre los factores a considerar se puede mencionar:
    - Facilidad de conexión a Internet desde el sitio de teletrabajo del servidor público.
    - Funciones y responsabilidades del servidor público.

- Grado de responsabilidad e integridad del servidor público.

2. Definir herramientas aprobadas para realizar laborares en modalidad teletrabajo y sus requerimientos técnicos. Algunas herramientas a considerar son: correo electrónico institucional, llamadas telefónicas por medio de VoIP, conexión VPN.
3. Definir un acuerdo de teletrabajo por escrito para labores de manera remota.
4. El servidor público debe hacer uso de un equipo asignado por la Institución. El servidor público deberá llenar un formulario que autorice la salida del bien de la Institución.
5. Establezcan reglas a seguir al momento de realizar teletrabajo. Por ejemplo:
    - La modalidad de teletrabajo aplica para el personal que, de acuerdo a sus funciones y cargo, puede adoptar de manera eficiente esta modalidad.
    - Cada *Director* o *Jefe Inmediato* determinará si el personal puede acogerse a esta modalidad.
    - El personal que se acoja a la modalidad de teletrabajo, tiene que entregar informe semanal a su jefe inmediato de las funciones realizadas, cumpliendo con el horario de la Institución.
    - Si el jefe inmediato por razones laborales, requiere la presencia del servidor público, el mismo debe acudir a las oficinas de la Institución. Se debe establecer un tiempo considerable para que el funcionario pueda trasladarse hacia las oficinas de la Institución.
    - Prohibir la salida de documentación física de la Institución.
    - Se debe coordinar y realizar una inducción, en la que le expliquen al servidor público cómo se debe laborar en modo teletrabajo y las herramientas definidas para realizar teletrabajo.
    - El servidor público debe leer, llenar el acuerdo que establece y reglamenta la modalidad del teletrabajo, más el formulario para uso de equipo fuera de la oficina.
6. Publicar en el sitio web de su Institución las consideraciones y reglas que contempla su Institución para realizar teletrabajo.