VÍA CORREO ELECTRÓNICO

30 de diciembre de 2020

CARTA CIRCULAR NÚM. 2020-05

A TODOS LOS SECRETARIOS, DIRECTORES Y A LOS PRINCIPALES OFICIALES DE INFORMÁTICA DE LAS AGENCIAS DEL GOBIERNO DE PUERTO RICO

Glorimar Ripoll Balet
Principal Ejecutiva de Innovación e Información, Gobierno de Puerto Rico
Directora Ejecutiva, PRITS

GUIAS PARA ESTABLECER LAS MEDIDAS MINIMAS DE PROTECCION, A LOS FINES DE GARANTIZAR LA CONFIABILIDAD Y CONFIDENCIALIDAD DE LA INFORMACION Y EL USO ADECUADO DE LOS SISTEMAS DE INFORMACION DEL PROGRAMA DE TELETRABAJO

La Ley 75 -2019, conocida como la *"Ley de la Puerto Rico Innovation and Technology Service"* (Ley 75) fue creada con el fin de establecer y promover la política pública sobre la elaboración, manejo, desarrollo, coordinación e integración interagencial efectiva en lo pertinente a la infraestructura tecnológica e informática del Gobierno de Puerto Rico, así como desarrollar de forma ordenada e integrada los proyectos tecnológicos puntuales necesarios para promover la integración efectiva de la tecnología a la gestión gubernamental, entre otros.

Mediante la Ley 75-2019, se crea un nuevo andamiaje de gobierno innovador, atemperado a las exigencias del siglo XXI y capaz de valerse de la tecnología avanzada, para cumplir con las expectativas de la ciudadanía y con los estándares modernos de gobernanza efectiva. La innovación promueve la eficiencia gubernamental, así como un manejo más apropiado de los recursos humanos y físicos, lo que se traduce en un desarrollo económico positivo de Puerto Rico. Es por ello que PRITS evalúa de forma continua todos los mecanismos posibles para mejorar el funcionamiento y eficiencia de las agencias gubernamentales y demás dependencias del Gobierno.

Por otro lado, la Ley 36-2020, conocida como "Ley de Trabajo a Distancia del Gobierno de Puerto Rico", tiene el propósito principal de transformar la manera en que opera el Gobierno de Puerto Rico a una más práctica y efectiva, estableciendo el marco legal para una implementación eficiente del Programa de Teletrabajo en las agencias gubernamentales. El teletrabajo propicia economía operacional, mientras promueve una administración eficiente. Además, propicia la resiliencia al brindar alternativas para mantener en marcha la operación y servicios del gobierno en situaciones de emergencia o no favorables ya que el teletrabajo permite a un empleado ejecutar, toda o parte de sus labores, fuera del área regular de oficina.

A raíz de la situación global relacionada a la pandemia del COVID-19, el Gobierno de Puerto Rico ha tomado medidas para atemperar la realidad operacional de sus funciones, así como contribuir a la utilización efectiva de los recursos económicos y fiscales, protegiendo a su vez a la empleomanía, buscando crear un ambiente de trabajo seguro y libre de riesgos.

Base Legal

Esta Carta Circular se promulga en virtud de las facultades delegadas al PRITS, conforme la Ley 75. En virtud del inciso (a) del Artículo 6 de la Ley, el PRITS está facultado para implantar, desarrollar y coordinar la política pública del Gobierno sobre la innovación, información y tecnología. Por su parte, el inciso (w) del mismo artículo dispone que el PRITS establecerá e implementará los planes estratégicos, las políticas, estándares y la arquitectura integrada de las tecnologías de información y telecomunicación del Gobierno. Además, el Artículo 7, inciso (3) faculta al PRITS a emitir órdenes administrativas, opiniones y/o cartas circulares.

Por otra parte, la Ley 36-2020, en su Artículo 8, faculta al PRITS de emitir las guías que cada Agencia y demás dependencias gubernamentales deberán adoptar en torno a las medidas mínimas de protección, a los fines de garantizar la confiabilidad y confidencialidad de la información y procurar por el uso adecuado de los sistemas de información a través del teletrabajo.[1]

Propósito y Alcance

Esta Carta Circular tiene como propósito establecer las guías que contemplan las medidas de protección que cada Agencia y demás dependencias gubernamentales deberán adoptar en torno a los aspectos de tecnología y seguridad de la información para la modalidad del teletrabajo. Esto con el propósito de garantizar la confiabilidad y confidencialidad de la información, así como procurar el uso adecuado de los sistemas de información.[2]

[1] Se recomienda la lectura de la Ley 36-2020 en conjunto con esta carta circular para fines de disipar cualquier interrogante relacionada.

[2] Ver Art. 8 Ley 36-2020

Aplicabilidad

Esta Carta Circular será aplicable a todas las Agencias, según definidas en la Ley 75 y es de estricto cumplimiento.

Medidas para el Programa de Teletrabajo

Cada Agencia, y su Oficial Principal de Informática (OPI), será responsable de la implementación del Programa de Teletrabajo mediante un plan que considere las exigencias operacionales de la Agencia y de cada empleado participante del Programa.

De conformidad con el Articulo 13 de la Ley 75, el OPI de cada Agencia es responsable de cumplir e implementar las políticas, protocolos, y guías establecidas por el PRITS. A esos efectos, será su responsabilidad el velar por el fiel y estricto cumplimiento de las disposiciones contenidas en esta carta circular por medio de auditorías, capacitación y orientación de los procesos a ser efectuados, entre otros aspectos. De encontrar algún tipo de desviación en torno a los procesos y requerimientos establecidos, será su obligación referir el mismo para el trámite correspondiente, dependiendo de la situación.

Se reconoce la diversidad de labores de los empleados gubernamentales, por lo que cualquier excepción se hará con la evaluación y autorización del OPI de la Agencia. De entender necesario, podría consultarse con el PRITS.

Será responsabilidad de cada Agencia y su OPI procurar que cada empleado posea las destrezas básicas del uso de la computadora, los sistemas, y las plataformas digitales de colaboración y comunicación de la Agencia. De lo contrario, el empleado debe tomar los adiestramientos necesarios para la utilización de los sistemas necesarios para el teletrabajo. Igualmente, debe siempre promoverse una comunicación efectiva en caso de que el empleado necesite asistencia técnica durante la vigencia del teletrabajo.

Además, se recomienda la adquisición, configuración y distribución de equipos y herramientas que faciliten el teletrabajo y cumplan con los fines de garantizar la seguridad de la información y de los sistemas del gobierno. Las *laptops* o *desktops* deben tener capacidad suficiente para ejecutar adecuadamente todas las aplicaciones necesarias para las funciones del empleado. Antes de entregarse, los equipos deben tener todas las instalaciones y configuraciones requeridas para lograr efectivamente los propósitos de estas guías.

En términos de la conectividad, el empleado debe contar con servicio de Internet de banda ancha, que le permita navegar a una velocidad alta y estable, apropiado para sus funciones de manera que estas no se vean interrumpidas.

A continuación, se detallan las guías mínimas requeridas a los fines de garantizar la confiabilidad, confidencialidad de la información y procurar por el uso adecuado de los sistemas de información a través del teletrabajo a ser establecido por cada Agencia:

A. Controles del acceso a la información de la Agencia y los sistemas de información

Responsabilidades del Oficial Principal de Informática de la Agencia

1. Proveer a todo empleado bajo el Programa de Teletrabajo un correo electrónico oficial a través del estándar de dominio de PR.GOV establecido por PRITS con el formato @agencia.pr.gov.

2. Llevar un registro sobre los accesos a los diversos sistemas que cada empleado requiere para ejercer sus funciones mediante el Programa de Teletrabajo.

3. Promover y facilitar que cualquier comunicación o manejo de documentos pertinente a las funciones y tareas del empleado se haga a través de las herramientas digitales de manejo de documentos, de comunicación y de colaboración oficiales de la Agencia. Esto incluye las herramientas web-based bajo la subscripción de Office 365, como Outlook, Teams, SharePoint, OneDrive, entre otras.

4. Configurar las reglas de seguridad para proteger la información y los sistemas utilizados por los empleados, especialmente los que requieren acceso remoto a sistemas internos del gobierno. Dichas reglas deben incluir la administración de los servidores y aplicaciones de servicios críticos de la Agencia a través de acceso remoto. El acceso a sistemas internos debe siempre configurarse utilizando un *virtual private network* (VPN) para establecer una conexión segura a través de un túnel virtual encriptado entre el cliente y la aplicación.

5. Asegurarse que las aplicaciones administrativas de importancia para la Agencia, como son las utilizadas por las áreas de Finanzas, Presupuesto, Recursos Humanos, entre otras, estén protegidas por un *firewall* y solamente los usuarios autorizados puedan acceder dichas aplicaciones.

6. Configurar y exigir la utilización del *multi-factor authentication* (MFA) para acceder los diversos sistemas requeridos para las funciones del empleado, en la medida que esta funcionalidad esté disponible. En el caso específico de la subscripción de Office 365, ésta debe accederse siempre utilizando MFA, preferiblemente mediante el Microsoft Authenticator App.

7. Requerir el uso de los sistemas electrónicos, computadoras portátiles, equipos de telecomunicaciones y otros recursos que sean propiedad, estén administrados y protegidos bajo los protocolos establecidos por la Agencia. No se recomienda el uso de dispositivos electrónicos personales para propósitos del teletrabajo.

8. De permitir y ser autorizado el uso de dispositivos electrónicos personales, se debe desarrollar una política de *Bring Your Own Device* (BYOD) que contemple el manejo de los accesos y los equipos permitidos en la organización.

Responsabilidades del Empleado

1. El empleado debe mantener y proteger sus credenciales de acceso a todas sus cuentas para acceder los diversos sistemas y redes de la Agencia, incluyendo su correo electrónico oficial.

2. El empleado debe poder llevar a cabo transacciones, correspondencia y cualquier comunicación y trámite de documentos utilizando medios electrónicos; entiéndase, uso de computadoras portátiles, teléfono o móvil, entre otros.

3. El empleado deberá acceder los sistemas y la red de la Agencia a través de la conexión de internet disponible en su hogar, sea una conexión alámbrica, inalámbrica (W*i-Fi*), o a través de su conexión móvil (*hotspot*). Si hubiese la necesidad, a modo de excepción, de utilizar redes inalámbricas públicas, lo cual no es recomendado, será exclusivamente mediante autorización e instrucciones del OPI.

4. El empleado debe poteger sus contraseñas (passwords). Las contraseñas no deben ser fácilmente identificables y deben ser robustas, Ej.: tener de 8 a 12 caracteres mínimo y uso de letras mayúsculas, números y caracteres especiales (¡!@#$%^&|\/{}[]¿?).

B. Protección de la información de la Agencia, incluyendo información del personal

Responsabilidades del Oficial Principal de Informática de la Agencia

1. Establecer procedimientos pertinentes a la permanencia, accesibilidad, seguridad, confidencialidad y resguardo de toda información e interacción producto de las labores del empleado. Esto incluye establecer un mecanismo para asegurar el resguardo (*backup*) de todas las comunicaciones, documentos, expedientes del empleado, según determinado por las políticas de la Agencia u otras políticas aplicables.

2. Orientar al empleado en asuntos de privacidad y confidencialidad de la información que maneja para evitar los riesgos asociados al envío de archivos y correos electrónicos que contengan información confidencial o sensitiva, como seguros sociales y cuentas bancarias, por mecanismos inseguros. Se deben configurar las herramientas de correos electrónicos, mensajería y colaboración para alertar o prevenir el envío de dicha información.

3. Asegurarse que todas las computadoras facilitadas a los empleados en teletrabajo por la Agencia tengan el disco duro encriptado y no contengan cuenta Admin local, para mantener la seguridad de los datos y la configuración establecida por la Agencia.

Responsabilidades del Empleado

1. Al empleado no se le está permitido a enviar información confidencial o *Personally Identifiable Information* (PII) de ciudadanos, empleados o contratistas, entre otros, tales como seguros sociales y cuentas bancarias, a través de medios electrónicos que no cuenten con los protocolos de seguridad adecuados. Esta información sólo debe enviarse de manera encriptada o a través de las aplicaciones de la Agencia que cuenten con los protocolos necesarios y que fueron asignadas para ese uso según las funciones del empleado.

2. Al empleado no se le está permitido a guardar información relacionada a sus funciones oficiales en equipos personales.

C. Protección de sistemas de información que no estén bajo el escrutinio de la Agencia y que se utilizan en el Programa

Responsabilidades del Oficial Principal de Informática de la Agencia

1. Evaluar y autorizar sistemas de información que no estén bajo el escrutinio del gobierno, según la necesidad expresada por el empleado para lograr sus labores remotas. No debe promoverse el uso de herramientas y aplicaciones fuera del dominio del gobierno, especialmente si existen herramientas bajo el dominio del gobierno que hacen funciones iguales o similares. De ser autorizado su uso, el OPI debe asegurar que el empleado esté orientado en relación con las mejores prácticas para un uso seguro sin poner en riesgo la información y recursos de la Agencia.

Responsabilidades del Empleado

1. El empleado debe solicitar, justificar y recibir autorización por el OPI de su Agencia sobre el uso de sistemas de información fuera del dominio de ésta.

D. Prevención del uso inapropiado del tiempo y del equipo de la Agencia, manteniendo unos estándares altos de calidad y seguridad cibernética

Responsabilidades del Oficial Principal de Informática de la Agencia

1. Coordinar la orientación, capacitación y adiestramiento a los empleados para prevenir el uso inapropiado de los equipos, para fomentar mayor conciencia de

los temas relacionados a la seguridad cibernética y para lograr un trabajo remoto de alta calidad exclusivamente mediante la utilización de herramientas digitales.

2. Establecer métricas que validen la cantidad de tiempo que invierten los empleados en teletrabajo mediante las herramientas de colaboración y video conferencia, al igual que otras métricas que se determinen relevantes para monitorear y asegurar el mejor uso del tiempo y del equipo.

3. Desactivar o desinstalar servicios y programas innecesarios, fomentando un mayor enfoque en las funciones particulares del empleado.

Responsabilidades del Empleado

1. El empleado no puede usar los equipos de la Agencia para fines personales, incluyendo el uso de mensajería y correos electrónicos personales. Tampoco puede utilizar las aplicaciones, herramientas de productividad y navegadores para fines que no sean relacionados a las tareas oficiales asignadas.

2. El empleado no puede compartir los equipos de la Agencia con terceras personas.

E. Limitar e identificar las vulnerabilidades de los sistemas

Responsabilidades del Oficial Principal de Informática de la Agencia

1. Revisar los *Log Files* diariamente, como los SignIn en Office365, conexiones VPN, *Firewall Rules Logs* y el *Usage Report* de TEAMS. Los mismos deben ser resguardados en un archivo digital con una frecuencia mínima semanal.

2. Realizar diagnósticos de las laptops y otros equipos utilizados para el teletrabajo a través de herramientas de acceso remoto y en previa coordinación con el empleado.

3. Asegurar que todo equipo utilizado para el teletrabajo esté configurado con antivirus y otros mecanismos que detecten y eviten la entrada de vulnerabilidades. Además, se recomienda una solución de antivirus que revise el contenido de las descargas.

4. Asegurar que los diferentes programas y sistemas operativos que se encuentren instalados en los equipos utilizados para el teletrabajo se mantengan actualizados. Se debe tener activada la opción de actualización automática.

5. Velar que los equipos asignados no tengan un puerto de USB o lo tengan deshabilitado, no tengan un CD-ROM, ni tengan otros dispositivos externos, para prevenir la transmisión de virus o malware, o la ejecución de programas maliciosos.

6. Orientar a los empleados sobre las características de un correo electrónico sospechoso u otras circunstancias que pueden levantar sospechas con el propósito de identificar y escalar cualquier situación rápidamente, evitando comprometer los equipos, sistemas y redes de la Agencia. Además, debe orientar a los empleados sobre el procedimiento oficial a seguir al detectar la sospecha, incluyendo el notificar la situación. A modo general, se debe orientar en el uso y manejo de la seguridad en las diversas herramientas y aplicaciones.

Responsabilidades del Empleado

1. El empleado no puede impedir que los equipos y programas se actualicen. De necesitar que el equipo se actualice en otro momento, es responsabilidad del empleado dejar el mismo actualizando cuando no esté en uso.

2. El empleado debe notificar inmediatamente al OPI si recibe un correo electrónico sospechoso para que el mismo verifique si se trata de un correo electrónico dañino. No debe abrir los archivos adjuntos sin antes concluir la evaluación requerida.

3. El empleado no puede descargar (*download*) contenido no autorizado por la Agencia. Sólo deberá descargar contenido oficial autorizado y facilitado por la Agencia.

F. Salvaguardar el equipo de la Agencia utilizado para la ejecución del Programa

Responsabilidades del Oficial Principal de Informática de la Agencia

1. Identificar y poseer un inventario de los equipos, computadoras portátiles, programas, licencias u otros recursos que se proveerá a cada empleado para viabilizar el teletrabajo.

2. Autorizar, en coordinación con el encargado de la propiedad de la Agencia, el uso de los equipos para el teletrabajo. Esto debe incluir un registro del equipo y recursos según se entregue el mismo, además de asegurar que el empleado comprende su responsabilidad en proteger el equipo tecnológico o bienes muebles bajo su custodia pertenecientes a la Agencia.

3. Establezca protocolos para proteger los dispositivos de teletrabajo controlados por la Agencia contra riesgos, pérdida o robo.

Responsabilidades del Empleado

1. El empleado debe tener claro que la Agencia es dueña del equipo, aplicaciones y

los datos reteniendo control y propiedad de estos. El equipo, propiedad de la Agencia, se utilizará exclusivamente para asuntos oficiales.

2. El empleado debe tener un espacio dedicado que permita realizar su trabajo eficientemente bajo la privacidad que amerita sus labores y permita mantener el equipo asignado de manera segura y libre de riesgos.

3. El empleado es responsable de notificar inmediatamente al OPI o su representante autorizado, cualquier malfuncionamiento, avería o robo del equipo.

Derogación

Esta Carta Circular deja sin efecto cualquier otra Carta Circular, Memorando, Orden Administrativa, Políticas, Normativas, comunicación escrita o instrucción anterior que en todo o en parte sea incompatible con ésta, hasta donde existiera tal incompatibilidad.

Vigencia

Esta Carta Circular tendrá vigencia inmediata.