Guía para el Trabajo Remoto durante la Pandemia del COVID-19

SAGRADO

Universidad del Sagrado Corazón

Guía para el trabajo remoto durante la Pandemia del Coronavirus (COVID-19)

Tabla de Contenido

Propósito 2
Duración 2
Aplicabilidad y definiciones 3
Asignación de Trabajo Remoto 3
Equipo 3
Comunicación 4
Seguridad de la información 4
Seguridad cibernética (*Cybersecurity*) 5
Seguridad en el teletrabajo y tiempo trabajado 6
Cumplimiento con políticas institucionales 7
Consultas sobre esta guía 8
ANEJO – *Responsabilidades de todos/as los/as empleados/as* 9

Propósito

El propósito de esta guía institucional es crear las bases de confianza y reglas necesarias para flexibilizar el lugar desde donde realizarán su trabajo los/as empleados/as administrativos/as y los/as empleados/as docentes de la **Universidad del Sagrado Corazón.**

El trabajo remoto, también conocido como teletrabajo o trabajo a distancia (*telecommuting* en inglés) permite a los/as empleados/as trabajar en un lugar alejado de las instalaciones de la universidad, como por ejemplo desde su casa o en una ubicación satelital, durante toda o parte de su semana laboral, mediante la utilización de las tecnologías de la información y la comunicación.

La **Universidad del Sagrado Corazón** considera que el trabajo remoto puede ser apropiado para algunos/as empleados/as, pero no para todos ni todas. A tales efectos, reconocemos que no todas las funciones esenciales podrán realizarse remotamente. El trabajo remoto es un acuerdo temporero para ciertas funciones y de ninguna manera cambia las expectativas que se tienen de la posición, ni los términos y condiciones de empleo con la institución. Por consiguiente, continúan con vigencia las demás políticas y normas de la institución, incluso las de recursos humanos y las de su área de trabajo.

El trabajo remoto es una modalidad como excepción a la regla de trabajo regular en la Universidad del Sagrado Corazón. Actualmente, el mismo se está utilizando exclusivamente en casos de distanciamiento social y como mecanismo necesario para brindar continuidad a los servicios que brindamos. Este mecanismo será utilizado por un periodo de tiempo limitado y por la situación extraordinaria de la pandemia del COVID-19 que afecta a todo Puerto Rico. Esta concesión temporera de trabajo remoto no crea un derecho a que este arreglo se haga en el futuro.

Este tipo de acuerdo de trabajo requiere de un alto grado de disciplina por parte de los/as empleados/as y sus supervisores/as, por lo que, de buena fe, tanto la **Universidad del Sagrado Corazón** como los/as empleadas participantes pondrán todo su empeño para que el mismo funcione adecuadamente. La buena comunicación es esencial para el éxito de estos arreglos.

Duración

Cualquier acuerdo o asignación de trabajo remoto será a modo de emergencia y su duración está sujeta a los acontecimientos de la pandemia del COVID-19, las Órdenes Ejecutivas que emita el Gobierno del Estado Libre Asociado de Puerto Rico y las decisiones institucionales. La **Universidad del Sagrado Corazón** puede dejar sin efecto en cualquier momento el acuerdo de trabajo remoto. Se hará todo lo posible para proporcionar un aviso previo razonable para dicho cambio, pero puede haber casos en los que no sea posible proveer tal aviso.

Aplicabilidad y definiciones

Esta guía aplica a los/as empleados/as administrativos/as y docentes identificados, a discreción de la universidad, como elegibles para realizar trabajos remotos. A continuación, se brindan definiciones de aplicabilidad:

1. **Empleados/as administrativos/as**. El personal a tiempo completo y tiempo parcial que usual y regularmente trabaja en oficinas de servicios y labores de apoyo gerencial incluso empleados por propuesta.

2. **Empleados/as docentes-administrativos**. Los/as profesores/as a tiempo completo que se descargan un máximo de 15 créditos para ocupar un puesto de naturaleza administrativa. Mientras ocupen la posición, conservarán su estatus de profesores/as y los beneficios que le acompañan. Podrán considerarse para acenso en rango siempre y cuando cumplan con los requisitos identificados en el Manual de Evaluación y Ascenso en Rango de la Facultad.

3. **Empleados/as docentes**. El personal de la Universidad con rango académico o su equivalente que realiza funciones de enseñanza, dirección o coordinación de actividades académicas o de apoyo a la gestión institucional, a saber: profesor/a con rango en la sala de clases, personal con rango en tareas administrativas, bibliotecarios/as, y profesores/as del Programa de Apoyo al Estudiante.

Asignación de Trabajo Remoto

La **Universidad del Sagrado Corazón** podrá realizar asignaciones de trabajo remoto de conformidad con la necesidad operacional.

Equipo

Según el caso, la Universidad determinará, con la información suministrada por el/a empleado/a y su supervisor/a, las necesidades de equipo apropiadas (incluyendo *hardware, software, módems*, líneas telefónicas y de datos y otros equipos de oficina) para cada arreglo o asignación de trabajo remoto. La unidad de Desarrollo Organización y Recursos Humanos (DORH) y la unidad de Informática y Tecnología Integrada (ITI) servirán como recursos de ayuda para los/as empleados/as participantes. Estos/as deberán cuidar de cualquier equipo asignado y coordinar cualquier necesidad de servicio o mantenimiento con estas unidades.

La **Universidad del Sagrado Corazón** no acepta ninguna responsabilidad por daños o reparaciones a los equipos propiedad de los/as empleados participantes. De permitirse el uso de una computadora personal, el/la empleado/a deberá utilizar la cuenta de correo electrónico institucional separada del resto de las cuentas personales. El equipo suministrado por la Universidad se debe utilizar solo con fines de trabajo, y bajo ninguna circunstancia será utilizado para hacer trabajos de otra organización o asunto personal. La Universidad se reserva el derecho de hacer auditorías a los equipos provistos para asegurar

su buen uso. El/la empleado/a que trabaje de forma remota debe firmar un inventario de todos los bienes de la Universidad recibidos y aceptar tomar las medidas apropiadas para proteger dichos bienes contra daños o robos. De finalizar el empleo, todos los bienes de la Universidad serán devueltos.

Los empleados/as participantes deben tener un ambiente de trabajo apropiado dentro de su hogar o lugar de trabajo remoto para fines laborales. La universidad no será responsable de los costos asociados con la configuración de tales espacios como los costos de muebles, iluminación, reparaciones o remodelaciones, entre otros.

Comunicación

Cada área de trabajo establecerá sus objetivos de trabajo, incluyendo los del trabajo remoto. Es importante establecer y mantener canales de comunicación para aclarar cualquier duda sobre estos objetivos y cómo alcanzarlos. Se recomienda acordar la frecuencia y horarios de las comunicaciones y los medios de comunicación a utilizar.

Los mecanismos de comunicación autorizados por la Universidad serán instalados por la unidad de ITI y se adiestrará a quienes requieran algún tipo de adiestramiento para el uso de estos. A continuación, se detallan:

- Correo electrónico institucional (No se autoriza utilizar correos electrónicos personales)
- *Google Drive*
- *Microsoft Teams*
- *Zoom*
- *Otras aplicaciones de uso por la facultad (Canvas, eLearning, Panopto, etc)*

El/la empleada docente o administrativo/a, y su supervisor/a a cargo, deben ser juiciosos y prudentes en el momento de utilizar los mecanismos de comunicación. Deben acordar cuáles serán los mecanismos más apropiados para trabajar con información compleja, privilegiada y/o confidencial de la institución, como también con información de estudiantes.

Dentro de lo posible, los horarios para las reuniones presenciales o virtuales, y los plazos de entrega de los trabajos, se calendarizarán de antemano. Se fomenta la utilización de las videoconferencias, por su naturaleza participativa, para discutir el estatus de los trabajos y/o proyectos asignados. De esta manera a su vez, fomentamos el contacto humano entre los equipos de trabajo.

En caso de tener complicaciones con la comunicación, deberán informarlo a la unidad de ITI, para asistirle en la solución de sus problemas de comunicación y tecnología.

Seguridad de la información

Al igual que con las expectativas de seguridad de la información de la Universidad con respecto a los/as empleados/as que trabajan en el campus o los/as profesores que ofrecen cursos presenciales en el campus, se espera que los aquellos/as que trabajen de forma remota también garanticen la protección de la información de la Universidad y de los/as estudiantes que sea accesible desde su oficina o espacio remoto. Se recomienda el uso de archivos y escritorios cerrados, el mantenimiento regular de contraseñas y cualquier otra medida apropiada para la protección apropiada de la información.

Los/a empleados/as participantes en el teletrabajo utilizarán única y exclusivamente las plataformas provistas por la Universidad para almacenar y compartir archivos y documentos variados de su trabajo. Las plataformas institucionales son: *Microsoft Teams y Zoom para colaboración y videoconferencias*, *Google Drive y Microsoft OneDrive para archivo electrónico de documentos; Canvas, eLearning, Zoom y Panopto para cursos; Jenzabar EX para el sistema de información de estudiantes (SIS); y Kuali para el sistema de información y transacciones financieras.* En caso de duda sobre las plataformas institucionales, favor de comunicarse con su supervisor/a.

Por otro lado, cada unidad debe adoptar las mejores prácticas sobre el manejo de la información de la institución, del personal y del estudiantado. Deben abstenerse de imprimir documentos en la medida que sea posible.

Es responsabilidad de todo el personal administrativo y docente cumplir con las políticas y procedimientos institucionales que son pertinentes al teletrabajo, incluyendo por ejemplo, la Política para el Uso de los Recursos de Información y Tecnología disponible en https://politicas.sagrado.edu/wp-content/uploads/Politica-de-Uso-Acceptable-de-Recursos-de-Tecnologia-de-Informacion.pdf, la Política de Seguridad de la Información disponible en https://politicas.sagrado.edu/wp-content/uploads/Politica-para-la-Seguridad-de-la-Informacion.pdf, y la Política para la Privacidad de la Información disponible en https://politicas.sagrado.edu/wp-content/uploads/Politica-de-Privacidad-de-la-Informacion.pdf. Para información sobre nuestras políticas puede acceder a: https://politicas.sagrado.edu/.

Seguridad cibernética (*Cybersecurity*)

Debido a que el trabajo a realizar será remoto, es posible que se intente vulnerar la seguridad del *software* y *hardware* provisto por la Universidad por parte de personas ajenas y malintencionadas.

Algunas de las técnicas utilizadas para esto son:

Phishing

Es la práctica de enviar correos electrónicos fraudulentos que se parecen a correos electrónicos de fuentes confiables. El objetivo es robar datos confidenciales como números de tarjetas de crédito e información de inicio de sesión. Es el tipo más común de ciberataque.

También suelen recurrir a anuncios o sitios web que se parecen mucho a los que ya usted conoce. Por ejemplo, alguien que intente efectuar un ataque de *phishing* podría enviarle a usted un correo que parezca proceder de su banco para que facilite los datos sobre su cuenta.

Los correos electrónicos o sitios web de *phishing* pueden solicitarle que ingrese:

- Nombres de usuario y contraseñas, incluyendo cambios de contraseñas
- Número de Seguro Social
- Números de cuentas bancarias
- Números de identificación personal (PIN)
- Números de tarjetas de crédito

- Los apellidos de un familiar (madre) y fecha de nacimiento

Para evitar este tipo de ataques, usted debe sospechar siempre que reciba un correo de un sitio web en el que le soliciten información personal.

Si recibe este tipo de correo electrónico:

- No haga clic en ningún enlace ni proporcione información personal hasta que confirme que el correo es auténtico. Compruebe que la dirección de correo y el nombre del remitente coinciden.
- Antes de hacer clic en un enlace, coloque el cursor sobre él. Si la URL del enlace no coincide con la descripción, es posible que le lleve a un sitio web de *phishing*.
- Revise las cabeceras de los mensajes para asegurarse de que el campo "De" no indica un nombre incorrecto.

Ransomware

Es un tipo de *software* malicioso. Está diseñado para extorsionar con dinero, bloqueando el acceso a los archivos o al sistema informático hasta que se pague el rescate. Pagar el rescate no garantiza que los archivos se recuperarán o que se restaurará el sistema.

Malware

Es un tipo de *software* diseñado para obtener acceso no autorizado o para dañar una computadora. Si usted sospecha que ha sido vulnerable a este tipo de ataque, debe informarle inmediatamente al Sr. Luis Gotelli, Principal Oficial de Informática, persona asignada para trabajar con este tipo de situación.

La seguridad en el teletrabajo

Se espera que los/as empleados participantes en el teletrabajo mantengan su espacio de trabajo remoto seguro y libre de riesgos. Las lesiones sufridas por un/una empleada en un espacio de trabajo remoto y que están relacionadas a sus deberes laborales regulares normalmente están cubiertas por la póliza institucional con la Corporación del Fondo del Seguro del Estado (CFSE). Los/as empleados/as en trabajo remoto son responsables de notificar a la Universidad sobre tales lesiones tan pronto como sea posible. El/la empleada es responsable de las lesiones sufridas por los visitantes a su hogar o lugar de trabajo remoto. En casos que ocurra violencia de género, deberá comunicarse de inmediato con la unidad de Desarrollo Organizacional y Recursos Humanos.

Tiempo trabajado

El/la empleado/a administrativo/a y docente tiene que completar sus responsabilidades y cumplir con el itinerario de trabajo y fechas de entrega de tareas o proyectos que acuerde con su supervisor/a. El itinerario del/la empleado/a administrativo/a debe ser el mismo que sigue cuando trabaja desde el campus (por ejemplo: de 8:00 a.m. hasta las 5:00 p.m.) o aquel horario que acuerde con su supervisor/a inmediato/a.

Los/as empleados/as administrativos trabajando remoto que sean no exentos de la legislación sobre horas y salarios deberán registrar con precisión todas las horas trabajadas y periodos de tomar alimentos utilizando según sea acordado con su supervisor. Es decir, durante su día de trabajo remoto el/la empleado/a no exento deberá: (a) registrar sus horas de trabajo de trabajo con expresión de su hora de comienzo a trabajar, (b) no trabajar más de ocho (8) horas diarias, ni cuarenta (40) en una semana, sin estar autorizado por escrito para ello, asegurándose, además, de comenzar a disfrutar de una (1) hora de tomar alimentos luego de concluida la segunda, pero no después de comenzada la sexta hora de trabajo.

Las horas trabajadas en exceso a las programadas por día y por semana laboral requieren la aprobación previa del/a supervisor/a de empleado/a no exento. No podrá trabajar más allá del periodo de tiempo autorizado. El incumplimiento de este requisito puede resultar en medidas disciplinarias.

El personal trabajando remoto debe notificar tardanzas y sus ausencias por razones personales o de enfermedad, de la misma forma que lo harían trabajando de manera presencial en el campus. En la eventualidad de que un/una supervisor/a encuentre que un/una empleado/a incumple con estas normas o haya un patrón de ausencias no programadas, podrá recomendar la aplicación de las medidas disciplinarias que correspondan.

El/la empleado/a administrativo/a debe acordar con su supervisor/a el tiempo que necesite tomar para gestiones personales (por ejemplo, citas del/la empleado/a o de algún familiar con profesionales de la salud) y registrarlo a la licencia correspondiente en el sistema de gerencia de personal (ADP) antes de tomar el tiempo solicitado.

Cumplimiento con políticas institucionales

Los/as empleados/as administrativos/as y docentes que trabajen de manera remota aceptan cumplir con las políticas y los procedimientos de la Universidad vigentes o que se establezcan en el futuro incluyendo el Manual de Empleado y el Manual de la Facultad. De incumplir con alguna de éstas, el empleado/a pudiera estar sujeto a procesos disciplinarios con las sanciones correspondientes. Para información sobre nuestras políticas puede acceder a: https://politicas.sagrado.edu/.

La Universidad, en el sano ejercicio de su discreción, podrá cambiar, modificar o dejar sin efecto esta guía. Cuando lo entienda necesario para mantener la continuidad de las operaciones, la Universidad podrá extender o reducir la duración del periodo de trabajo remoto. La Universidad podrá solicitar al empleado/a que trabaje de manera remota o que se reincorpore al trabajo físicamente en el campus. De tener alguna situación que le impida su regreso al campus, el/la empleado/a debe comunicarse inmediatamente con su supervisor/a o con la unidad de Desarrollo Organizacional y Recursos Humanos y presentar evidencia que justifique el no poder regresar.

Consultas sobre esta guía

El presidente de la Universidad emite esta guía bajo circunstancias extraordinarias por motivo de la emergencia del COVID-19. Las consultas sobre el alcance y la interpretación de esta guía deben dirigirse a la unidad de Desarrollo Organizacional y Recursos Humanos

Aprobado:

Gilberto J. Marxuach Torrós
Presidente
24 de agosto de 2020

ANEJO – *Responsabilidades de todos/as los/as empleados/as*

1. Cumplir con el itinerario de trabajo actualmente establecido u otro que se acuerde con el/la supervisor/a.
2. Cumplir con las guías de trabajo para el buen y normal funcionamiento de su unidad de trabajo incluyendo puntualidad, disponibilidad, comunicación y cumplir con sus responsabilidades correctamente y a tiempo.
3. Cumplir con las responsabilidades del puesto, así como los objetivos y las métricas de desempeño acordadas con su supervisor/a y cualquier otro que el/a supervisor/a defina adaptado a la modalidad de trabajo remoto.
4. Estar disponible para atender diligentemente las llamadas telefónicas, correos electrónicos y mensajes de texto que serán enviadas por las plataformas oficiales de Sagrado para asuntos relacionados a su trabajo.
5. Estar disponible para participar en las reuniones virtuales, telefónicas u otros medios electrónicos a las que sea citado.
6. En todo momento utilizar las plataformas y los medios electrónicos institucionales autorizados por la Universidad para realizar sus labores y cumplir con la Política para el Uso de los Medios Electrónicos Durante la Emergencia del COVID-19 disponible en https://politicas.sagrado.edu/wp-content/uploads/Politica-para-el-Uso-de-Medios-Electronicos-Durante-la-Emergencia-COVID-19.pdf. Para información sobre nuestras políticas puede acceder a: https://politicas.sagrado.edu/.
7. Cumplir con las leyes de derechos de autor en relación con los acuerdos de licencias con los terceros dueños de los medios electrónicos.

Responsabilidades adicionales para los/as Empleados/as No-Exentos/as

1. Disfrutar de su periodo de almuerzo en el horario establecido por su supervisor/a. El mismo debe ser luego de la segunda hora, pero antes de comenzar la sexta hora.
2. Comunicar a su supervisor/a su hora de entrada y salida. Si hay algún cambio sobre su registro de tiempo y asistencia le será notificado por su supervisor/a con anterioridad.
3. Tener autorización de su supervisor/a para trabajar horas extras antes de incurrir en el trabajo.

Responsabilidades adicionales para los/a Empleados/as Docentes

1. Indicar los medios alternos a utilizar para comunicarse con sus estudiantes.
2. Documentar los acuerdos entre estudiante/profesor/a para manejar el proceso de educación a distancia, en caso de que algún estudiante presente una necesidad particular.
3. Mantener los acuerdos con respecto al tiempo requerido como horario de oficina remoto.