Políticas para Asistencia Remota a Usuarios

I. OBJETIVO

La presente política tiene como objetivo establecer las pautas, condiciones, responsabilidades y niveles de seguridad correspondientes en el uso de la herramienta de asistencia remota siguiendo criterios de confidencialidad que permitan mejorar el servicio a los usuarios de la UP con una reducción significativa en los tiempos de atención de requerimientos, incidentes o problemas.

II. ALCANCE

Esta política se aplica a los usuarios de la UP, para brindarles atención remota de incidencias, en lo referente al uso, funcionalidad de su equipo o aplicación informática exclusivamente cuando se encuentren en equipos y dispositivos que son propiedad de la Universidad

Quedan excluidos de esta política los equipos que forman parte de la infraestructura tecnológica administrados por el área de Gestión de Plataforma Tecnológica.

III. DEFINICIONES

Ultra VNC: Escrito como uVNC, es un software libre de escritorio remoto bajo Microsoft Windows mediante protocolo de comunicaciones "VNC", que permite visualizar la pantalla de otra computadora (vía Internet u otra red) en la pantalla del usuario. El programa permite el uso del ratón y del teclado para controlar otro computador remotamente. Esto quiere decir que se puede trabajar en un computador remoto como si se estuviese sentado frente a él desde cualquier ubicación.

Usuarios: Las personas que utilizan infraestructura y servicios de tecnología que brinda la UP.

Asistencia Remota: Dar soluciones a incidencias y /o problemas de los usuarios, a través de una conexión segura a su equipo, sin necesidad de estar presente.

Sobre el uso del Equipo del Usuario: El presente servicio que usted acepta permite que el Software de Acceso remoto (Ultra VNC) pueda utilizar el procesador y el ancho de banda del equipo que usted está utilizando, con el fin limitado de facilitar la comunicación entre el usuario y el área de soporte a usuarios.

Protección del equipo (recursos) del Usuario: Usted comprende que el área de soporte a usuarios, hará los esfuerzos que sean necesarios para proteger la privacidad e integridad de la comunicación y de los recursos del equipo que Usted está utilizando.

Manipulación: El usuario está impedido de hacer algún tipo de modificación o manipulación en la configuración del software de acceso remoto (Ultra VNC), mientras ésta no sea solicitada, requerida y guiada por el área de soporte a usuarios.

Confidencialidad: Seguridad de que la información es accesible solamente a quienes están autorizados para su uso.

Integridad: Protección de la exactitud y estado completo de la información.

Eficiencia: Rapidez en la solución de los casos que presenten los usuarios, además de un aporte extra que pueda requerir el usuario y esté dentro de nuestras posibilidades ayudarlo.

Seguridad de la Información: Característica de la información que se logra mediante la adecuada combinación de políticas, procedimientos, estructura organizacional y herramientas informáticas especializadas a efectos que dicha información cumpla los criterios de confidencialidad, integridad y disponibilidad, definidos de la siguiente manera:

I. Confidencialidad: La asistencia remota a usuarios debe ser accesible sólo a aquellos que se encuentren debidamente autorizados.
II. Integridad: La información debe ser completa, exacta y válida.
III. Disponibilidad: La información debe estar disponible en forma organizada para los usuarios autorizados cuando sea requerida.

GIIT: Gerencia de Información e Innovación Tecnológica.

Usuarios Críticos: Usuarios con cargos importantes y que requieran de atención personalizada; usuarios que se resistan al cambio o no depositen su confianza.

IV. SOFTWARE DE ASISTENCIA REMOTA

El software de asistencia remota que se utilizará será el Ultra VNC (uVNC) en sus versiones Viewer y Server. La versión Viewer permite brindar asistencia remota y la versión Server permite recibir asistencia remota.

V. MANEJO DE NOMENCLATURAS EN LA ATENCIÓN DE REQUERIMIENTOS, INCIDENCIAS O PROBLEMAS UTILIZANDO ASISTENCIA REMOTA

- Para brindar asistencia remota se necesita la dirección IP o el nombre del equipo.
- La Universidad asigna direcciones IP dinámicas; por ello, se instalará el programa BackInfo que permite mostrar el nombre del equipo y la dirección IP del usuario afectado en el escritorio de su PC, formando parte del papel tapiz institucional.

- Este nombre está establecido según la "Política para Nomenclaturas de Equipos de Cómputo" y cuyo historial se encuentra registrado en el "Formato de Kárdex de Equipos de Cómputo."
- Es responsabilidad del equipo de Soporte a Usuarios el actualizar la nomenclatura según corresponda y actualizar el kárdex que se tomará como base de datos de los equipos para acceder a la asistencia remota por el uVNC.

VI. NIVELES DE SEGURIDAD EN EL USO DE LA ASISTENCIA REMOTA[1]

1. El Software para asistencia remota que se maneja en GIIT, solamente podrá ser utilizado con el fin de brindar soporte técnico a usuarios de la UP.
2. Los dispositivos de los usuarios catalogados como usuarios críticos tendrán el más alto nivel de seguridad de acceso para asistencia remota.
3. Las oficinas desde donde se brinda asistencia remota son áreas de acceso restringido, por tal motivo el ingreso y permanencia debe ser controlado y supervisado.
4. El acceso a los diferentes equipos informáticos que se administren por asistencia remota debe seguir los mecanismos de autenticación establecidos de acuerdo con los siguientes niveles de seguridad y según el tipo de usuario que utilice el equipo:

   Equipos Públicos: Son equipos de uso genérico. No tienen un usuario específico asignado para su uso, por lo que no requieren de la aceptación del usuario para ser administrados por asistencia remota. Este es el caso de los equipos de laboratorios, auditorios y de salas de control.

   - Instalar el Ultra VNC Server que sólo permite recibir llamadas de asistencia remota.
   - No se debe mostrar el ícono de notificación para que el usuario no tenga acceso a las opciones del uVNC.
   - Bloquear las opciones de configuración del uVNC al usuario para que no modifique las propiedades principales.
   - Colocar una contraseña que sólo será de conocimiento por el personal de GIIT o quienes la Gerencia indique.
   - Configurar para que no solicite aceptación del usuario al momento de acceder al equipo de manera remota.

   Equipos privados:

   - Instalar el Ultra VNC Server que sólo permite recibir llamadas de asistencia remota.

[1] Para la instalación y configuración del uVNC ver el Procedimiento de Instalación y Configuración del uVNC para Asistencia Remota a Usuarios

- Se debe mostrar el ícono de notificación del uVNC para que el usuario tenga conocimiento que está instalado y que su equipo puede ser atendido mediante asistencia remota cuando lo requiera.
- Bloquear las opciones de configuración del uVNC al usuario para que no modifique las propiedades principales.
- La persona que brinde asistencia remota enviará una notificación solicitando permiso. El usuario es quien decide aceptar o rechazar la asistencia remota.

Equipos GIIT:

- Instalar el Ultra VNC Server y Ultra VNC Viewer que permiten recibir y enviar llamadas de asistencia remota, respectivamente.
- Se debe mostrar el ícono de notificación del uVNC para que el usuario tenga conocimiento que está instalado y que su equipo puede ser atendido mediante asistencia remota cuando lo requiera.
- Desbloquear las opciones de configuración del uVNC al usuario para que pueda modificar las propiedades principales.

Permisos para brindar Asistencia Remota:

Sólo se puede brindar asistencia remota siempre y cuando se cumplan con los siguientes requisitos:

- El usuario que brinda asistencia remota se encuentra dentro del Grupo GIIT del Directorio Activo.
- El equipo desde el que se brinda asistencia remota tiene una IP Fija dentro del rango permitido.

5. El acceso no autorizado al Software para asistencia remota está prohibido. Se considera que hay uso indebido de la información y de los recursos, cuando la persona incurre en cualquiera de las siguientes conductas:
   a. Facilitar el control del Acceso Remoto a quien no tiene derecho a su uso.
   b. Usar el Acceso Remoto con el fin de obtener beneficio propio o de terceros.
   c. Ocultar el uso del acceso remoto maliciosamente causando cualquier perjuicio.
   d. Instalar otro software de Acceso Remoto (que no sea el UVNC que es el vigente autorizado) o de Monitoreo sin la debida autorización.
   e. Intentar modificar o eliminar información de cualquier índole en equipos de cómputo que se acceda remotamente sin la autorización del usuario o personal responsable.
   f. Capturar sin autorización la información de los accesos de otros usuarios (passwords de correos, aplicaciones, carpetas, documentos, etc.) a los sistemas que ellos administran.

g. Transgredir o burlar los mecanismos de autenticación del software de Acceso Remoto (UVNC).
h. Adueñarse del trabajo de otros usuarios, o de alguna manera apropiarse del trabajo ajeno.
i. Usar cualquier medio para dañar o perjudicar de alguna manera los recursos disponibles electrónicamente.
j. Lanzar remotamente cualquier tipo de virus, gusano o programa de computador cuya intención sea hostil o destructiva.
k. Utilizar el acceso Remoto para publicar material ilegal, con derechos de propiedad o material nocivo usando un recurso de la UP.

6. Los usuarios de equipos privados tienen la opción de cambiar la contraseña para establecer una conexión de asistencia remota. Si cambian la contraseña, es de su responsabilidad la custodia de la misma.
7. Se debe verificar en un número de computadoras elegidas al azar, los niveles de seguridad del Ultra VNC, tanto en equipos de usuarios como en equipos de GIIT, cada 6 meses.
8. Someter a pruebas en un entorno controlado las actualizaciones del software que usa el Software para asistencia remota (uVNC).
9. Actualizar o investigar sobre cómo mejorar el Software para asistencia remota (firewall, software, políticas de uso, etc.)

VII. RESPONSABILIDADES

- Es responsabilidad de la Gerencia de Información e Innovación Tecnológica la supervisión o seguimiento del cumplimiento de la presente política.
- Es responsabilidad del Coordinador de Soporte a Usuarios y el Supervisor de Soporte Técnico la aplicación de la presente política y vigilar su correcto cumplimiento.
- Todos los integrantes de GIIT que brinden atención remota son responsables del cumplimiento de la presente Política. Su incumplimiento puede ser calificada como Falta Grave.
- En todo momento debe considerarse que solamente el Equipo de la Gerencia de Información e Innovación Tecnológica (y quien su Gerente indique) tienen acceso a la presente información.
- Son responsables de la mejora continua del presente documento todos los integrantes de GIIT.
- Es responsabilidad de cada usuario que recibe asistencia remota, permanecer frente a su equipo, visualizando las acciones de soporte, durante todo el tiempo que dure la atención (Responsabilidad a incorporarse en el Reglamento de Trabajo).

VIII. DOCUMENTOS RELACIONADOS

- Política para Nomenclaturas de Equipos de Cómputo.
- Formato de Kárdex de Equipos de Cómputo.

IX. RESTRICCIONES O COMPLICACIONES A TENER EN CUENTA

1. No se podrá dar en algunos de los casos una buena comunicación con el usuario y el personal de Soporte a Usuarios en el caso de aulas por ejemplo donde no cuentan con teléfonos para mantener la comunicación, para estos casos cuando no sabemos específicamente lo que requiere el usuario no se podrá dar asistencia remota.
2. Todos los usuarios deben tener conocimiento de la funcionalidad de esta herramienta para asistencia remota, pero para casos en que el usuario se resista al cambio (atención física por atención remota) se debe tratar de persuadir al usuario que será efectiva y beneficiosa; en caso se resista se considerará como usuario crítico.
3. La persona que brinde soporte a través de asistencia remota, debe verificar que el usuario está utilizando el equipo que le fue asignado y que no está en el equipo de otro usuario.
4. La persona que brinde soporte a través de asistencia remota, debe verificar que el usuario se encuentra presente frente a su equipo durante toda la sesión de asistencia remota.