Deberes y Restricciones por parte de los Usuarios Finales de la Red Corporativa de Datos de la UCV

Objetivo:

Proveer un marco referencial de actuación a los usuarios finales pertenecientes a las distintas facultades y dependencias que hacen uso de la Red Corporativa de Datos en materia de seguridad de la información y resguardo de los equipos asignados, a fin de que sea incorporado a sus rutinas de trabajo, lo cual contribuirá a garantizar una plataforma corporativa estable y segura, que permita realizar sus funciones administrativas y/o académicas.

De los Deberes:

Con el fin de no comprometer la seguridad de la red y resguardar los recursos asignados para realizar sus actividades institucionales, todos los usuarios deben cumplir con las siguientes responsabilidades:

1. Internalizar la importancia del cumplimiento de estos deberes y respetar las restricciones definidas para el usuario final, que contribuyan al buen funcionamiento de la red y la prestación de los servicios corporativos.
2. Velar por el buen estado y funcionamiento de los equipos que le sean asignados, considerando que los mismos son de uso corporativo y pertenecen a la Institución.
3. Acceder a los servicios de red: Correo, Navegación por Internet, Archivos Compartidos, Impresoras, Antivirus, entre otros, a través de la autenticación del usuario en el dominio correspondiente a su facultad o dependencia.
4. Respetar el hecho de que las claves de acceso de sus cuentas son intransferibles y las consecuencias que se generen por el uso indebido de las mismas, será responsabilidad del usuario.

5. Modificar periódicamente sus claves personales de acceso a la red corporativa, tomando en cuenta las consideraciones del administrador de la red, para la definición de las mismas.
6. Respaldar y resguardar, en un lugar seguro, la información que haya sido clasificada como de alto riesgo o confidencial por parte de la facultad o dependencia y que se encuentre bajo su responsabilidad, así como los medios de almacenamiento, manuales y listados de información.
7. Compartir la información necesaria a través de Servidores de Archivos y no desde su equipo, para lo cual deberá contactar al administrador de la red, quien le publicará su información a través de directorios con la permisología adecuada.
8. Apagar el equipo, una vez finalizada la jornada de trabajo de la semana, lo que incluye CPU, monitor, cornetas y cualquier otro dispositivo periférico. Sin embargo, pueden haber excepciones las cuales deben ser notificadas y autorizadas por su supervisor inmediato.
9. Destruir cualquier documento que contenga información importante y vaya a ser desechado, previa autorización correspondiente de su supervisor inmediato.
10. Notificar a su supervisor inmediato y responsable de la Unidad de Tecnología de la facultad o dependencia, cuando exista la sospecha o se descubra que su información ha sido manipulada sin autorización.
11. Bloquear la sesión de trabajo en el equipo para evitar el acceso de otras personas al mismo, cuando deba alejarse de su puesto de trabajo.
12. Retirar listados o documentos con información confidencial de las impresoras.
13. En aquellos casos que así lo amerite, el usuario deberá indicar al personal de la Unidad de Tecnología, la información que requiere respaldar presente en el disco duro de su equipo, y hacer una revisión de la información respaldada (copia) para verificar que se hizo correctamente.

14. Informar al personal de su Unidad de Tecnología sobre cualquier traslado, ingreso o retiro de equipos.
15. Notificar al personal de su Unidad de Tecnología acerca del ingreso, modificación o retiro del personal que tenga a su cargo.
16. Reportar al personal de su Unidad de Tecnología sobre cualquier desperfecto o falla del equipo (a nivel de hardware o software), así como la necesidad de instalar programas o aplicaciones requeridas para realizar sus labores administrativas y/o académicas, previa aprobación de la autoridad competente.
17. Cualquier otra responsabilidad y/o restricción que vaya en beneficio del rendimiento de la plataforma tecnológica que utiliza y por ende del desarrollo de las funciones fundamentales de la Institución.

De la protección contra virus:

1. Reportar al personal de la Unidad de Tecnología de su facultad o dependencia, cuando haya detección o sospecha de la existencia de virus informáticos y/o software malicioso en el equipo.
2. Revisar cualquier información proveniente de diskettes, CD o pendrives, así como archivos anexos a correos, a través de la aplicación corporativa de antivirus instalada en su equipo, por parte del personal de la Unidad de Tecnología, a fin de asegurar que no contenga ningún virus informático y software malicioso.
3. Solicitar al personal de la Unidad de Tecnología que desconecte el equipo de la red, en caso de existir o sospechar la presencia de virus, hasta que no sea revisado por el personal de la mencionada unidad.

De las restricciones:

Para evitar situaciones que comprometan la seguridad de la red y por lo tanto de la Institución, los usuarios **NO DEBEN**:

1. Divulgar cualquier clave de acceso de su cuenta personal, que le sea asignada para el uso de los servicios de la Red Corporativa de Datos.

2. Realizar la instalación de cualquier programa o aplicación en las estaciones de trabajo.
3. Instalar programas ilegales en los equipos de computación de la Institución.
4. Acceder a la Red Corporativa de Datos con equipos asignados a otros usuarios sin su previa autorización.
5. Comer, beber o fumar mientras estén utilizando los equipos de computación de la Institución.
6. Utilizar los equipos de computación y la información contenida en ellos, para fines distintos a los cuales han sido destinados.
7. Realizar copias no autorizadas de programas instalados en su equipo de computación.
8. Instalar programas o aplicaciones en los directorios de datos de los servidores.
9. Extraer cualquier tipo de información de la Institución sin previa autorización.
10. Enviar mensajes con archivos anexos a través de la mensajería instantánea (aplicación para conversación o chat, como Messenger), porque son susceptibles a la transmisión de virus y software malicioso.
11. Colocar claves de acceso al equipo para su arranque sin previa autorización del personal de la Unidad de Tecnología.
12. Enviar correos con archivos anexos que tengan las extensiones ad, scr, mp3, mp4, pif, exe, bat, cmd, com, B64, mim, BHX, Uu, hqx, pIF, HQX, entre otros, porque son susceptibles a la transmisión de virus y software malicioso.
13. Acceder a Páginas WEB relacionadas con Pornografía, Sexo, Violencia, Música, Videos, entre otros, que no tengan vinculación con sus obligaciones institucionales.