ANEXO 3
AL CONTRATO DE AGENCIA CELEBRADO ENTRE
TELEFÓNICA MÓVILES S.A. Y EL AGENTE

NORMAS TÉCNICAS DE SEGURIDAD PARA AGENCIAS

I. Identificación y Autenticación

1. La AGENCIA deberá proporcionar a TELEFÓNICA MÓVILES los nombres de las personas y el número del documento de identidad a las cuales se les asignará las cuentas de acceso a los sistemas. Las personas a quienes se les entregará las cuentas deben estar registradas en la planilla de empleados de la AGENCIA.
2. Todo usuario de la AGENCIA que haya sido autorizado a acceder a la red y a los sistemas, deberá hacerlo mediante una única cuenta de acceso personal (llamada también user_id, login o identificación) y su clave de acceso respectiva (llamada clave, contraseña o password). Esta clave debe ser personal e intransferible, la Agencia deberá hacer firmar un cargo a la persona que reciba el acceso.
3. La AGENCIA se obliga a cumplir y hacer cumplir a su personal las siguientes Recomendaciones Básicas en la utilización de contraseñas:
    - Evitar la escritura, copia o reproducción de las mismas en papel o almacenarlas en un fichero sin protección.
    - Cambiar las contraseñas siempre que sospechen que pudieran haber sido comprometidas.
    - Cambiar siempre las contraseñas iniciales o reiniciadas en el primer acceso.
    - Cambiar las contraseñas mínimo cada 30 días.
    - Seleccionar contraseñas difíciles de adivinar y fáciles de recordar (contraseña fuerte).
    - El uso o aceptación de claves de acceso obtenida por medios ilegales constituye una falta grave para efectos laborales y está sujeta a sanción disciplinaria al empleado usuario. La sanción disciplinaria será aplicada por la AGENCIA, en su condición de empleadora del trabajador infractor.
4. Los usuarios de la AGENCIA se identificarán y autenticarán en el acceso a los sistemas de información y redes de comunicaciones de TELEFÓNICA MÓVILES, de modo que se pueda reconocer su identificación y comprobar la autenticación del usuario que accede de forma inequívoca.
5. El acceso a la red y a los sistemas está limitado sólo a direcciones específicas autorizadas por TELEFÓNICA MÓVILES, no debe intentarse acceder a otras direcciones.
6. En caso que la AGENCIA utilice certificado digital, se obliga a utilizar los certificados digitales únicamente en los locales para los cuales le hayan sido asignados. Consecuentemente, LA AGENCIA asume todo tipo de responsabilidades frente a TELEFÓNICA MÓVILES en caso dicho certificado fuese utilizado para acceder a los sistemas de TELEFÓNICA MÓVILES desde un local no autorizado**.**

7. La AGENCIA no podrá realizar actividad alguna con un certificado digital que no corresponda a uno de sus locales asignados.

8. La AGENCIA utilizará autenticación de segundo nivel, con mecanismos biométricos para el control sobre los activos donde se realizan las transacciones.

II. Control de Accesos

9. La utilización de las cuentas y claves de acceso asociadas es **estrictamente personal.** Los usuarios no permitirán a otros realizar actividad alguna con su cuenta. En forma similar los usuarios están prohibidos de realizar actividad alguna con una cuenta perteneciente a otro usuario.

10. Los equipos de cómputo personales desde donde los usuarios accederán a la red y a los sistemas de TELEFÓNICA MÓVILES deben estar situadas en un ambiente físico aislado y seguro, y estar protegidos con control de accesos físicos.

11. En caso que la AGENCIA envíe un equipo de cómputo a mantenimiento o a servicio técnico, previamente deberá desinstalar el certificado digital asociado a dicho equipo y eliminar cualquier información de TELEFÓNICA MOVILES para evitar su divulgación a personal no autorizado. En caso que no se pueda desinstalar por cualquier motivo, la AGENCIA deberá formatear el disco duro del equipo de cómputo para eliminar toda información del mismo.

12. Es obligación de la AGENCIA comunicar a TELEFÓNICA MÓVILES de forma inmediata las bajas causadas por personal cesado que pertenezca a la AGENCIA, a fin de que TELEFÓNICA MÓVILES pueda deshabilitar los accesos de los mismos de manera oportuna.

13. Las cuentas de acceso que no se hayan utilizado durante un periodo máximo de 30 días (periodo de inactividad) serán deshabilitados.

14. Las cuentas de acceso de las personas que se ausenten por los siguientes motivos: vacaciones, licencia por maternidad, enfermedad deben ser comunicados a su gestor de TELEFÓNICA MOVILES para su bloqueo temporal.

III. Registro de Auditoria y Monitorización

15. Cualquier usuario que utilice una cuenta en cualquiera de los sistemas de **TELEFÓNICA MÓVILES** aceptará que el uso de la misma podrá ser monitorizado y tendrá el siguiente mensaje de recordación:

    "Este sistema es propiedad de **TELEFÓNICA MÓVILES**. Para acceder a este sistema usted necesita estar previamente autorizado, estando estrictamente limitado al uso indicado en dicha autorización. El acceso a este sistema es exclusivamente para el cumplimiento de las labores internas de **TELEFÓNICA MÓVILES**. El acceso no autorizado a este sistema o el uso indebido del mismo está prohibido y es contrario a la legislación y a la Política Corporativa de Seguridad vigentes. **TELEFÓNICA MÓVILES** se reserva el derecho de auditar su empleo, sancionar conforme a ley a las personas que hagan uso no autorizado, mal uso o uso malintencionado del mismo, y/o denunciar penalmente a aquellas personas que mediante manipulación dolosa al sistema

causen perjuicio a **TELEFÓNICA MÓVILES**. El uso que realice de este sistema está siendo monitorizado**"**.

IV. Redes y Comunicaciones para Agencias que no se encuentren conectadas a la red de TELEFÓNICA MOVILES.

16. LA AGENCIA para conectarse a los servicios de la red y a los sistemas de TELEFONICA MOVILES debe contar con acceso a internet con IP Fija.
17. Las estaciones de trabajo de las Agencias que se conecten a los Sistemas de Telefónica mediante cableado de red no deberán hacer uso de sus redes inalámbricas simultáneamente.
18. Si la AGENCIA cuenta con red WiFi, debe cumplir con las siguientes especificaciones:
    - Cambiar la contraseña por defecto del router (Administrador), las contraseñas deben cumplir con criterios de contraseña robusta.
    - Cambiar el nombre del identificador SSID (Service Set IDentifier) de la red WIFI.
    - Desactivar el broadcast del SSID (Service Set IDentifier), para que no sea público.
    - El cifrado de la red debe ser el máximo que soporta el dispositivo.
    - Activar el filtrado por direcciones MAC para el acceso a la WIFI e inscribir las MACs solo de las PCs autorizadas.
    - Desactivar el Servidor DHCP y asignar un IP fija a las PCs que tendrá acceso a la red WIFI.
19. Toda conexión de la AGENCIA a Internet debe estar protegida por un firewall que permita segmentar la red (red interna con redes externas) y que debe evitar tráfico entrante y saliente que no tenga relación con los servicios que brinda la AGENCIA. Asimismo, la AGENCIA deberá implementar un Sistema de Prevención de Intrusos que proteja el acceso de los usuarios.

V. Redes y Comunicaciones para Agencias que se conecten a la Red de TELEFÓNICA MOVILES

20. Las estaciones de trabajo de las Agencias que se conecten a los Sistemas de Telefónica mediante cableado de red no deberán hacer uso de sus redes inalámbricas simultáneamente.

VI. Control de Hardware, Software y Seguridad de estaciones de trabajo de agencias para evitar Spyware, malware, troyanos, antivirus, antispam, etc.

21. Los equipos que utilice la AGENCIA deberán cumplir con todos los requisitos mínimos de seguridad:

- Solo podrá utilizarse software licenciado, no se debe instalar software que permitan vulnerar los accesos asignados.
- Los sistemas operativos de estos equipos deberán contar con los parches de seguridad actualizados evitando vulnerabilidades en dichos sistemas y riesgos que comprometan la red corporativa y los Sistemas Informáticos de TELEFÓNICA MÓVILES.
- Está terminantemente prohibida la instalación de software de control remoto.
- En los equipos de cómputo de la AGENCIA, los medios de almacenamiento externo (USB, lector/grabador de CD, lector/grabador de DVD, etc.) deben estar deshabilitados.
- Las configuraciones de los Sistemas de TELEFÓNICA MOVILES deben mantenerse tal cual fueron instaladas y no deben ser modificadas

22. TELEFÓNICA MÓVILES podrá implementar software de Control de Seguridad en los equipos de las Agencias que le permita monitorear el uso de accesos desde dichos equipos hacia los sistemas Informáticos de TELEFÓNICA MÓVILES.
23. La AGENCIA deberá eliminar la información de TELEFÓNICA MOVILES cuando la PC sea dada de baja.
24. La AGENCIA deberá informar a TELEFÓNICA MOVILES en forma inmediata cualquier tipo de incidencia (robo, siniestro, u otros) con los equipos de cómputo que se conectan a los sistemas de TELEFÓNICA MOVILES.
25. La AGENCIA deberá usar y actualizar regularmente el software antivirus que permita reducir las vulnerabilidades y virus maliciosos y destructivos que puedan entrar al sistema a través de la actividad de correo electrónico de su personal.
26. La AGENCIA está obligada a contar con controles de detección, prevención y recuperación frente a códigos maliciosos (virus, troyanos, parches de seguridad, etc.).

VII. Responsable de seguridad

27. La AGENCIA deberá nombrar a un responsable técnico de la seguridad de la información, quien coordinará con TELEFÓNICA MÓVILES (en la persona de su responsable de Seguridad de la Información) los temas de Seguridad de Información.
28. La AGENCIA informará a TELEFÓNICA MOVILES en la persona de su responsable de Seguridad de la Información los datos concernientes a la seguridad de los equipos que se conectan a las redes o sistemas de TELEFÓNICA MOVILES
29. La AGENCIA deberá informar a TELEFÓNICA MÓVILES en la persona de su responsable de Seguridad de la Información cuando ocurra algún evento o incidente de seguridad que involucre su red de comunicación de datos de La AGENCIA.
30. Los códigos de usuario deben ser utilizados única y exclusivamente en el local ubicado en la dirección para el cual haya sido solicitado.

31. En caso LA AGENCIA necesite trasladar un usuario de un local a otro, La AGENCIA deberá informar a TELEFÓNICA MÓVILES el nombre del usuario, la cuenta de acceso a la red y a los sistemas de TELEFÓNICA MOVILES que usa y el nombre del nuevo local desde donde ingresará el usuario para que TELEFÓNICA MOVILES permita ingresar el usuario desde ese nuevo local; de lo contrario, el usuario no podrá conectarse.

VIII. Conformidad

32. La AGENCIA deberá cumplir los controles determinados por el marco normativo que cautela la protección de datos de carácter personal y el Secreto de las Telecomunicaciones de acuerdo al nivel de seguridad de la información a que acceda su personal.
33. La AGENCIA y el personal de la AGENCIA únicamente podrán hacer aquello que se encuentre previsto de manera expresa y anteladamente respecto de los sistemas de TELEFÓNICA MÓVILES.
34. Es obligación de la AGENCIA devolver o destruir la información propiedad de TELEFÓNICA MÓVILES a la terminación del Contrato de Agencia.
35. Es obligación de la AGENCIA verificar la integridad de su personal que vaya a estar adscrito a la ejecución del Contrato de Agencia.
36. La AGENCIA deberá capacitar y concientizar en temas de Seguridad de Información e Ingeniería Social a su personal que accederá a los servicios de red y sistemas de TELEFÓNICA MÓVILES.
37. Es responsabilidad de la AGENCIA mantener la confidencialidad de las credenciales de acceso y no compartirlas con terceros no autorizados, así como comunicar a TELEFÓNICA MÓVILES cualquier anomalía o incidente. La AGENCIA está prohibida de hacer uso de los sistemas de TELEFÓNICA MÓVILES de forma que ponga en riesgo la confidencialidad, integridad y disponibilidad de la información, así como la seguridad y la reputación de ésta última.
38. Es deber de la AGENCIA que solicita cuentas de acceso para el personal a su cargo, disponer que el referido personal tome conocimiento de las disposiciones indicadas.
39. La AGENCIA declara tener conocimiento de las Políticas y Normas Corporativas de Seguridad de Información de TELEFÓNICA MÓVILES, las mismas que se obliga a cumplir, en su condición de tercero, en la ejecución del Contrato de Agencia.
40. TELEFÓNICA MÓVILES podrá verificar y comprobar que la seguridad de los equipos de la Agencia que se conecta sea suficiente, y que no ponga en peligro la seguridad de la red interna de TELEFÓNICA MÓVILES.

41. TELEFÓNICA MÓVILES se reserva el derecho de auditar y monitorizar el cumplimiento de los requisitos y controles de Seguridad establecidos en el Contrato de Agencia.

42. Con la finalidad de verificar el cumplimiento de estas Normas, el área de Seguridad de la Información de TELEFÓNICA MÓVILES podrá efectuar visitas periódicas a los locales donde se laboran con dichos usuarios y accesos para revisar que se cumpla con su buen uso. De conformidad con lo dispuesto en los artículos 1470°, 1471° y 1472° del Código Civil, la AGENCIA asume como propia la obligación de sus empleados de utilizar correctamente los sistemas de TELEFÓNICA MÓVILES así como sus respectivas cuentas de acceso personal y claves de acceso asociadas. El mal uso por parte de la AGENCIA, o de sus empleados, de sus respectivas cuentas de acceso personal y claves de acceso asociadas, entregados por TELEFÓNICA MÓVILES a la AGENCIA, podrá acarrear la resolución automática y de pleno derecho del Contrato de Agencia y de sus addendum, independientemente del cobro de las penalidades aplicables y el pago de la indemnización por daño ulterior que pudiese resultar de cargo de la AGENCIA, y de la responsabilidad penal personal que pudiese ser de aplicación.

Lima, de de 2013.

EL AGENTE **TELEFÓNICA MÓVILES S.A.**