Política de uso y seguridad en redes WI-FI

1. Información General.

Esta política de Uso Aceptable de la red Wireless *(5.1),* para [*proteger la integridad y confidencialidad de los datos e investigaciones*] en [SerRom Investigations SAU] (de aquí en adelante, la ***empresa***), así, como la protección de sus clientes, usuarios, productos, servicios, infraestructura de red, seguridad física y lógica, y promover la alta disponibilidad de los recursos que dispone. Se pretende instruir, concienciar, y regular el acceso a todos los recursos por parte de empleados y personal externo que visite o trabaje en la empresa. *Todos los usuarios están obligados a leer esta política, firmar, y, por último, entregar a su responsable asignado*.

2. Alcance de la política.

Se pretende dejar claro el correcto uso de la red Wireless *(5.1),* así como la seguridad implementada y las restricciones aplicadas.

3. Descripción de la política.

3.1 Uso General y Propiedades de la Política:

3.1.1 Uso Correcto de la red Wireless:

- Los ***empleados deberán usar sus dispositivos y el Punto de Acceso*** *(5.b)* ***asignados***, cumpliendo los acuerdos firmados en la ***"política de uso aceptable de los equipos y red de la empresa".***
- La red Wireless (5.1) será usada por dispositivos conectados para realizar streaming (5.3) en salas de reuniones y conferencias, mejorando la capacidad de comunicación, así, como la adaptabilidad de ubicación de la misma, sin requerir el uso exclusivo de un espacio determinado para ello. Cada empleado que requiera de dichos dispositivos para su uso, deberá autenticarse como se explicará en el punto "3.2.1 Autenticación de empleados" de esta política.
- Los empleados que requieran mover su equipo y hacer uso de la conexión a la red Wireless deberán rellenar una incidencia de uso en la intranet de la empresa cumplimentando un formulario con la Dirección MAC (5.4) de su dispositivo, e-mail de la empresa y motivo de la conexión Wireless, mediante la cual se le otorgará acceso por un tiempo limitado a esa red. Cada empleado deberá autenticarse como se explicará en el punto "3.2.1 Autenticación de empleados" de esta política.
- Las restricciones para empleados en el uso de la red vendrán explicadas en el punto "3.1.3 Seguridad de la red Wireless -> 3.1.3.2 Restricciones para empleados".

3.1.2 Uso Correcto de los Dispositivos y Red Wireless en la Empresa por Personas Ajenas de la misma:

- Toda persona ajena a la empresa que necesite la conexión a la red Wireless lo hará desde un dispositivo asignado a la misma una vez entre en la oficina de la empresa.
- Habiéndose registrado en la entrada y recepción del edificio, se le asignará este dispositivo con aplicaciones preinstaladas con el cual podrá realizar las comunicaciones y búsquedas que realice oportuno siempre y cuando cumpla los requisitos explicados en las restricciones de seguridad en el punto "3.1.3 Seguridad de la red Wireless -> 3.1.3.3 Restricciones para personas ajenas" de esta política.
- Para poder conectarse a la red desde el dispositivo, deberán realizar los pasos oportunos descritos en el punto "3.2 Autenticación -> 3.2.2 Personas Ajenas a la Empresa" de esta política, para poder conseguir la Autorización que les de acceso a la red Wireless (5.1).

3.1.3 Seguridad de la red Wireless:

3.1.3.1 Seguridad aplicada a la red Wireless:

- La red Wireless tendrá una ***SSID*** *(5.5)* ***oculta***, la cual se deberá introducir en la configuración de los dispositivos, por parte del equipo de seguridad, una vez tengan los dispositivos preparados los Administradores de la empresa.
- La contraseña de la red será de tipo ***WPA2*** (5.6), la cual deberá introducir el equipo de seguridad después de la SSID.
- Los dispositivos estarán en un ***Filtro de MAC*** (5.7) mediante el cual se evitará, más si cabe, la posibilidad de conexión de dispositivos externos de la empresa.
- El DHCP (5.8) de la empresa asignará IP al equipo, ya sea por red cableada o Wireless, pero la dirección IP de la red Wireless será usada para pasar un ***filtro de IP*** (5.9) para aumentar la seguridad.
- El dispositivo deberá tener instalado un ***certificado digital*** por el equipo de seguridad de la empresa, el cual deberá renovarse y está explicado en la *"política de actualizaciones y seguridad en equipos",* el cual será "solicitado" por la red Wireless como último paso antes de la autenticación final del dispositivo en la conexión a la red.
- El último paso, es la ***autenticación del factor humano*** (empleado/persona ajena) para poder tener autorización y acceso final a la red Wireless.
- Todos estos puntos excepto el anterior, serán *tareas realizadas por el equipo de seguridad* en el último paso de la configuración de dispositivos para empleados/personas ajenas, por lo que solamente las personas pertenecientes a dicho equipo, deben prestar atención a este punto.

3.1.3.2 Restricciones para Empleados:

- Las restricciones de los empleados una vez sean autorizados al uso de la red Wireless son las mismas que cuando hacen uso de la *red cableada*.

3.1.3.3 Restricciones para Personas Ajenas:

- Una vez sean autorizadas en la red Wireless las personas ajenas, deberán hacer *uso de las aplicaciones* de correo electrónico, o de la nube, *preinstaladas*, iniciando su sesión en ellas. *No podrán acceder a los sitios web de las mismas*.
- La navegación en internet, será exclusivamente, en páginas que sean del sector, siempre y *cuando pasen las reglas configuradas* en el firewall y proxy de la empresa.
- *No podrán seguir enlaces* externos a documentos.
- *Podrán enviar y recibir correos, nunca descargar* los elementos que contengan los mismos salvo que la fuente envidadora de ellos, en origen, sea nuestra empresa.
- Cualquier intento de instalar alguna aplicación en el dispositivo será rechazado debido a la configuración del mismo.
- No tendrán acceso a ningún recurso de la empresa compartido en red.

3.2 Autenticación

3.2.1 Empleados

- Deberán introducir el ***usuario y la contraseña*** de empleado en el proceso de conexón a la red Wireless.
- Una vez completado el paso, quedan los ***factores biométricos*** (huella dactilar en el lector de huellas del portátil) y la inserción de la tarjeta de empleado en el lector de ***smartCardID*** (5.J) conectado a su equipo.

3.2.2 Personas Ajenas a la Empresa

- Las personas ajenas a la *empresa* deberán haberse registrado en la entrada del edificio con su ***DNI, correo electrónico***, y una ***huella dactilar*** como indica la "*política de seguridad perimetral y física de la empresa*".
- Para poder conectarse a la red, deberán ir a la recepción de la oficina una vez lleguen, dejar sus datos, y motivo de la necesidad del acceso. *Deberá firmar* un papel en el cual *acepta las consecuencias en caso de mal uso*. Se habilitará ***un usuario y contraseña para dicho invitado***, los cuales serán las credenciales para el proceso de autenticación en la red Wireless *(5.a)*.
- Una vez completado el paso, quedan los factores ***biométricos*** (huella dactilar en el lector de huellas del portátil) y la inserción del ***DNI*** en el lector de smartCardID (5.J) conectado a su equipo.

3.3 Autorización

3.3.1 Empleados

- Una vez se pasen los 3 factores (al igual que en el AP), tendrán acceso a la red Wireless.

3.3.2 Personas Ajenas a la Empresa

- Una vez se pasen los 3 factores, tendrán acceso a la red Wireless.
- El ***DNI*** de la persona ajena será en esta instancia *"la tarjeta de empleado"* (habiéndose creado un fichero con los datos de dicha persona, los cuales están almacenados en su chip del DNIe).
- La ***huella dactilar*** se le pedirá en recepción para la lectura e inserción en una base de datos de personal ajeno (como el DNI) contra la cual se realizará *la autenticación del factor biométrico*

4. Consecuencias.

4.1 Empleados

- Todos los empleados son conocedores de la política una vez ésta es firmada y entregada a su responsable, lo que *conlleva su conocimiento*.
- Aquel empleado que realice un *mal uso de la red Wireless, será despedido*.
- Aquel empleado que realice un mal uso de la red Wireless, deberá atenerse a las *consecuencias legales* a las que el equipo de abogados de la empresa demande, con respecto a políticas y acuerdos de confidencialidad y secreto profesional firmados.
- Aquel empleado que realice un mal uso de la red y equipos de la empresa (cableada o Wireless) y *lleve a cabo tareas de investigación personal* o que no tienen nada que ver con la labor desempeñada en la empresa y su función, *serán objeto de reclamación de Propiedad Intelectual* como derecho de la empresa.

4.2.2 Personas Ajenas a la Empresa

- Debido a la naturalidad de la excepción en cuanto a la conexión, y al estar identificada la persona digital y biométricamente, *es responsable de las conexiones y comunicaciones* que realice desde el dispositivo que le proporciona una vez accede a la empresa y desde el cual deberá autenticarse para tener acceso a la red Wireless.
- Dichas personas, son conocedoras de la política una vez este firmada y entregada en la recepción, lo que *conlleva su aceptación*.
- Aquella persona ajena a la empresa que firma este documento, *deberá haber firmado* también los documentos correspondientes a los *acuerdos de confidencialidad y secreto profesional* que habrá debido firmar para poder entrar.
- Toda persona ajena que *introduzca* de cualquiera de las formas una unidad de almacenamiento, dispositivo electrónico, dispositivo de grabación, o cualquier aparato tecnológico no permitido por los acuerdos anteriormente firmados, y por ello suceda cualquier anomalía en la red de la empresa (cableada o Wireless), *será objeto de investigación* por parte de las autoridades pertinentes tras la correspondiente ***demanda presentada por nuestro equipo legal acorde a la ley de protección de datos, derechos y propiedad intelectual, y por último, a una demanda por espionaje industrial***.

- Aquella persona ajena de la compañía que además sea un *cliente de la misma*, ***si incumple las políticas*** de uso aceptable en la red Wireless que se relatan en este documento, *dejaran instantáneamente de ser clientes mediante la* ***extinción del contrato*** *vinculante entre ambas partes* (clausula incluida en el contrato).

5. Terminología.

5.A Red Wireless: Red WI-FI

5.B Punto de Acceso (AP): Toma de red a la que se conectarán físicamente los equipos asignados a cada empleado.

5.C Streaming: Reproducir videollamadas en la pantalla de la sala conectando un dispositivo que la soporte.

5.D Dirección MAC: Dirección de identificación única de la tarjeta de red física del equipo asignado, mediante la cual puedes tener acceso a la misma red.

5.E SSID: Nombre de la red WI-FI.

5.F WPA2: Protocolo de conexión inalámbrica con cifrado AES (algoritmo).

5.G Filtro de MAC: Compara la dirección MAC del equipo/dispositivo del empleado/persona ajena, con una lista completada por el equipo de seguridad.

5.H DHCP: Protocolo que asigna dirección IP a un equipo/dispositivo.

5.IFiltro de IP: Compara la dirección IP de red asignada al /dispositivo del empleado/persona ajena, con una lista completada por el equipo de seguridad.

5.J smartCardID: Lector de tarjetas inteligentes

6. Revisión Histórica.

Nombre	***Contacto***	***Fecha Revisión***
Sergio Romero Plaza	[email@email.com]	Noviembre 2018

Firma del empleado: Fecha: __ / __ /____ Firma Responsable: