Schmidt-Clemens Spain

POLÍTICA DE DISPOSITIVOS DIGITALES
| NORMAS DE USO E INDICACIONES DE SEGURIDAD |
Versión 1.0

1.-ÁMBITO DE APLICACIÓN.

La presente Política de uso de dispositivos digitales comprende las normas y condiciones de utilización de los servicios, recursos, dispositivos y medios digitales contratados, propiedad o en posesión de la ORGANIZACIÓN, que le hubieran sido facilitados o puestos a disposición de la PERSONA en el marco de la Relación que une a las Partes.

Sin ánimo limitativo, por "Medios Digitales" se entenderá tanto los recursos de tipo hardware (ordenadores, portátiles, impresoras, elementos de red, discos duros etc.), software (sistemas operativos, cliente de correo, navegador, etc.) como servicios (compartición de ficheros, redes sociales, correo, comunicaciones, etc.)

2.-PROHIBICIÓN DE USO PRIVADO SALVO AUTORIZACIÓN EXPRESA.

2.1.- La totalidad de los Medios Digitales tienen la consideración de recursos de trabajo. La PERSONA queda advertida de la prohibición expresa de utilización de tales Medios Digitales **para fines ajenos al cumplimiento de sus obligaciones y funciones, no pudiendo, en consecuencia, utilizar los Medios Digitales para un uso personal o privado, salvo que dicha posibilidad esté prevista en la presente política.**

2.2. Se entenderá que una utilización de los recursos es contraria a la presente política cuando dicho uso:

- pueda contemplar un riesgo para la seguridad informática de la ORGANIZACIÓN en especial si pudiera afectar a la integridad, disponibilidad y confidencialidad.
- afecte, limite o altere el uso de otros usuarios, por ejemplo, mediante el consumo del ancho de banda.

2.3. La PERSONA no podrá poner a disposición o dar acceso a ningún tercero ajeno a la ORGANIZACIÓN a los recursos o informaciones ubicados en los Medios Digitales.

2.4. Queda terminantemente prohibido la detención, deshabilitación, desinstalación o bloqueo de servicios y/o programas con los que la ORGANIZACIÓN haya equipado los Medios Digitales, en especial, software de antivirus, firewall, contraseñas y programas o servicios de monitorización y seguimiento de la actividad en el sistema.

2.5.- Los fallos o vulnerabilidades que puedan existir tanto en el hardware como en el software, incluyendo al respecto la ausencia o deficiente configuración de los mismos, no podrán servir de base para una utilización contraria a las presentes directrices, quedando por tanto prohibido su aprovechamiento.

3.-INDICACIONES DE SEGURIDAD.

3.1- SISTEMAS DE IDENTIFICACIÓN: NOMBRE DE USUARIO Y CONTRASEÑA.

- Los sistemas de identificación en los sistemas y servicios son de carácter personal e intransferible.
- En el caso de que el sistema esté basado en un nombre de usuario y contraseña, la PERSONA deberá elegir una contraseña (y en su caso un nombre de usuario) que sea compatible con los requisitos de seguridad establecidos. En el caso de la contraseña deberá tener al menos ocho (8) caracteres, con una mezcla de letras, números y símbolos.
- Queda prohibido que la PERSONA utilice la dirección de correo electrónica corporativa para darse de alta en cualquier servicio o portal ajeno a la ORGANIZACIÓN, y que no guarde relación con la

vinculación laboral, y a la reutilización de las contraseñas en otro tipo de sistemas, páginas web, servicios, etc. ya sean personales, de la propia ORGANIZACIÓN, como de terceros.

- Queda prohibida la revelación de la/s contraseña/s a cualquier tercero, sea personal de la ORGANIZACIÓN o no, sin la autorización expresa de la ORGANIZACIÓN. En el caso de que la contraseña sea conocida fortuita o fraudulentamente por terceros no autorizados, la PERSONA deberá comunicarlo de manera inmediata a la ORGANIZACIÓN para proceder a su cambio y para que se adopten las medidas de seguridad oportunas.
- La PERSONA no podrá en ningún caso autenticarse en el sistema con credenciales de otro usuario salvo que esté expresamente autorizada por la ORGANIZACIÓN o sea personal informático realizando funciones de mantenimiento, supervisión, configuración o similares de la infraestructura.
- Las contraseñas o sistemas de cifrado que la PERSONA pueda utilizar para el acceso y/o utilización de los Medios Digitales, no están implementadas para garantizar la privacidad de la utilización y acceso a los Medios Digitales ni de la información personal o profesional que pueda ser albergada en dichos Medios Digitales, sino como una garantía de seguridad informática.

3.2 ACCESO A LA INFORMACIÓN.

La PERSONA deberá acceder únicamente a la información que sea necesaria para el desarrollo de las funciones encomendadas. La mera posibilidad técnica de acceso a más información de la que pueda necesitar, no legitima dicho acceso. A los efectos oportunos se le informa de la monitorización y registro de todos los accesos y usos que pudieran realizarse de la información.

3.3. EXTRACCIÓN DE INFORMACIÓN Y SALIDA DE SOPORTES.

La PERSONA deberá solicitar autorización para cualquier extracción de información o Medio Digital (memoria USB, portátil, etc.) de la ORGANIZACIÓN. En el caso de que se le conceda dicha autorización, la PERSONA deberá extremar las medidas de seguridad y vigilancia fuera de las instalaciones y en caso de pérdida o sustracción del recurso, deberá ponerlo inmediatamente en conocimiento de la ORGANIZACIÓN.

3.4. UTILIZACIÓN DE RECURSOS AJENOS A LA ORGANIZACIÓN.

La PERSONA deberá solicitar autorización para la utilización o conexión de cualquier recurso o medio informático ajeno a la ORGANIZACIÓN. En especial, deberá abstenerse de conectar equipos ajenos a la red interna y/o conectar los recursos de la ORGANIZACIÓN a redes inalámbricas públicas o con una seguridad deficiente.

3.5. INCIDENTES DE SEGURIDAD: BRECHAS DE SEGURIDAD.

La PERSONA deberá notificar a la ORGANIZACIÓN cualquier incidente de seguridad del que pueda tener conocimiento que tenga relación con los Medios Digitales de la ORGANIZACIÓN.

4.-NORMAS DE USO DE DETERMINADOS RECURSOS

4.1.- SERVICIO DE CORREO ELECTRÓNICO.

4.1.1.-GENERALIDADES.

El correo electrónico y los servicios dependientes de éste, como calendario, contactos, y en su caso almacenamiento asociados, **tienen la consideración de un medio de trabajo y en ningún caso se facilitan para fines particulares**, debiendo destinarse por tanto a un uso profesional en el marco de la Relación existente.

No obstante, lo anterior, se autoriza el empleo de la misma para un ámbito personal siempre y cuando ello no interfiera en el trabajo y/o en la seguridad informática de la ORGANIZACIÓN.

En todo caso, la PERSONA debe tener presente que la información almacenada en los Medios Digitales puede ser eventualmente accedida por la ORGANIZACIÓN, especialmente si concurren los supuestos descritos en esta política, salvaguardando siempre el derecho al honor y a la intimidad.

4.1.2.-CORREO EN MOVILIDAD/DESDE EL EXTERIOR.

Será necesaria autorización expresa de la ORGANIZACIÓN para la descarga y/o sincronización del correo en dispositivos móviles, tales como, portátiles, "tabletas" o teléfonos móviles propiedad de la ORGANIZACIÓN.

En el caso de que el dispositivo sincronizado (como, por ejemplo, teléfono móvil, tableta, etc.) fuera extraviado y/o robado, la PERSONA deberá poner en conocimiento de la ORGANIZACIÓN dicha circunstancia a la mayor brevedad posible, aunque el mismo sea de su titularidad.

4.1.3.- ACCESOS AL BUZÓN DEL CORREO ELECTRÓNICO.

La ORGANIZACIÓN, en el caso de ausencia, baja laboral, vacaciones o cualquier motivo fundado, podrá en los casos en los que legalmente proceda:

- Insertar un mensaje de autorrespuesta, en el caso de que no lo haya hecho la PERSONA, o el que haya insertado no se ajuste al modelo y/o instrucciones establecidas por la ORGANIZACIÓN. El mensaje a insertar informará de que la cuenta de correo no va a ser atendida.
- Acceder a buzón de correo asignado a la PERSONA, incluyendo los mensajes de correo electrónico almacenados, o no leídos que sean profesionales, contactos, etc. en el caso de que la PERSONA no esté atendiendo la cuenta de correo durante su ausencia o sea necesario, a juicio de la ORGANIZACIÓN, acceder a determinada información para seguir prestando los servicios, realizar labores de mantenimiento informático y finalmente, verificar el cumplimiento de la presente política de uso de medios digitales, acuerdo de confidencialidad y/o desempeño en el trabajo.

En el caso de que durante la Relación la PERSONA se niegue a entregar aquella información contenida en su buzón que la ORGANIZACIÓN estime necesaria para la actividad de la misma, la ORGANIZACIÓN podrá acceder al buzón de la PERSONA a los efectos de localizar, acceder y tratar dicha información.

Una vez finalizada la Relación existente entre la PERSONA y la ORGANIZACIÓN, esta última, entre otras acciones podrá, respetando los límites marcados por la normativa:

a) Acceder al contenido del buzón, en los casos que legalmente proceda.

b) Eliminar cuando lo estime oportuno el buzón.

4.1.4.-FIRMA CORPORATIVA EN LOS CORREOS.

La PERSONA deberá utilizar la firma o firmas de correo facilitadas por la ORGANIZACIÓN que podrán incluir un "disclaimer" o descargo de responsabilidad por parte de la empresa.

4.1.5.- MENSAJES NO SOLICITADOS.

Queda prohibido el envío de mensajes de correo electrónico de forma masiva con fines ajenos al correcto funcionamiento de la ORGANIZACIÓN**.**

4.1.6.- ACCESO CORREO ELECTRÓNICO DE TERCEROS.

Queda prohibido intentar leer, borrar, copiar o modificar los mensajes de correo electrónico o archivos de otros usuarios. Sin perjuicio de las consecuencias que en el orden laboral pueda tener esta conducta, la PERSONA queda advertida de que dichas acciones pueden ser constitutivas de un delito contra la intimidad del artículo 197 del Código Penal.

4.2.-NAVEGACIÓN.

4.2.1.-La navegación web deberá emplearse en el ámbito de las funciones y tareas a desarrollar por la PERSONA en la ORGANIZACIÓN. La PERSONA queda autorizada expresamente a acceder a todo tipo de páginas que:

a) Guarden relación con las funciones a desarrollar en la ORGANIZACIÓN.

b) Sirvan de formación para la PERSONA, ya sea específica de su área de actividad como de cultura general y/o actualidad.

4.2.2.-No obstante, lo anterior, se permite un uso privado de la anterior herramienta, siempre y cuando la PERSONA consienta la monitorización de la actividad y la misma se realice bajo las siguientes condiciones:

a) No interfiera con las funciones y tareas desarrolladas por la PERSONA en la ORGANIZACIÓN. En este sentido no podrá afectar en ningún caso al rendimiento y/o productividad de la PERSONA en la ORGANIZACIÓN ni ocupar un tiempo que pueda considerarse excesivo.

b) No se ponga en riesgo la seguridad informática de la ORGANIZACIÓN.

c) No se consuma un ancho de banda excesivo o que en cualquier caso perturbe el uso de la red por parte de los demás usuarios y/o aplicaciones de la ORGANIZACIÓN.

d) No sea abusiva.

Queda excluido en todo caso, la utilización de los medios digitales propiedad de la ORGANIZACIÓN para la conexión a redes sociales, salvo las autorizadas para el cumplimiento de sus responsabilidades profesionales.

La navegación no amparada en alguno de los casos descritos en los apartados anteriores, será considerada contraria a la presente política y por tanto no autorizada.

4.3.-TELÉFONOS MÓVILES.

Se autoriza a la PERSONA la instalación de aplicaciones en los dispositivos móviles de la ORGANIZACIÓN puestos a su disposición y el uso personal de dichos terminales fuera del horario, siempre que dicho uso:

a) No interfiera con las funciones y tareas desarrolladas por la PERSONA en la ORGANIZACIÓN. En este sentido no podrá afectar en ningún caso al rendimiento y/o productividad de la PERSONA en la ORGANIZACIÓN.

b) No sea abusivo.

c) No suponga un coste adicional para la ORGANIZACIÓN o, en su defecto, cuente con el consentimiento expreso de la ORGANIZACIÓN.

Los usuarios de teléfonos móviles deberán ser muy cuidadosos en el uso de los terminales en el extranjero o en aquellas circunstancias que pueda haber un sobrecoste significativo, pudiendo asumir la PERSONA costes derivados de un uso inapropiado del teléfono móvil con fines lúdicos, como por ejemplo el visionado de películas, juegos, uso como navegador… El usuario, cuando sea posible, utilizará las conexiones wifi disponibles de empresas que visite, hoteles…

La PERSONA deberá tener el software del terminal totalmente actualizado, debiendo instalar a la mayor brevedad las actualizaciones tanto del sistema operativo como de las aplicaciones que se vayan liberando por los diferentes fabricantes, salvo que el Departamento de Informática determine otras instrucciones.

La PERSONA deberá establecer una contraseña de acceso al terminal, que deberá cambiar regularmente.

4.4.-CERTIFICADOS DIGITALES.

Los certificados digitales de representación y/o apoderamiento de la ORGANIZACIÓN únicamente podrán ser utilizados por la PERSONA para el cumplimiento legal de sus obligaciones laborales, debiendo finalizar su uso y dar de baja estos certificados una vez que finalice la RELACIÓN con la empresa y/o cese su nombramiento como apoderado de la ORGANIZACIÓN.

Los certificados digitales personales, podrán ser utilizados indistintamente personalmente como profesionalmente, en cuanto identifican a la persona, pero no necesariamente a la empresa. Cuando se hayan utilizado certificados digitales personales para autenticarse en páginas de organismos de uso profesional, deberá finalizar la autorización en dichas organizaciones.

5.- SISTEMAS DE CONTROL.

5.1.- La PERSONA queda advertida de la existencia de sistemas que registran de manera automática y en algunos casos de manera imprescindible gran parte de la actividad generada por los Medios Digitales, como por ejemplo, el proxy, controlador de dominio, servidor de impresión e impresoras, servidor de DNS, servicio de correo, sistema de filtrado antispam y antivirus, firewall perimetral, etc. que pueden registrar la actividad y usos de las herramientas informáticas empleadas por la PERSONA, como por ejemplo:

- Detalles de la navegación (como por ejemplo páginas visitadas, frecuencia, tiempo de permanencia…)
- Detalles de impresión de ficheros (fecha, nombre del fichero…)
- Uso de la red: Ip origen/destino y protocolo empleado para la comunicación de información.
- Flujo de envío y recepción de los correos electrónicos; detalles de la comunicación, tales como destinatario, asunto…
- Inicio, tiempo de sesión, recursos accedidos.
- Detalles de los ficheros accedidos en los servidores, como, por ejemplo, número de ficheros, acciones realizadas sobre los mismos (como copia, lectura, modificación etc.)
- Detalle de las llamadas efectuadas desde terminales de la ORGANIZACIÓN (datos de origen-destino de las llamadas, así como su duración).

El listado anteriormente facilitado no es exclusivo y pueden existir o crearse otros tipos de registros automáticos no programados que registren la actividad de los Sistemas Informáticos.

5.2.- Duración de la conservación de los registros: Los registros indicados en el punto anterior se mantendrán almacenados hasta la expiración de la prescripción de las acciones que pudieran existir derivadas de la Relación.

6.- SUPUESTOS QUE LEGITIMAN EL ACCESO.

La ORGANIZACIÓN podrá controlar y/o acceder a los Medios Digitales que utilice la PERSONA, por ejemplo, mediante el acceso a los registros generados por los servicios, servidores o programas; y/o el acceso a dichos recursos o la información que tratan en los siguientes supuestos:

- Cuando la ORGANIZACIÓN tenga indicios de cualquier acto ilícito, transgresión de la buena fe contractual o de la presente política de uso de Medios Digitales.
- Cuando se presente cualquier tipo de problema o incidencia de tipo de informático, ya sea a nivel de software o de hardware cuya solución precise dicho acceso o control, específicamente en caso de existencia de virus, troyanos o gusanos informáticos.

- Para la realización de operaciones de mantenimiento, configuración, instalación de nuevas aplicaciones, etc., que la ORGANIZACIÓN estime como oportunas de cara a la finalidad de las herramientas y servicios regulados en las presentes directrices.
- Con ocasión de la aplicación de la normativa de protección de datos y en concreto, con la aplicación de las medidas de seguridad que se puedan definir por parte de la ORGANIZACIÓN en base al análisis de riesgo.

7.-AUTORIZACIONES Y PERMISOS.

Las autorizaciones y permisos a las que hacen referencia la presente Política de Medios Digitales podrán ser otorgadas por cualesquiera miembros de Dirección de la ORGANIZACIÓN o del Departamento de Informática de la ORGANIZACIÓN.

8.-CONSECUENCIAS DE LA VIOLACIÓN DE LAS NORMAS.

La violación de las presentes directrices será considerada una utilización fraudulenta de los medios de trabajo que quiebra la buena fe y la diligencia exigible, por lo que puede ser sancionada con las medidas disciplinarias establecidas en el Convenio Colectivo y el Estatuto de los Trabajadores, pudiendo incluso ser causa de rescisión del contrato de trabajo, así como la responsabilidad civil y penal que pudiera derivarse de ese incorrecto uso.