GUÍA

DE USUARIOS DE LOS SISTEMAS DE INFORMACIÓN DEL GRUPO VINCI

JUNIO DE 2018

TABLA DE CONTENIDO

En caso de discrepancias entre la versión francesa y una traducción, prevalece la versión francesa.

PREÁMBULO

Los Sistemas de Información son vitales para garantizar el correcto funcionamiento y el rendimiento de la empresa. Dado que los actos malintencionados, la falta de vigilancia o una utilización incorrecta de los Recursos pueden entrañar importantes riesgos de cara a la competencia, de índole financiera, jurídica o de imagen, la concienciación y la responsabilización de los usuarios, así como el refuerzo de los medios de protección y de control son indispensables.

En ese marco, la presente Guía define:

- las reglas generales de utilización de los Recursos del Sistema de Información;
- las prohibiciones y los puntos de vigilancia sobre cualquier tipo de información, cualquier tipo de tratamiento de la información, todos los elementos de los Sistemas de Información, todas las herramientas de comunicación y todos los equipos que la empresa pone a disposición;
- los principios de protección y control que se pueden establecer.

La Guía precisa pues los derechos, deberes y obligaciones del usuario en lo que respecta al uso de los Recursos del Sistema de Información.

Ámbito de aplicación de la guía

La Guía se aplica a todos los usuarios de los Recursos del Sistema de Información de la empresa.

Se entiende por «usuario» toda persona, independientemente de su estatus en la empresa (asalariado, personal temporal, becario, consultor, prestatario...), que pueda utilizar dichos recursos.

Se entiende por «Recursos»:

- los equipos del Sistema de Información de cualquier tipo (en particular ordenadores, softwares, periféricos de impresión, redes internas, servidores compartidos, soportes de almacenamiento amovibles);
- los medios de comunicación de cualquier tipo;
- la información y los datos (en particular los ficheros y bases de datos).

El conjunto de esos Recursos que se proporcionan a los asalariados, así como su contenido son propiedad de la empresa.

La Guía se aplica en todos los países en los que el Grupo ejerce alguna actividad. Se puede completar en función de las necesidades mediante adiciones adaptadas a las características de los países y las entidades.

Normas generales de utilización de los recursos

Acceso a los Recursos

Las autorizaciones de acceso a los Recursos son expedidas por la empresa a cada usuario en función de su papel y de sus misiones.

Esas autorizaciones son estrictamente personales y no pueden, por principio, en ningún caso, ser cedidas, prestadas o transmitidas, sea de la forma que sea, a un tercero de dentro o de fuera de la empresa, incluso temporalmente.

Toda modificación del estatus profesional del usuario puede acarrear una modificación de las autorizaciones.

Toda nueva autorización ha de ser objeto de una solicitud previa específica en virtud de los procedimientos vigentes.

Las autorizaciones pueden suspenderse, modificarse o retirarse de acuerdo a los procedimientos de habilitación y de gestión de los accesos, en particular, en caso de que se identifique un riesgo para el correcto funcionamiento de los Sistemas de Información.

Todas las autorizaciones finalizan con la suspensión o cese de la actividad profesional, lo más tardar, con el fin del contrato de trabajo.

Principio de uso de los Recursos

Los Recursos se proporcionan a los usuarios con fines de uso profesional, en el marco de sus atribuciones y de conformidad con la misión que les asigna su contrato.

La totalidad de los Recursos así como su contenido son propiedad de la empresa. No obstante, el usuario es responsable de ellos y contribuye, a su nivel, a su seguridad.

La utilización de esos Recursos no ha de implicar la responsabilidad de la empresa ni socavar su imagen.

Asimismo, estos Recursos no deben en ningún caso:

- ser utilizados para llevar a cabo actividades personales de carácter comercial;
- trabar o limitar el uso profesional de los Recursos de la empresa, su mantenimiento o su seguridad (lo que incluye su confidencialidad, disponibilidad y su integridad).

El usuario no debe llevar a cabo en ningún caso ningún tipo de actividad sea cual sea que vulnere la ley o que pueda menoscabar la imagen de la empresa o la seguridad, integridad o rendimiento del Sistema de Información de la empresa.

Derecho a la desconexión

Las modalidades del derecho a la desconexión indicadas a continuación están destinadas a sensibilizar y responsabilizar a los usuarios.

Por consiguiente, se invita* a los usuarios a:

- abstenerse de enviar emails y mensajes de texto, así como de efectuar llamadas fuera de los horarios de trabajo habituales;
- acudir, de ser el caso y si lo permite el cliente de mensajería, a la función de envío diferido de los mails;
- indicar en sus mensajes un término de vencimiento del plazo de respuesta;
- dar a conocer su no disponibilidad mediante un mensaje de ausencia y remitir, de ser posible, a un interlocutor disponible;
- desactivar las notificaciones de mails fuera de los horarios de trabajo habituales.

Igualmente se recuerda a los usuarios que no es obligatorio dar respuesta a los mails, llamadas o mensajes de texto fuera de las horas de trabajo habituales*.

Finalmente, cabe resaltar la importancia del ejemplo dado por los managers en cuanto al uso razonable y razonado de las herramientas digitales.

Uso de los servicios de Internet

El acceso a Internet se concede individualmente a los usuarios y se pone a su disposición para un uso profesional. Se parametra y administra a tal efecto.

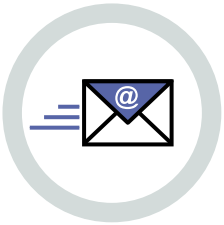
Para no debilitar el nivel general de seguridad, el usuario debe usar los servicios de Internet cumpliendo la ley y las normas de las páginas que visita.

No debe:

- conectarse o intentar conectarse de otra forma que no sea mediante el acceso a internet oficial proporcionado a través de la red de la empresa;
- consultar páginas que puedan suponer un riesgo para la seguridad de los Recursos o violar la confidencialidad de la información;
- de forma general, utilizar servicios de Internet con fines comerciales, lúdicos o ilícitos.

* Salvo casos especiales, por ejemplo del tipo trabajo por turnos.

Además, se recuerda que, en el marco de la ejecución de su contrato, todos los empleados están sujetos a la obligación de lealtad. Esta obligación también se aplica en los espacios públicos de internet y, especialmente, en los blogs, foros y redes sociales. Toda divulgación, en ese tipo de sitios, en todo media social o en Internet en general, de información propiedad de la empresa o que dañe su imagen está estrictamente prohibida.



Utilización de los sistemas de mensajería electrónica

El acceso a la mensajería electrónica de la empresa se pone a disposición de los usuarios para un uso profesional. Se parametra y administra a tal efecto.

Por imperativos de disponibilidad y de rendimiento de los Recursos, se ha de limitar el volumen y el número de mensajes. La dirección de los Sistemas de Información se reserva el derecho de limitar el tamaño máximo de los mensajes, buzones y algunos tipos de ficheros adjuntos.

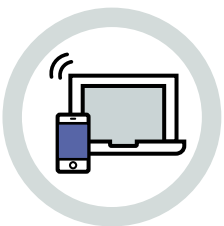
Cuando se difunde un mensaje, se ha de prestar especial atención a la pertinencia de la lista de destinatarios, a su presentación, a su contenido, a su tamaño.

El usuario velará por aplicar las normas siguientes:

- redactar explícitamente el asunto del mensaje;
- utilizar las listas de difusión internas y externas con precaución;
- ser especialmente cuidadoso con cualquier comunicación de datos de carácter personal (ver el apartado Sobre la protección de los datos personales en la pág. 10);
- no transmitir a nivel interno mensajes que puedan contener virus (en caso de duda, póngase en contacto con la dirección de Sistemas de Información);
- no enviar fuera de la red de la empresa mensajes o documentos adjuntos con contenido confidencial (de ser necesario, póngase en contacto con la dirección de Sistemas de Información) o que puedan dañar la reputación de la empresa;
- no transmitir fuera del Grupo tarjetas de direcciones u organigramas.

En lo que respecta a la recepción de mensajes:

- cualquier mensaje dudoso, no legítimo, no solicitado (remitente y nombre de dominio desconocido, mensajes sin asunto, asunto sensacionalista o atrayente, etc.) deberá eliminarse sin abrirlo ni hacer clic en los enlaces o archivos adjuntos que contenga;
- el usuario procurará ser especialmente prudente a la hora de suscribirse a listas de distribución públicas, que, a menudo, son origen de mensajes publicitarios no solicitados (spam) y propagan virus mediante la suplantación de identidad.



Movilidad

Los usuarios de ordenadores portátiles y de todo tipo de terminales móviles se comprometen a proteger y a velar escrupulosamente por su material y por el acceso a los datos que contiene, sea cual sea el lugar en el que se encuentren, en el territorio nacional o en el extranjero, y en particular, en los transportes públicos o colectivos.

En caso de que desaparezca un equipo del Sistema de Información como consecuencia de su pérdida o del robo presunto o fehaciente de éste el usuario debe imperativamente avisar, por todos los medios de que disponga y a la mayor brevedad, a la dirección de Sistemas de Información, para que se adopten las medidas indispensables para la protección del Sistema de Información de la empresa.

Paralelamente, informará a sus superiores del evento para que se pueda llevar a cabo una evaluación del perjuicio potencial que ello conllevaría para la empresa.

En caso de conexión a la red de la empresa desde un lugar público o un puesto de trabajo que no pertenezca a la empresa, el usuario deberá procurar no registrar su contraseña de conexión desde el navegador de Internet, desconectar todas las sesiones abiertas, eliminar el historial de navegación y cerrar los programas que utilizó para establecer la conexión.

Asimismo, el usuario procurará no almacenar información de carácter profesional en equipos que no sean los que la empresa ha puesto a su disposición.

Por último, todo usuario deberá de conectar su ordenador portátil a la red de la empresa con la mayor frecuencia posible para que las operaciones de mantenimiento, actualización de los medios de protección se efectúen de conformidad con la política de seguridad de la empresa o con las buenas prácticas existentes en la materia.

Adecuación de los materiales, programas y aplicaciones

Material

Con el fin de garantizar una óptima adecuación entre los equipos individuales (ordenadores, estaciones de trabajo, etc.), las aplicaciones del Sistema de Información y la red, la empresa proporciona configuraciones estándar. Por ende, la validación previa por parte de la dirección de Sistemas de Información de toda instalación de equipamiento que no hubiere facilitado, incluso tratándose de materiales estrictamente idénticos a los ya desplegados, es obligatoria.

Los soportes de almacenamiento amovibles (tipo lápices de memoria o discos duros externos) pueden transmitir virus a los puestos de trabajo y a la red. Es obligatorio usarlos con prudencia y más especialmente cuando procedan de fuera de la empresa. En caso de duda, el usuario deberá ponerse en contacto con la dirección de Sistemas Informáticos, que llevará a cabo los oportunos controles de seguridad.

Por otra parte, habida cuenta de que se pueden perder o robar con facilidad por ser tan pequeños, es imperativo borrar los ficheros una vez realizada la transferencia de datos.

Por último, en caso de que no hubiere una configuración predefinida para una determinada necesidad, el usuario ha de ponerse en contacto con la dirección de Sistemas de Información para estudiar la solución que mejor se adapte a esa necesidad en cuestión.

Préstamo y reventa de material

Está prohibido prestar, vender o ceder a terceros los equipos facilitados por la empresa.

Programas y aplicaciones

Las configuraciones de softwares son definidas por la empresa con el fin de atender las necesidades de los usuarios. Todo intento de modificación de la configuración inicial está proscrito dado que podría provocar importantes deficiencias de los Recursos (incidencia en el rendimiento, la seguridad, etc.).

En caso de que no hubiere una configuración predefinida para determinada necesidad, el usuario ha de ponerse en contacto con la dirección de Sistemas de Información para estudiar la solución que mejor se adapte a esa necesidad en cuestión.

Por último, para garantizar un nivel constante de seguridad y de rendimiento, está prohibido bloquear los procesos automáticos de actualización de los softwares.

Desarrollos informáticos individuales

Los desarrollos informáticos a partir de herramientas ofimáticas (macros, bases de datos, etc....) y su mantenimiento están bajo la total responsabilidad de los usuarios que los hayan originado.

Préstamo y reventa de software o de licencia

De conformidad con la legislación en materia de propiedad intelectual, la empresa abona el canon de uso y de licencia de los softwares.

Por ello, está prohibido prestar, vender o ceder a terceros los softwares, licencias, programas de instalación y las herramientas que haya facilitado la empresa. Esta prohibición se aplica también a los softwares desarrollados por los equipos informáticos de la propia empresa.

Seguridad y protección de datos

Cada usuario contribuye a la seguridad y a la protección de los Recursos, en particular de los datos procesados, y se compromete a no esquivar, perturbar, trabar, interrumpir o suprimir voluntariamente los dispositivos de seguridad (antivirus, etc....), de filtrado o de control desplegados por la empresa.

El usuario debe avisar lo antes posible a la Dirección de Sistemas de Información sobre cualquier disfuncionamiento constatado o sobre toda anomalía descubierta, como por ejemplo una intrusión en el Sistema de Información, etc. Debe asimismo notificar a su responsable jerárquico toda posibilidad de acceso a un recurso que no corresponda a su habilitación.

En lo relativo a la mensajería electrónica e Internet

La mensajería electrónica deja de ser un canal de comunicación seguro en cuanto se envía un mensaje fuera de la empresa.

Es cierto que la empresa puede controlar su red interna, pero no tiene ninguna visibilidad ni posibilidad de acción en lo que respecta a los datos que transitan por la red de Internet pública. Por ello, es preciso calibrar la sensibilidad de la información antes de transmitirla por esa vía a terceros que no sean de la empresa.

Por otra parte, los mecanismos de protección de ficheros ofimáticos gracias a las contraseñas que proponen las aplicaciones de edición (Word, Excel, Powerpoint, PDF, etc.) no constituyen una protección eficaz, dado que existen numerosos softwares libremente accesibles en Internet con los que éstas pueden ser fácilmente vulneradas.

Por ello, si por imperativos profesionales el usuario tiene que intercambiar con un tercero que no sea de la empresa información especialmente sensible, se pondrá en contacto con la dirección de Sistemas de Información de la que depende para obtener una solución adaptada a la necesaria confidencialidad y compatible con los Recursos de la empresa.

Cuando la empresa tiene la obligación legal de establecer un sistema de registro* y filtrado** de los accesos a Internet, de la mensajería y de los datos compartidos, presentará las declaraciones necesarias a las autoridades de control competentes.

En lo relativo a la utilización de medios criptográficos

El usuario tiene la obligación de utilizar únicamente soluciones aprobadas por la empresa para proteger sus datos.

En lo relativo a la protección del puesto de trabajo

Las autorizaciones de acceso a los Recursos, incluido el puesto de trabajo, se expiden personal y nominalmente al usuario. En ese contexto, para evitar que un tercero acceda a ellos, sea quien sea, incluido de forma puntual, cada usuario tendrá que:

- aplicar la política de la empresa relativa a las contraseñas (renovación, longitud suficiente, complejidad, etc.) para acceder a los Recursos;
- mantener secretas las contraseñas que en ningún caso han de cederse, prestarse o transmitirse de la forma que sea a un tercero sea o no sea de la empresa, incluso temporalmente (sin perjuicio de las necesidades urgentes de servicio, en cuyo caso se deberá modificar la contraseña);
- bloquear su puesto de trabajo cuando se ausente y apagarlo al final de la jornada y durante el fin de semana, salvo imperativo técnico relacionado con el mantenimiento de los Recursos o necesidad operativa;
- no aprovechar y/o publicar cualquier eventual fallo de la seguridad que afecte a los Recursos que le hayan sido facilitados y del que tendría conocimiento, e informar de ello a la mayor brevedad a la dirección de Sistemas de Información;
- no intentar eludir o inhibir los sistemas de protección instalados en los puestos de trabajo (antivirus, cortafuegos, etc.);
- utilizar los medios que la empresa ha puesto a su disposición para proteger los puestos de trabajo;
- realizar los guardados de su puesto de trabajo. En caso de anomalía, informará de ello a la dirección de Sistemas de Información.

En lo atinente a las intervenciones a distancia en la sesión del usuario, éstas sólo se podrán llevar a cabo previa solicitud de asistencia del usuario, o previa solicitud de la dirección de Sistemas de Información y con la autorización de los superiores correspondientes. Sólo el personal habilitado por la empresa para ello tiene permiso para intervenir en los Recursos que se hayan facilitado a los usuarios.

* Conservación de la información técnica de conexión, tales como la hora de acceso, la dirección IP del usuario.

** La implantación de un filtrado de acceso a las páginas Internet puede requiere, de ser necesario, descifrar los datos intercambiados entre el equipo del usuario y el sitio Internet. Este análisis se realizará de manera global: los datos descifrados no se registrarán (información inaccesible). La recogida diaria de los flujos descifrados es equivalente al registro configurado para los flujos HTTP estándares (hora, cuenta de usuario, URL del sitio Internet, autorización de acceso, virus identificado). No se registrará ninguna información adicional.

En lo relativo a la continuidad de la actividad

Para garantizar la continuidad de la actividad, el usuario, de ausentarse, ha de poner en marcha las delegaciones necesarias para que se pueda acceder a sus datos profesionales y no debe comunicar sus códigos de acceso a terceros.

El usuario debe igualmente salvar y archivar con frecuencia los datos que explota, crea o transforma en aras de la continuidad del servicio, valiéndose de los softwares, materiales y/o procedimientos que la empresa pone a su disposición y en particular los espacios de red.

Cuando cese su actividad, el usuario tiene la obligación de devolver a la empresa, además del material que se le ha asignado, los archivos, carpetas, ficheros, correos electrónicos, y, en general, todo documento electrónico de carácter profesional en aras de la continuidad de la actividad.

Sobre la protección de los datos personales

En el ejercicio de sus funciones, los usuarios pueden tener que acceder a datos de carácter personal (salarios, clientes potenciales, colaboradores, etc.) y declaran reconocer la confidencialidad de dichos datos.

Por «datos de carácter personal» se entiende toda información que se refiera a una persona física identificada o identificable; se considera una «persona física identificable» a una persona física que se puede identificar de forma directa o indirecta, en particular, por un identificador como un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos específicos pertenecientes a su identidad física, fisiológica, genética, psicológica, económica, cultural o social.

Por consiguiente, los usuarios deben tomar todas las precauciones necesarias en el marco de sus funciones para proteger la confidencialidad de la información a la que tienen acceso y, en particular, impedir que se comuniquen a personas que no estén expresamente autorizadas para recibir esa información.

Por ello, se invita a los usuarios a:

- no utilizar, reproducir o utilizar los datos de carácter personal a los que pueden acceder con otros fines que no tengan que ver con sus funciones;
- divulgar estos datos únicamente a las personas debidamente autorizadas en razón a sus funciones, para recibirlos, tanto si se trata de personas particulares, públicas, físicas o jurídicas y en los casos expresamente previstos por los procedimientos de la empresa;
- no hacer ninguna copia de estos datos, salvo que sea estrictamente necesario para la ejecución de sus funciones;
- tomar todas las medidas necesarias en el marco de sus funciones para evitar el uso no adecuado o fraudulento de estos datos;
- informar lo antes posible a su superior jerárquico de cualquier comunicación a terceros no autorizada, pérdida, destrucción o alteración accidental de datos de carácter personal;
- tomar todas las medidas necesarias, especialmente de seguridad, para proteger la privacidad física y lógica de estos datos (por ejemplo: obligación de introducir un identificador/contraseña y de mantener secreta la contraseña de conexión a los recursos).

Control del uso de los recursos

De conformidad con los principios de transparencia y proporcionalidad, con fines de seguridad, de verificación del correcto acceso a los Recursos de la empresa, de correcto funcionamiento del Sistema de Información, y con el fin de que no se comprometa su responsabilidad penal o civil por el uso que los usuarios hagan de los Recursos, la empresa se reserva la posibilidad de realizar verificaciones y controles regulares.

Por las razones que anteceden, la empresa establece y garantiza el correcto funcionamiento de dispositivos de filtrado y de control (en particular cortafuegos, sistemas de control de los accesos y sistemas de trazabilidad) relativos a la utilización de los Recursos de la empresa (en particular, Internet, la mensajería electrónica, los servidores de redes compartidas, la telefonía fija o la móvil).

Estos sistemas pueden desplegarse, en particular en lo tocante a la mensajería electrónica, con el fin de controlar todo mensaje entrante o saliente (control de virus, control antispam, control de integridad, control del tamaño, lista de destinatarios, etc....), y también con el fin de bloquear, en particular sobre la base de una lista de palabras clave, los mensajes, intercambios electrónicos o los accesos a sitios no autorizados.

Implementación

Difusión

Las entidades del Grupo se encargarán de difundir el presente documento.

Cumplimiento de la normativa vigente

En virtud del uso de los recursos puestos a su disposición, el usuario se compromete a cumplir tanto la presente Guía como las disposiciones legislativas y normativas vigentes en su país.

Sanciones

El incumplimiento de las normas y medidas de que consta la presente Guía puede implicar la responsabilidad personal del usuario, o si se tratara de un prestatario, la responsabilidad de la sociedad que le emplee. En caso de que se demostrara que le son personalmente imputables infracciones a las mismas, el usuario se expone en su caso a sanciones disciplinarias, en virtud de las normas internas (en particular del reglamento interno en caso de que exista), e incluso a acciones judiciales, a tenor del derecho aplicable.

LOS VERDADEROS ÉXITOS SON LOS QUE SE COMPARTEN

Edición de junio de 2018 – GSI-2018-06-ES – Fotografía: rawpixel.com from Pexels – Diseño: www.gcommeuneidee.com

VINCI
1, cours Ferdinand-de-Lesseps
92851 Rueil-Malmaison Cedex
Tel.: + 33 1 47 16 35 00
www.vinci.com