Arabako Kalkulu Gunea, A.B.
Centro de Cálculo de Álava, S.A.

MANUAL DE BUEN USO DE LOS SISTEMAS DE INFORMACIÓN PARA EMPRESAS PROVEEDORAS

-MSGUSIEX-

Versión 1.1

ÍNDICE

1. ENTORNO

Las relaciones establecidas con terceras entidadespor parte del Centro de Cálculo de Álava, S.A. (en adelante CCASA), implican el acceso a la información y a los Sistemas de Información del CCASA o de sus entidades cliente, con lo que se hace necesario establecer las medidas de seguridad, organizativas y técnicas que protejan esta información y los sistemas que la tratan. El acceso a este tipo de información acarrean unas responsabilidades a las personas usuarias, que han de respetar:

- los derechos de otras personas usuarias (del CCASA y ajenas a la organización)
- la integridad de los sistemas de información y de los recursos físicos (propios y de terceras entidades)
- la disponibilidad de los recursos (del CCASA y de terceras entidades)
- las leyes y regulaciones vigentes.

Nota aclaratoria:

A lo largo de la norma se hace referencia a la "propiedad" de elementos del CCASA. Debe entenderse que el concepto de propiedad se refiere exclusivamente a la concesión de uso realizado por la DFA para uso interno del CCASA o para la gestión de clientes del CCASA.

De la misma manera, se entiende como "personal externo" al personal de empresas, personal en prácticas, servicios de vigilancia, etc. que prestan servicios al CCASA.

Por último, las referencias a "*personas usuarias*" se refieren al personal externo con acceso a los sistemas de información propiedad de CCASA, independientemente de que los sistemas de información se encuentran en infraestructuras gestionadas por CCASA o no.

2. OBJETIVO

El objetivo del presente documento es asegurar la correcta utilización de los Sistemas de Información que facilitan la realización de la misión del CCASA.

3. ALCANCE

Agentes

Este manual es de aplicación para todas las *personas usuarias* desde el momento en que hagan uso de los recursos expuestos en el siguiente apartado.

El personal de otras organizaciones clientes del CCASA, que comparten activos informáticos o de comunicaciones con el CCASA se rige por las políticas, normas, manuales, etc. propios de su organización.

Recursos

Las normas establecidas en este manual son de aplicación a todos los sistemas de información e infraestructuras, así como a la información que alberguen, gestionen, pertenezcan o estén administrados por CCASA, para consumo propio o de sus entidades cliente.

4. NORMAS DE USO

A continuación se definen una serie de normas que regulan el buen uso, disponibilidad y nivel de servicio de los Sistemas de Información del CCASA. Aquellos *personas usuarias* que de forma reiterada o deliberada o por negligencia las ignoren o las infrinjan, se pueden ver sujetas a las actuaciones técnicas (para minimizar los efectos de la incidencia) o contractuales que el CCASA estime oportunas.

Las actuaciones de CCASA, en relación a los puntos referidos en el presente documento, cumplirán estrictamente todas las obligaciones derivadas de la legalidad vigente, respetando en todo momento los derechos de las *personas usuarias*.

Los sistemas de información disponibles en CCASA **se deben utilizar con fines estrictamente profesionales, no estando autorizado su uso para intereses personales**.

Por otra parte, **CCASA prohíbe almacenar información personal** en los recursos compartidos que pone a disposición de las *personas usuarias*. Además, CCASA recomienda no almacenar información personal en los puestos de trabajo (PCs, portátiles, etc.) al poder ser utilizados por otras personas; siendo las *personas usuarias* conscientes de que no pueden reclamar a CCASA ni la información personal albergada en dichos equipos, ni responsabilidades por el acceso de otras personas a dicha información.

Las *personas usuarias* deben respetar la integridad de los recursos sobre los que se soportan, los derechos de otras *personas usuarias*, las leyes y regulaciones vigentes.

CCASA pone a disposición de todas las *personas usuarias* a la persona Responsable de Seguridad, para resolver cualquier duda o comunicar las sugerencias relacionadas con la seguridad de la información que entiendan oportunas. Así mismo, las empresas proveedoras que no conocieran normas, procedimientos, guías, etc. que se refieren en la presente norma han de contactar con la persona Responsable de Seguridad de CCASA para obtener copia de las mismas.

4.1. Confidencialidad de la información

El contrato firmado entre CCASA y la empresa proveedora de servicios establece cláusulas relativas a la confidencialidad de la información. Las *personas usuarias* han de ser conocedores de las citadas cláusulas, siendo deber de la empresa proveedora informar de las mismas.

Además de las cláusulas específicas de cada contrato, toda *persona usuaria* debe cumplir el Compromiso de Confidencialidad que CCASA tiene con sus entidades cliente:

> "I. El personal que presta sus servicios a CCASA, en el ejercicio de sus funciones, tiene acceso autorizado a datos de carácter personal, información de negocio de CCASA y de sus clientes.
>
> II. Dicho personal tiene la obligación de secreto profesional respecto a la información especificada en el punto anterior, así como el deber de guardarlos y, en especial a la adopción de las obligaciones y deberes relativos al tratamiento de datos de carácter personal y demás normativa legal o interna vigente.
>
> III. Estas obligaciones subsistirán aún después de finalizar su relación con CCASA.
>
> IV. El citado personal tiene responsabilidad frente a CCASA, a los efectos de resarcir los daños y perjuicios que se pudieran ocasionar, derivados de un incumplimiento culpable, de las obligaciones en materia de confidencialidad y protección de datos de carácter personal propias de su puesto de trabajo.".

Las *personas usuarias* tienen el deber de proteger la información a la que tenga acceso como consecuencia de las tareas encomendadas por CCASA.

Una vez finalizada la relación contractual con CCASA, las *personas usuarias* se comprometen a no utilizar la información o conocimiento obtenido durante la relación contractual en beneficio propio o de terceras entidades. Además, toda información propiedad de CCASA o de sus entidades cliente debe ser devuelta o destruida, acreditando en su caso la destrucción, según el criterio indicado en cada caso por CCASA.

4.2. Política de claves y control de accesos

Las *personas usuarias* que necesiten acceder a los sistemas de información de CCASA, disponen de una tarjeta con certificado electrónico ó de un Identificador personal junto a una Clave para acceder a los mismos.

Los sistemas de información propiedad de CCASA deben disponer de mecanismos para identificar a las *personas usuarias* que acceden, así como para controlar si están autorizados a acceder a los recursos y el modo (lectura, modificación, etc.) en que pueden realizar el acceso. Por ello, las *personas usuarias* deben utilizar exclusivamente los identificativos asignados a su persona, manteniendo en secreto las pertinentes contraseñas, PINs, etc., y siendo responsables de las acciones que se ejecuten con su identificativo.

Quienes administran los Sistemas y el personal de soporte (incluido personal externo que ejecute estas funciones) puede acceder, exclusivamente por motivos de mantenimiento y/o de seguridad, a aquellos ficheros personales, de CCASA o de sus entidades cliente que les permitan detectar, analizar y seguir las trazas de una determinada incidencia; manteniendo en todo momento el deber de secreto y requiriendo autorización del Responsable de Seguridad para permitir el acceso de terceros a recursos del CCASA o de sus clientes.

4.3. Bloqueos de sesión y equipos desatendidos

Las *personas usuarias* deben bloquear la sesión siempre que se ausenten del ordenador durante un periodo prolongado de tiempo. En los equipos conectados al dominio de DFA-CCASA, la sesión se bloquea automáticamente por inactividad de acuerdo con la política de puesto establecida en DFA-CCASA. Se recomienda que los equipos con acceso a sistemas de información propiedad de CCASA, que no se encuentren conectados al dominio de DFA-CCASA, habiliten políticas que los bloqueen automáticamente tras un periodo de inactividad.

4.4. Licencias y aplicaciones

Las *personas usuarias* de los sistemas de información no deben utilizar programas (malware, virus, troyanos, etc.) que puedan dañar otras máquinas o sistemas de seguridad.

Las *personas usuarias* de los sistemas de información deben respetar las condiciones de licencia y copyright del software que utilicen. El CCASA facilita, al personal externo con equipos conectados a la red de DFA-CCASA, el software necesario para el correcto desempeño de sus funciones, estando dicho software autorizado en la “Plataforma de Software” de CCASA o en proceso de estudio. Por lo tanto, todo software que se utilice en equipos propiedad de CCASA debe estar debidamente licenciado.

Quienes no utilicen equipos propiedad de CCASA son responsables de los daños derivados por el uso ilegal de software, no responsabilizándose CCASA de ninguna de estas instalaciones.

Por último, la información en formato electrónico sujeta a derechos de autor deberá ser usada de acuerdo a la legislación vigente (Propiedad Intelectual, etc.).

4.5. Herramientas de comunicación

El correo electrónico, las listas de distribución, servicios en la nube (almacenamiento, etc.), herramientas colaborativas, intranet/extranets, servicios de mensajería instantánea o foros de discusión son herramientas que facilitan la comunicación entre las personas, así como la difusión de información a varios interlocutores de una sola vez.

Por ello, las *personas usuarias* son responsables de todas las actividades realizadas con este tipo de herramientas de comunicación que pudiera facilitar CCASA. Estas personas deben utilizar estos servicios de comunicación para actividades personales que tengan relación con las propias del desempeño laboral, evitando en todo momento el envío de mensajes con contenido fraudulento, ofensivo, obsceno o amenazante, cartas encadenadas, esquemas piramidales o actividades similares, o cuyo contenido atente contra los derechos reconocidos en la legalidad vigente. Así mismo, no está permitido el envío al exterior de información de CCASA que no sea pública y que pudiera comprometer los intereses de la organización.

Las *personas usuarias*, con cuenta de correo facilitada por CCASA, aceptan que el correo catalogado por el CCASA como correo indiscriminado (spam), podrá ser borrado. Además estas personas podrán solicitar, a nivel personal, su deseo de no recibir correo clasificado como SPAM.

Por otra parte, CCASA puede bloquear el envío y/o recepción de ciertos tipos de ficheros en función de directrices de seguridad y/o rendimiento de los sistemas de información.

4.6. Infraestructura de comunicaciones

El CCASA dispone de una infraestructura de comunicaciones diseñada para facilitar la conectividad de la organización internamente y hacia el resto de organizaciones/personas. El diseño de esta infraestructura de comunicaciones ha sido realizada en base a unos consumos habituales de la organización y siguiendo metodologías que mejoren la eficacia, eficiencia y seguridad de las mismas.

Por ello, no está permitido la instalación de ningún servicio telemático (Servidor de Correo electrónico, Servidores Web, FTP, etc.), ni ningún dispositivo de comunicaciones en la red gestionada por CCASA sin la autorización expresa de las personas encargadas de administrar las infraestructuras de CCASA.

Además las *personas usuarias* no deben utilizar la infraestructura de comunicaciones para la apropiación indebida, destrucción o manipulación de información que circule por la red de CCASA o de terceros, o para ocultar o manipular su identidad.

El personal que administra las infraestructuras, o el personal en el que se delegue, está exento de estas restricciones con la única condición de que su actividad debe de estar orientada a acometer acciones planificadas o la resolución de incidencias.

4.7. Accesos a la red y Servicios de Internet

Las *personas usuarias deben* evitar acaparar recursos compartidos de forma que impidan a integrantes de la propia organización o de terceras realizar sus tareas de forma eficiente. CCASA puede habilitar mecanismos para limitar el acceso a los servicios de red e Internet.

En el caso de que las *personas usuarias* necesiten utilizar los recursos de la organización para emitir/recibir información, que sospechen pudiese generar la posibilidad de bloqueo al resto de *personas usuarias*, se deben coordinar estos envíos/recepciones con el personal encargado de administrar la infraestructura.

Como se ha expuesto anteriormente, cada *persona usuaria es* responsable del buen uso del equipamiento y la red que CCASA pone a su disposición. Existen determinados recursos (servidores, aplicaciones, bases de datos, red) cuyo uso o explotación es compartido por un grupo de *personas usuarias*, por ello, estos recursos serán gestionados por el personal encargado de administrar la infraestructura.

4.8. Uso de los servicios de Impresión

Cada *persona* es responsable de recoger las copias impresas que en cada momento mande imprimir en las impresoras locales o departamentales.

Cualquier *persona* que encuentre documentos "sin propiedad" debe eliminarlos o destruirlos, siempre y cuando después de realizar una revisión de los mismos, no se encuentre reflejado en ellos referencia a la persona propietaria. Los equipos de reprografía no deben albergar más documentos que los impresos recientemente.

4.9. Intercambio de información y soportes de almacenamiento removible

Se considera soporte de almacenamiento removible a cualquier dispositivo con capacidad de almacenar información en formato electrónico y fácilmente transportable. (CD, DVD, Llaves USB, teléfonos móviles…)

CCASA autoriza el uso interno de estos soportes, siendo necesaria la autorización de las personas responsables de la información de las respectivas áreas para su envío al exterior.

Además, el intercambio de información con el exterior, y en especial aquella que contenga datos de carácter personal, requiere la autorización del Responsable de Seguridad de CCASA con objeto de aplicar los mecanismos de seguridad que correspondan en cada caso.

4.10. Telefonía y dispositivos móviles

Se considera "*personas usuarias de dispositivos móviles*" a quienes por las características de su puesto de trabajo utilizan habitualmente un portátil, smartphone, teléfono móvil, tableta, etc. dentro y fuera de la organización. Estas *personas usuarias de dispositivos móviles* y sus equipos tendrán consideraciones especiales en materia de seguridad, tal y como se especifican en la "Guía de seguridad de la información[1]" disponible en la Intranet.

Los teléfonos se deben utilizar exclusivamente para desempeñar funciones laborales. CCASA se reserva el derecho de revisar la utilización del dispositivo telefónico ante cualquier sospecha de un uso inapropiado del mismo.

4.11. Datos de Carácter Personal.

Se entiende por datos de carácter personal cualquier información concerniente a personas físicas identificadas o identificables. El CCASA, para el desempeño de sus funciones, requiere realizar un tratamiento de datos de carácter personal. El tratamiento de este tipo de datos está regulado legalmente tanto por legislación estatal como autonómica.

Por ello, el personal que para el desempeño de sus funciones maneje datos de carácter personal debe estar formado y conocer la normativa legal vigente en materia de protección de datos de carácter personal, de sus obligaciones y de las implicaciones del incumplimiento de la legalidad.

La legislación en materia de protección de datos de carácter personal supone para *estas personas*, entre otras, las siguientes obligaciones:

- Proteger los datos de carácter personal contra accesos no autorizados
- No crear nuevos ficheros con datos de carácter personal sin autorización de la persona Responsable de Seguridad
- Notificar a su Responsable de Seguridad cualquier incidencia que afecte a datos personales
- Crear ficheros temporales en recursos con control de acceso definido, y destruir los citados ficheros una vez han dejado de ser útiles para la finalidad para la que se crearon.
- No enviar datos al exterior sin la autorización de su Responsable de Seguridad.
- Destruir la información de los soportes que se desechen o reutilicen.
- Utilizar el "Procedimiento de obligaciones administrativas sobre datos de carácter personal[2]" ante solicitudes de acceso, rectificación, cancelación y oposición al tratamiento de datos personales.

[1] Disponible en la Intranet o a través de Responsable de Seguridad.
[2] Disponible en la Intranet o a través de Responsable de Seguridad

- Tratar los datos de carácter personal de acuerdo con las directrices de su Responsable de Fichero y Responsable de Seguridad correspondiente.

4.12. Incidencias

Ante cualquier sospecha o evidencia de defecto o anomalía que pudiera afectar a la seguridad de los recursos del CCASA o de sus clientes, las *personas usuarias* deberán informar al CAU, siendo el CAU quien se ocupe del registro y tratamiento de la misma.

Las incidencias producidas en sistemas de información relacionados con CCASA, aún no estando gestionados por CCASA, han de ser comunicadas al Responsable de Seguridad de CCASA.

Entre las posibles incidencias que se pueden dar se encuentran:

- Bloqueos de identificativos personales y contraseña.
- Funcionamiento anómalo de Hardware o Software.
- Violaciones de acceso a los Recursos de Información.
- …..

4.13. Copias de información

Las *personas usuarias* no deben realizar copias de la información clasificada como "confidencial" o "secreta", al margen de los procedimientos de backup definidos por CCASA, sin autorización de la persona propietaria de la misma. El almacenamiento de esta información sobre cualquier soporte físico (papel, cartuchos, CD, disquette, memoria USB, etc.), distinto de las aplicaciones de gestión de CCASA, está sujeto a la "Normativa de Inventario y Clasificación de Activos[3]".

Las empresas proveedoras que alberguen sistemas de información de CCASA en infraestructura no gestionada por CCASA, deberán realizar copias de seguridad de los datos de acuerdo a las directrices especificadas por la persona Responsable de Seguridad de CCASA.

Las copias temporales se deben destruir una vez finalizada la necesidad de su uso. Los métodos de destrucción de las copias se detallan en la "Normativa de Inventario y Clasificación de Activos". Las *personas usuarias* han de guardar especial cuidado en no dejar dentro de las "papeleras", carpetas temporales, etc. del ordenador ninguna copia de la información "confidencial" o "secreta" destruida.

4.14. Almacenamiento de Información en el puesto de trabajo

Las *personas usuarias*, con acceso a los servidores corporativos de CCASA, no deben almacenar información influyente para el negocio de CCASA o para sus clientes en sus equipos personales de trabajo. La información debe ser almacenada en los servidores de datos de CCASA. En el caso de personas usuarias sin acceso a los servidores corporativos de CCASA, deberán albergar la información en ubicaciones que cumplan con las condiciones de disponibilidad, integridad y confidencialidad acordadas con CCASA.

La información que no sea relevante para el negocio de CCASA, no deberá ser almacenada en servidores corporativos de CCASA, consiguiendo así un uso correcto de los recursos de red.

Toda *persona usuaria que* utilice dispositivos móviles debe, a la mayor brevedad posible, alojar la información de negocio en los servidores corporativos de CCASA.

[3] Disponible en la Intranet o a través de Responsable de Seguridad

4.15. Seguridad Física y Política de Mesas Limpias

Todo el personal debe de ser cauteloso de cuidar que la información presentada por las aplicaciones no sea visible por personas no autorizadas.

Además, antes de abandonar su puesto de trabajo, debe verificar que el material y la documentación utilizada en el desempeño de sus funciones se encuentran debidamente recogidos.

Al finalizar la jornada, los ordenadores deben quedar apagados. En el caso de que sea necesario que permanezcan encendidos, la pantalla debe estar bloqueada.

El acceso físico a las instalaciones donde se encuentren ubicados los sistemas de tratamiento de la información queda restringido, salvo al personal autorizado a ello, respetando en todo momento los controles de acceso de seguridad establecidos.

El personal externo que realice sus funciones en los edificios de DFA-CCASA deberá llevar visible la tarjeta identificativa personal o de VISITA.

Por otra parte, las *personas usuarias* que no se encuentren en instalaciones de DFA-CCASA o trabajen en sistemas de información no gestionados por CCASA, deberán aplicar medidas similares a los especificados en los párrafos previos, de manera que se aseguren los acuerdos de confidencialidad acordados con CCASA.

4.16. Otros documentos

CCASA informa a las *personas usuarias* que, además de la presente normativa, existen otros procedimientos, normativas, guías, política de seguridad, etc. publicados en el área de Seguridad de la Intranet, cuyo conocimiento y cumplimiento es obligado. Las *personas usuarias* que no dispongan de acceso a la Intranet, podrán contactar con el Responsable de Seguridad de CCASA para que facilite la citada información.

Los nuevos documentos relacionados con la seguridad de los sistemas de información y las revisiones de los ya existentes, se publicitarán por los medios habituales.

5. MONITORIZACIÓN

Las *personas usuarias* conectadas a la infraestructura tecnológica de CCASA son conscientes de que los sistemas de información usados para el acceso a/desde/dentro la red de CCASA son propiedad exclusiva de CCASA. Por ello, estas personas entienden que no tienen el derecho de propiedad y confidencialidad en su uso. Esto significa que CCASA puede en todo momento ejercer su derecho a procesar controles basados en la identidad de la *persona usuaria* y contenido de las comunicaciones/almacenamientos, respetando en todo momento la legalidad vigente, sin la necesidad de informar a la persona afectada.

Así pues, CCASA se guarda el derecho de monitorizar toda actividad relacionada con sus sistemas de información, para asegurar el correcto funcionamiento y uso, por parte de todas las *personas usuarias*, de los recursos informáticos respetando en todo momento la legalidad vigente.

En caso de que, en aplicaciones de CCASA, se detecte mal uso, por parte de alguna *persona usuaria*, se comunicará a ésta, formándole, en caso de que sea necesario, para el correcto uso de dichos recursos. Si se detectase un uso malintencionado, CCASA puede ejercer las acciones que estime oportunas.

Por último, CCASA podrá realizar controles para observar el correcto cumplimiento de las normas, procedimientos, políticas, etc. vigentes.

6. CONSECUENCIAS DEL MAL USO DE LOS RECURSOS

6.1. Colaboración del personal.

Las *personas usuarias*, cuando se les solicite, deben colaborar con las personas administradoras de sistemas y la persona Responsable de Seguridad, en la medida de sus posibilidades, en cualquier investigación que se haga sobre incidentes de seguridad o mal uso de los recursos, aportando la información que se les requiera.

6.2. Acciones correctivas.

En el caso de que la persona administradora de sistemas detectara la existencia de un mal uso de los recursos y éste proceda de las actividades o equipo de una *persona usuaria* determinada, pueden tomar cualquiera de las siguientes medidas para proteger a otras personas, redes o equipos:

- Notificar la incidencia a la *persona usuaria* o Responsable de Seguridad.
- Suspender o restringir el acceso o uso de los servicios mientras dure la investigación. Esta suspensión podrá ser recurrida por la *persona usuaria* ante la Gerencia de CCASA.
- Con el permiso de Responsable de Seguridad y la debida justificación (funcional y legal), inspeccionar ficheros o dispositivos de almacenamiento de la *persona* usuaria implicada.
- Informar a la Gerencia del CCASA de lo sucedido.

6.3. Medidas sancionadoras.

En caso que fuera necesario y una vez sea informado por su Responsable de Seguridad o por la persona administradora de sistemas, corresponderá a la Gerencia del CCASA la adopción de medidas contractuales que estime oportunas hacia las *personas usuarias* infractoras de esta norma, según lo establecido en la legalidad vigente.