

SEGURIDAD

NORMA DE USO DE LOS SISTEMAS DE INFORMACIÓN PARA PERSONAL EXTERNO

Clasificación del documento: Público



Mayo 2025



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

Este documento permanecerá vigente hasta su revisión o actualización formal. Se realizará una revisión para asegurar su adecuación a los cambios normativos, tecnológicos y organizativos. Además, cualquier modificación relevante en el contexto, legislación o en los procesos internos implicará una revisión inmediata.

Índice

Entorno	4
Objetivo de la norma	4
Alcance de la norma	4
Desarrollo de la norma	4
Monitorización	13
Consecuencias del mal uso de los recursos	13

Entorno

Las relaciones establecidas con terceras entidades por 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 acarrea unas responsabilidades al personal externo, que han de respetar:

- los derechos de otras personas usuarias (del CCASA y terceras entidades).
- 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).
- la legislación vigente.

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 proveedoras, personal en prácticas, servicios de vigilancia, etc. que prestan servicios al CCASA, con acceso a los sistemas de información habilitados por CCASA, independientemente de que los sistemas de información se encuentran en infraestructuras gestionadas por CCASA o no.

Objetivo de la norma

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

Alcance de la norma

Agentes

Esta norma es de aplicación para todo el personal externo 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 documento 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.

Desarrollo de la norma

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. Aquel personal externo 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 del personal usuario.

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 del personal externo. Además, CCASA prohíbe almacenar información personal en los puestos de trabajo (PCs, portátiles, etc.) al poder ser utilizados por otras personas; siendo el personal externo consciente 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.

El personal externo debe respetar la integridad de los recursos sobre los que se soportan, los derechos de otras personas usuarias, las leyes y regulaciones vigentes, así como todas las normativas, políticas, procedimientos, etc. vigentes en CCASA.

CCASA pone a disposición de todo el personal externo 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 las normas, políticas, 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.

Confidencialidad de la información

El contrato firmado entre CCASA y la empresa proveedora de servicios establece cláusulas relativas a la confidencialidad de la información. El personal externo ha de ser conocedor de las citadas cláusulas, siendo deber de la empresa proveedora informar de las mismas.

Además de las cláusulas específicas de cada contrato, todo personal externo 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. La información referida en el anterior apartado tiene, por defecto, carácter confidencial. Sólo podrá ser considerada información no confidencial aquella que CCASA haya comunicado a través de los medios de difusión pública.
- III. 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.
- IV. Estas obligaciones subsistirán aún después de finalizar su relación con CCASA.
- V. 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.”.

Este Compromiso de Confidencialidad supone, entre otras cosas, que el personal externo:

- Evitarán la revelación, modificación, destrucción o mal uso de la información independientemente de su soporte, manteniendo la integridad de la información en todo momento.

- Minimizarán los informes en formato papel con información confidencial, y cuando sean necesaria su obtención se mantendrán en lugar seguro.
- En caso de acceder a información a la cual no deba tener acceso, deberá informarlo en la mayor brevedad posible al Responsable de Seguridad de CCASA.

El personal externo tiene 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, el personal externo se compromete 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.

Política de claves y control de accesos

El personal externo que necesite acceder a los sistemas de información de CCASA, dispondrá de un identificativo asignado a su persona, manteniendo en secreto las pertinentes contraseñas, PINs, etc., y siendo responsables de las acciones que se ejecuten con su identificativo. Por ello, ninguna persona debe ocultar o manipular su identidad bajo ninguna circunstancia.

Para la habilitación de conexiones a red o a recursos corporativos, CCASA podrá requerir la siguiente información:

- Nombre y apellidos
- DNI
- E-mail externo
- Número de teléfono móvil
- Persona del CCASA responsable del proyecto/servicio relacionado con el identificativo solicitado
- Fecha de finalización del contrato/servicio para el que presta servicio
- Información vinculada a la VPN

Los sistemas de información propiedad de CCASA disponen 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.

Además, con relación a las contraseñas utilizadas, el personal externo ha de:

- Establecer contraseñas de calidad (longitud mínima de 8 y mayor de 10 cuando se pueda, caracteres numéricos/especiales/alfanuméricos).
- Cambiar la contraseña ante sospecha de conocimiento por otra persona.
- Evitar reutilizar antiguas contraseñas.
- Cambiar las contraseñas por defecto o las asignadas inicialmente.
- Evitar incluir contraseñas en procesos automatizados de inicio de sesión.
- Notificar cualquier incidencia relacionada con las contraseñas.

Así mismo, está prohibido intentar obtener, sin autorización explícita, otros derechos o accesos distintos a aquellos que CCASA haya definido. De igual manera, no está permitida la distorsión de los registros de trazas de actividad (logs), ni el descifrado no autorizado de cualquier información existente en la red y/o los sistemas de información.

Aquel personal que acceda a Sistemas de Información para su administración, mantenimiento o resolución de incidencias (técnicas o de seguridad) puede acceder, exclusivamente por motivos de mantenimiento y/o de seguridad, a aquellos ficheros con datos personales, de CCASA o de sus entidades cliente, que les permitan detectar, analizar y seguir las trazas de una determinada incidencia. En consecuencia, deberán mantener en todo momento el deber de secreto y requerirán autorización del Responsable de Seguridad para permitir el acceso de terceros a recursos del CCASA o de sus clientes.

En ningún caso se deben facilitar los datos identificativos y autenticación a terceras personas, ni siquiera a personal propio de CCASA.

Bloqueos de sesión y equipos desatendidos

El personal externo debe bloquear la sesión siempre que se ausenten del ordenador durante un periodo prolongado de tiempo o cuando el equipo no esté supervisado. 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.

Licencias y aplicaciones

El personal externo no debe utilizar programas (malware, virus, troyanos, etc.) que puedan dañar otras máquinas o sistemas de seguridad. Por este motivo, el personal externo deberá utilizar software que mantenga el ciclo de actualizaciones del mismo, especialmente de actualizaciones de seguridad.

El personal externo a los sistemas de información debe 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.

Asimismo, queda prohibido el uso, reproducción, cesión, transformación o comunicación pública de cualquier tipo de obra, documento o invención protegida por la propiedad intelectual sin la debida autorización. Además, está prohibida la obtención de cualquier contenido de origen fraudulento que constituya un delito contra la propiedad intelectual.

Herramientas de comunicación y colaborativas

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, el personal externo es responsable de todas las actividades realizadas con este tipo de herramientas de comunicación y colaborativas que pudiera facilitar CCASA. Este personal debe 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.

El correo electrónico corporativo es una herramienta que puede ser facilitada por CCASA al personal externo con fines exclusivamente profesionales, que puede ser controlada o monitorizada y que no debe utilizarse con fines personales. Una vez finalizada la relación profesional con CCASA, CCASA podrá acceder a las herramientas que facilitó al personal externo para recuperar información que fuera de interés.

El personal externo, con cuenta de correo electrónico facilitada por CCASA, aceptan que el correo catalogado por el CCASA como correo indiscriminado (SPAM), podrá ser marcado/borrado.

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.

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 realizado 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, el personal externo no debe 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.

Accesos a la red y servicios de internet

El personal externo debe 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 el personal externo necesite utilizar los recursos de la organización para emitir/recibir información, que sospechen pudiese generar la posibilidad de bloqueo al resto de personal usuario, se deben coordinar estos envíos/recepciones con el personal encargado de administrar la infraestructura.

Como se ha expuesto anteriormente, el personal externo 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.

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.

Intercambio de información

En todo intercambio de información y almacenamiento de la información se deberá garantizar la protección de la misma, previniendo riesgos de seguridad como accesos no autorizados, pérdidas de datos, entre otros. Es responsabilidad del personal externo la información que se comparte en las herramientas corporativas.

En el caso de compartir información en la nube, solo se debe usar plataformas de almacenamiento aprobadas por la organización, donde todo archivo que contenga información confidencial debe ser cifrado y/o protegido mediante contraseña. El acceso a los archivos compartidos estará limitado al personal externo autorizado y deberá establecerse un periodo de validez para dicho acceso, asegurándose de revocar permisos una vez finalizado el tiempo permitido.

CCASA recomienda priorizar herramientas corporativas para el intercambio de información, desaconsejando el uso de almacenamiento removible¹. En casos excepcionales, donde no exista otra alternativa viable, se autorizaría el uso de estos soportes siendo necesaria la autorización de las personas responsables de la información que contenga.

En el caso de disponer de autorización para el uso de almacenamiento removible, la información deberá ir cifrada y/o protegida mediante contraseña. Del mismo modo, en caso de extravío o robo del dispositivo, el personal externo deberá informar de inmediato al equipo de seguridad de la información para mitigar posibles riesgos.

El acceso a información confidencial se otorgará mediante autorización, exclusivamente al personal externo que lo requieran para el desempeño de sus funciones siendo personal e intransferible. Además, el envío de información con datos de carácter personal al exterior requiere la autorización del Responsable del tratamiento, y en ausencia de esta persona, del Responsable de Seguridad de CCASA.

Los accesos concedidos tendrán un límite de tiempo previamente definido y se revocarán automáticamente al término del plazo. En casos excepcionales, las extensiones de tiempo deberán ser justificadas y aprobadas por el responsable correspondiente, dejando registro del motivo.

En caso de detectarse cualquier incumplimiento sobre las directrices establecidas en el intercambio de información, será reportado y gestionado como un incidente (véase apartado [Incidentes](#)).

¹ Cualquier dispositivo con capacidad de almacenar información en formato electrónico y fácilmente transportable. (CD, DVD, Llaves USB, teléfonos móviles...).

Equipamiento informático

Se considera equipamiento informático todo aquel dispositivo electrónico (ordenador portátil, sobremesa, teléfonos, dispositivos móviles, *tablets*, monitores, teclados, etc.), componentes y herramientas que sean suministradas para desempeñar funciones laborales, no estando permitido su uso a nivel personal. Es responsabilidad del personal externo, cuidar y mantener en buen estado el equipo asignado durante el periodo en que lo utilice.

CCASA se reserva el derecho de revisar la utilización del equipamiento informático ante cualquier sospecha de un uso inapropiado del mismo.

Se considera “personas usuarias de dispositivos móviles” a quienes por las características de su puesto de trabajo, utilizan habitualmente un portátil, smartphone, teléfono móvil, *tablet*, etc. dentro y fuera de la organización.

Además de cumplir con los demás apartados de la presente Norma, el personal externo deberá tener precauciones añadidas al ser dispositivos que pueden llegar a salir de las instalaciones:

- Mantener el dispositivo siempre bajo su control, especialmente en lugares públicos.
- No almacenar información confidencial de forma local en el equipo.
- Conectarse únicamente a redes Wi-Fi seguras y aprobadas.
- Usar una VPN corporativa para acceder a información o sistemas laborales fuera de la oficina.
- Se recomienda, desactivar funciones como Bluetooth, Wi-Fi y NFC cuando no las esté utilizando.
- En caso de extravío o robo, informar de inmediato al CAU para bloquear el dispositivo y proteger la información almacenada.
- Está prohibido realizar “*jailbreak*”² o “*rooting*”³ en dispositivos corporativos, ya que esto elimina las medidas de seguridad integradas.
- Cualquier modificación no autorizada será considerada una violación de las políticas de la organización.
- El personal externo es responsable de proteger su dispositivo y la información que maneja.

Si se detecta que el equipamiento presenta daños significativos que excedan del desgaste normal deberá informar al CAU e indicar las circunstancias del daño. Así mismo, CCASA evaluará si los daños fueron causados por negligencia, mal uso o factores externos.

Una vez finalizada la relación con CCASA, se debe de restituir a CCASA todo aquel material que haya sido entregado para la realización de las tareas encomendadas.

Cumplimiento normativo relacionado con la seguridad de la información

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.

² Proceso con el cual se eliminan las limitaciones impuestas por Apple en un dispositivo con iOS.

³ Proceso con el cual se consiguen permisos de ‘*superusuario*’ o administrador para acceder al sistema sin ningún tipo de restricción.

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 incidente 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 (Disponible en la Intranet o a través de Responsable de Seguridad.)” ante solicitudes de acceso, rectificación, cancelación y oposición al tratamiento de datos personales.
- Tratar los datos de carácter personal de acuerdo con las directrices de su Responsable de Fichero y Responsable de Seguridad correspondiente.
- El personal externo debe cumplir con las condiciones de tratamiento de datos carácter personal recogido en el contrato establecido.

Incidentes

Ante cualquier sospecha o evidencia de defecto o anomalía que pudiera afectar a la seguridad de los recursos del CCASA o de sus clientes, el personal externo deberá informar, tal y como se especifica en el “Procedimiento de resolución de incidentes de seguridad” al CAU (945 181818 - EXT: 54600 o cau@araba.eus), siendo el CAU quien se ocupe del registro y tratamiento de la misma.

Los incidentes de seguridad producidos en sistemas de información relacionados con CCASA, aun no estando gestionados por CCASA, han de ser comunicados al Responsable de Seguridad de CCASA con la mayor brevedad posible en un plazo máximo de 24 horas.

Entre los posibles incidentes que se pueden dar se encuentran:

- Bloqueos reiterados (y de origen desconocido) de identificativos personales y contraseña.
- Funcionamiento anómalo de Hardware o Software (asociados a Malware).
- Violaciones de acceso a los Recursos de Información.
- SPAM/Phishing (dirigidos): Correos electrónicos sospechoso o no solicitados.
- Suplantación de entidades.
- Detección de ataques dirigidos a la organización.
- Compromiso de identificativos personales y contraseñas.
- Acceso no autorizado a información o recursos.
- Pérdida de datos o información de CCASA y entes afines.
- Modificación no autorizada de información.
- Detección de vulnerabilidades en los sistemas.

Es de obligado cumplimiento informar de **Incidentes de seguridad graves con posible impacto en los sistemas de información de CCASA al Responsable de Seguridad de CCASA.**

Cualquier persona podrá trasladar al Responsable de Seguridad de CCASA sugerencias, debilidades, vulnerabilidades y/o situaciones de riesgo que pueda tener relación con la seguridad de la información y las directrices contempladas en las presentes políticas de las que tenga conocimiento.

Copia de información

El personal externo no debe realizar copias paralelas de la información del CCASA o de las entidades a las que presta servicio al margen de la ubicación de donde se encuentre operativa en la organización. Por consiguiente, no está permitido copiar información en cualquier dispositivo de almacenamiento (físico o en la nube), sin autorización expresa de la persona propietaria de la misma o del Responsable de Seguridad de CCASA.

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. El personal externo ha de guardar especial cuidado en no dejar dentro de las “papeleras”, carpetas temporales, etc. del ordenador ninguna copia de información que no sea pública.

Almacenamiento de información en el puesto de trabajo

El personal externo, con acceso a los servidores corporativos de CCASA, no deben almacenar información relevante 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 personal externo 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 y/o de las entidades a las que se presta servicio, no deberá ser almacenada en servidores corporativos de CCASA, consiguiendo así un uso correcto de los recursos de red.

Todo personal externo que utilice dispositivos móviles debe, a la mayor brevedad posible, alojar la información de negocio en los servidores corporativos de CCASA.

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, el personal externo que no se encuentre 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.

Otros documentos

CCASA informa al personal externo de los sistemas de información 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. El personal externo que no dispongan de acceso a la Intranet podrá 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 publicarán por los medios habituales.

Monitorización

El personal externo conectado 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, este personal entiende 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 del personal externo 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 todo el personal externo, 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 del personal externo, se comunicará a éste, 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.

Consecuencias del mal uso de los recursos

Colaboración del personal

El personal externo de los recursos informáticos y de la infraestructura de red de CCASA, 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.

Acciones correctivas y preventivas

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 del personal externo, pueden tomar cualquiera de las siguientes medidas para proteger a otras personas, redes o equipos:

- Notificar el incidente al personal externo, a su responsable dentro de la organización y/o al Responsable de Seguridad.

- Suspender o restringir el acceso o uso de los servicios mientras dure la investigación. Esta suspensión podrá ser recurrida por el personal externo 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 del personal externo implicado.
- Informar a la Gerencia del CCASA de lo sucedido.

Medidas contractuales

En caso de 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 hacia las empresas con personal externo infractor de esta norma, según lo establecido en la legalidad vigente.