SCOUTS Construir un Mundo Mejor
ASDE Exploradores de Murcia
Alba 601
Alcalde de Zalamea, 4
30366 El Algar
Tel: (+34) 686 14 53 44

CIRCULAR DE MEDIDAS DE SEGURIDAD CIRCULAR INFORMATIVA SOBRE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

Mediante este documento se describen las principales medidas de seguridad a adoptar las personas con acceso a datos para el cumplimiento de la política de protección de datos personales implantada en GRUPO SCOUT ALBA 601.

Estas normas obligan a cualquier persona que maneje datos personales en las instalaciones de esta entidad o que se encuentren bajo la responsabilidad de ésta.

Confidencialidad

- Toda la información custodiada en GRUPO SCOUT ALBA 601 ., ya estén contenidos en el Sistema de Información o custodiados en sus archivos, son responsabilidad de la organización y todas las tareas derivadas de su tratamiento resultan confidenciales.
- El personal sólo puede acceder a los datos necesarios para el desempeño de su función y respetarán la confidencialidad de esos datos.
- El personal está obligados legalmente a guardar secreto profesional respecto a los datos tratados, y al deber de guardarlos, es decir, evitar el acceso a dichos datos por personal no autorizado.
- La obligación de mantener la confidencialidad subsistirá aún en el caso de finalizar la relación con la organización.
- Se prohíbe expresamente copiar información con datos de carácter personal al ordenador personal o portátil y en cualquier tipo de soporte informático sin autorización expresa del Responsable del Tratamiento.
- Se prohíbe, así mismo la copia o reproducción de documentos escritos.

Correo electrónico (incluir solo si se dispone de correo del grupo)

- El correo electrónico se considera herramienta de trabajo, y como tal podrá ser revisado, y desviado en caso de ausencia o baja del trabajador:
    - Los controles por incidencias técnicas podrán realizarse sin preaviso.
    - Los controles preventivos se realizarán con presencia del trabajador o trabajadora, si fuera posible. Si se realizan sin presencia del mismo se realizará un preaviso del alcance de dicho control.
    - Cuando sea desviado se hará al jefe del departamento o a la persona designado por aquel, con la finalidad de no dejar desatendida ninguna tarea.
- No debe abrir ni ejecutar ficheros que se reciban por correo electrónico, especialmente si es de un remitente desconocido, salvo que se tenga la total certeza de su inocuidad, y siempre después de revisarlo con el programa antivirus.
- El correo electrónico no puede ser empleado para la transmisión de datos protegidos ni para fines diferentes a los establecidos para el correcto desarrollo de sus funciones laborales, sin la autorización del Responsable del Tratamiento.
- El envío de e-mail a varios destinatarios desde las cuentas de correo electrónicos asignadas por GRUPO SCOUT ALBA 601.se realizarán siempre introduciendo los destinatarios en el campo CCO
- **Únicamente se podrán remitir correos electrónicos a aquellas personas o empresas con las que exista una relación o que hayan pres**tado su consentimiento para la recepción de información de GRUPO SCOUT ALBA 601
- Se prohíbe la utilización del correo electrónico corporativo para usos personales o particulares. No se reenviarán mensajes ni documentos corporativos a cuentas privadas del trabajador o de sus familiares o amigos, ya que éstas no gozan del mismo nivel de seguridad. Tampoco se puede configurar la cuenta de correo corporativo para reenviar los mensajes recibidos a una cuenta de correo electrónico privado.
- Cuando se vaya a enviar información sensible por correo electrónico se deberá hacer cifrando los datos.

Alcalde de Zalamea, 4
30366 El Algar
Tel: (+34) 686 14 53 44

Uso de aplicaciones de mensajería (whatsapp, skype, telegram, etc.)

- En ningún caso, las aplicaciones de mensajería se utilizarán para el intercambio de información que pueda contener datos de carácter personal o cualquier otra información que puedan considerarse de carácter confidencial.
- Queda prohibido crear grupos en aplicaciones de mensajería sin el consentimiento expreso de todas las personas que vayan a formar parte del éste.

Uso de aplicaciones en la nube (dropbox, onedrive, wetransfer, google drive, etc.)

- Sólo se podrán utilizar aplicaciones en la nube previa autorización expresa de la dirección de GRUPO SCOUT ALBA 601
- Si se utilizan estas herramientas se tendrán que tener en cuenta los siguientes criterios:
  - Si se almacenan datos sensibles tendrá que hacerse cifrando previamente la información.
  - La aplicación en la nube estará vinculado al correo corporativo y no a cuentas personales.
  - Eliminar la información una vez expirada la finalidad para la que se ha creado.

Internet (solo si se dispone del mismo)

- GRUPO SCOUT ALBA 601se reserva el derecho a controlar o limitar el conjunto de servicios de Internet accesibles para los usuarios, por motivos de seguridad o rendimiento de la red, así como a establecer sistemas de control del uso de Internet por los usuarios para garantizar que este se realiza conforme a las presentes normas.
- Todo el material descargado desde Internet debe ser escaneado por el antivirus corporativo de GRUPO SCOUT ALBA 601 que etá instalado en su equipo, antes de ser alojados en el sistema informático de GRUPO SCOUT ALBA 601 o ser ejecutado en cualquier equipo.
- Queda terminantemente prohibido:
  - Descargar programas informáticos de tipo destructivo (por ejemplo, que contengan virus o código auto-replicante).
  - Descargar, recibir, imprimir o instalar material protegido por derechos de autor (software, imágenes, literatura, música, cine o cualquier información bajo copyright), en contravención de las leyes de protección intelectual.
  - Enviar, recibir, imprimir o distribuir información propietaria, secretos de negocio o cualquier otra información confidencial de GRUPO SCOUT ALBA 601 en contravención de las políticas de la empresa o derivados de contratos o acuerdos suscritos por la misma.

Imágenes

- La toma de imágenes (fotografías o grabación de video) en las instalaciones de GRUPO SCOUT ALBA 601 se realizará siempre por personal autorizado por el grupo, y dentro del ámbito de dicha autorización.
- No se pueden realizar fotografías, videos, ni cualquier tipo de toma de imágenes o grabaciones sonoras en las instalaciones de GRUPO SCOUT ALBA 601 o en el ámbito de las actividades organizadas por GRUPO SCOUT ALBA 601

Redes sociales o publicación de datos en internet (solo para los responsables de las publicaciones)

- No poner etiquetas con nombres de personas físicas en las fotos o videos.
- Avisar en los actos en que se vayan a realizar grabaciones o fotografías que vayan posteriormente a ser divulgadas por internet. Hacer uso del cartel de toma de imágenes
- No compartir fotos de personas con acceso a datos o familiares que no hayan dado su consentimiento previamente, salvo que dichas fotografías/videos hayan sido tomados en actos en los que se haya advertido previamente de tal circunstancia.
- No compartir las fotografías, y no difundirlas fuera del ámbito de la organización, salvo que se disponga de la autorización de las personas que aparecen en la misma.
- Si se van a tomar datos a través de cualquier vía, hay que poner una cláusula que informe a las personas con acceso a datos de sus derechos.
- Es conveniente que aparezca claramente la posibilidad de solicitar la cancelación de los datos personales, y que dirección dirigirse. Para ello se puede ubicar, por ejemplo, en la pestaña de información en facebook.

- No se deben publicar en redes sociales, internet o aplicaciones de mensajería instantánea imágenes de actividades realizadas en GRUPO SCOUT ALBA 601 ni insertar comentarios que afecten a la privacidad de las personas, sin la autorización previa del interesado. La publicación de contenidos privados en internet, redes sociales o aplicaciones de mensajería instantánea se considera una vulneración del deber de secreto.

Puestos de trabajo (en el caso de disponer de equipos personales o compartidos)

- En los medios y equipos de trabajo que están bajo tu responsabilidad deberás asegurarte que la información que muestran no pueda ser visible por personas no autorizadas
- Esto implica que tanto las pantallas como las impresoras u otro tipo de dispositivos conectados al puesto de trabajo deben estar físicamente ubicados en lugares que garanticen esa confidencialidad.
- Cuanto el responsable de un puesto de trabajo lo deje sin atención, debe dejarlo en un estado que impida la visualización de los datos protegidos. Esto se puede realizar a través de un protector de pantalla que impida la visualización de los datos. La reanudación del trabajo tiene que implicar la desactivación de la pantalla protectora con la autenticación del usuario. En lo que respecta a la documentación, esta no deberá dejarse expuesta.
- En el caso de las impresoras debe asegurarse de que no queden documentos impresos en la bandeja de salida que contengan datos protegidos.
- Se prohíbe la realización de nuevos tratamientos de datos personales sin previa autorización del Responsable del tratamiento.
- Se prohíbe ceder datos personales sin autorización.
- Los puestos asignados a cada persona se consideran herramientas de trabajo, y pueden ser revisados y accedidos desde dirección en el caso de ser necesario. El acceso al puesto no requerirá preaviso previo.

CONTRASEÑAS (EN EL CASO DE DISPONER DE EQUIPOS PERSONALES O COMPARTIDOS)

- Los usuarios son responsables de la confidencialidad de sus contraseñas. En el caso de que una contraseña sea conocida por una persona no autorizada, se hace constar como incidencia en Registro habilitado para tal fin.
- La contraseña de acceso caducará, debiendo ser modificada en el momento de realizar el primer acceso al sistema.
- No se accederá al sistema utilizando el identificador y la contraseña de otro usuario. Las responsabilidades de cualquier acceso realizado utilizando un identificador determinado, recaerán sobre el usuario al que hubiera sido asignado.
- En cuando a la configuración de la contraseña, se estará a lo dispuesto en el Manual de Seguridad.

Gestión de incidencias

- Incidencia es cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos, ya estén almacenados de manera automatizada o no (incluye también los datos almacenados en “formato papel”).
- Cualquier trabajador o trabajadora, si tiene conocimiento de una incidencia, es responsable de la comunicación de la misma al administrador del sistema, o en su caso del registro de la misma en el sistema de registro de incidencias.
- El conocimiento y la no-notificación de una incidencia por parte de un usuario del sistema es considerado como una falta contra la seguridad.
- Para la notificación de incidencias deberá ponerse en contacto con el administrador de sistemas o con la persona designada al efecto.

Gestión de soportes (pendrive, discos duros, cds, etc.) Utilizados para el tratamiento de carácter personal

- Si salen soportes u ordenadores portátiles que puedan contener datos sensibles deberán cifrarse los datos contenidos en ellos.
- La entidad debe garantizar el control de los datos personales de los que es responsable, con esta finalidad se realizará un control de los soportes o equipos portátiles utilizados que contengan datos de carácter personal responsabilidad del grupo, así como la persona responsable del mismo.
- No se deben utilizar soportes o equipos portátiles sin inventariar.

Alcalde de Zalamea, 4
30366 El Algar
Tel: (+34) 686 14 53 44

- Queda terminantemente prohibido facilitar, a persona alguna ajena a la entidad, ningún soporte conteniendo datos a los que haya tenido acceso en el desempeño de sus funciones, sin la debida autorización.

Gestión de documentación

- Los documentos deben almacenarse en áreas donde el acceso esté restringido, protegido con puertas de acceso y llave.
- Se adoptarán las medidas necesarias para evitar la sustracción, pérdida o acceso indebido durante su transporte (si la documentación es confidencial: traslado en sobres opacos y cerrados).
- La documentación en proceso de revisión, o tramitación, ya sea previo o posterior al archivo, debe ser custodiada por la persona que se encuentra al cargo de la misma, quien tendrá la responsabilidad de la confidencialidad de la misma, impidiendo el acceso de personas no autorizadas. Cuando se produce una salida de documentación de las instalaciones, el responsable de la misma es el encargado de velar para que no se produzcan accesos por terceros.
- La salida de documentos deberá estar previamente autorizada.
- Las copias y reproducciones de documentación, así como cualquier papel que contenga datos personales, deberá ser desechado de forma que se evite el acceso a la información y su recuperación posterior.
- En el caso de pérdida de documentación debe ser comunicada a la dirección con carácter inmediato, ya que constituye una incidencia.

Responsabilidades:

El usuario será responsable frente a GRUPO SCOUT y frente a terceros de cualquier daño que pudiera derivarse para unos u otros del incumplimiento de los compromisos anteriores y resarcirá a la entidad las indemnizaciones, sanciones o reclamaciones que ésta se vea obligada a satisfacer como consecuencia de dicho incumplimiento.

Ejercicio de derechos:

Cualquier usuario de datos personales de GRUPO SCOUT ALBA 601 debe conocer cuáles son los derechos que tienen los usuarios, que son los siguientes:

- Derecho de acceso: el interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales.
- Derecho de rectificación: el interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan.
- Derecho de supresión: el interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan.
- Derecho a la limitación de los datos: el interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos.
- Derecho a la portabilidad de los datos: el interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado.
- Derecho a oposición: el interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento basado en el interés legítimo, incluida la elaboración de perfiles sobre la base de dichas disposiciones.

Si cualquiera solicita ante el personal de GRUPO SCOUT ALBA 601 el ejercicio de estos derechos, aunque no sea con estas palabras, e incluso aunque sepamos que la empresa no tiene registrados ni trata datos suyos, se le darán las indicaciones de cómo ejercitar el derecho.

La persona autorizada para gestionar los ejercicios de derechos es el responsable de protección de datos, por lo que se le deberán comunicar todas las solicitudes de ejercicios de derecho, independientemente del canal de comunicación a través del que se reciban (en mano, por carta, e-mail, fax, etc.).

SCOUTS
Construir un Mundo Mejor
ASDE
Exploradores de Murcia
Alba 601

Alcalde de Zalamea, 4
30366 El Algar

Tel: (+34) 686 14 53 44