Medidas de seguridad técnicas y organizativas de Ferrero

1. CONTROLES GENERALES

1.1 Ferrero ha implementado políticas de protección de datos personales debidamente documentadas que son periódicamente actualizadas.

1.2 Los procedimientos de protección de datos personales de Ferrero están formalmente documentados, son objeto, en su caso, de actualizaciones periódicas y se sustentan en documentos objetivos (tales como actas de reuniones, listados, registros de IT), lo que demuestra una supervisión y una diligencia constantes en relación con la protección de datos personales en la gestión de las actividades que se llevan a cabo.

2. DERECHOS DE LOS TITULARES DE LOS DATOS (ART. 15 y siguientes del RGPD).

2.1 Los empleados de Ferrero conocen los procedimientos a los que pueden recurrir los titulares de los datos para ejercer sus derechos de acceso así como para comunicar las solicitudes de ejercicio de tales derechos al responsable del tratamiento.

2.2 Ferrero lleva un registro general en que aparecen registradas estas solicitudes, tales como el ejercicio del derecho de acceso.

2.3 Ferrero ha establecido un plazo para la comunicación de solicitudes al responsable del tratamiento.

2.4 Ferrero cuenta con un procedimiento para documentar, por escrito, cualquier negativa dada a cualquier titular de datos para ejercer su derecho de supresión, limitación de procesamiento o portabilidad de datos, así como para compartir esta documentación con el responsable del tratamiento.

3. POLÍTICA DE PRIVACIDAD (ART. 13 del RGPD) (en su caso)

3.1 Todos los empleados y otro personal de Ferrero responsable de gestionar la política de privacidad o de tramitar notificaciones sobre protección de datos personales con los titulares de los datos y/o para obtener el consentimiento de estos respecto a la recogida de dichos datos, incluso en nombre del responsable del tratamiento, han sido específicamente formados en cuanto a la normativa de protección de datos.

3.2 Ferrero realiza comprobaciones periódicas respecto a la forma de proceder de dicho personal en su gestión con los titulares de los datos.

3.3 En la tramitación de las políticas de privacidad/notificaciones sobre protección de datos personales con los titulares de los datos, los empleados u otro personal de Ferrero responsable de dicha tramitación deberán informar claramente a dichos titulares de sus derechos, ya sea oralmente como por escrito.

3.4 Ferrero lleva un registro de todas las fuentes de las que obtiene datos personales.

4. PERSONAL AUTORIZADO (ART. 29 DEL RGPD)

4.1 Ferrero ha procedido a nombramientos formales de todo el personal autorizado, tanto de forma individual o como parte de categorías homogéneas.

4.2 Todas las personas autorizadas designadas han recibido instrucciones escritas precisas sobre cómo procesar y proteger los datos personales.

4.3 Ferrero cuenta con una lista actualizada del personal autorizado, debidamente formado, que recibe instrucciones adecuadas sobre protección de datos personales. Dicha formación se documenta adecuadamente.

4.4 Los derechos de acceso facilitados al personal autorizado son adecuados y están actualizados. Las instrucciones facilitadas al personal autorizado están actualizadas. Esta actualización es objeto de confirmaciones periódicas.

5. FORMACIÓN

5.1 Todo el personal de nueva contratación es debidamente formado antes de empezar a procesar datos personales.

5.2 La fiabilidad e integridad de los empleados es objeto de examen previamente a confiarles actividades que impliquen el acceso a datos personales.

5.3 Todo el personal autorizado recibe habitualmente actualizaciones operativas sobre seguridad.

5.4 Ferrero facilita pautas de seguridad a todo el personal autorizado.

5.5 Ferrero mantiene documentación para apoyar y justificar las actividades de formación realizadas.

6. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

6.1 Ferrero ha definido un grupo de criterios y políticas para dejar clara su posición y respaldar la seguridad de la información así como los controles de seguridad en relación con los dispositivos móviles y el teletrabajo (teleconmutación, acceso remoto o puestos de trabajo virtuales).

6.2 Ferrero ha definido roles y responsabilidades individuales a efectos de seguridad de la información y los ha asignado a las personas adecuadas con el fin de evitar conflictos de interés y de impedir cualquier forma de proceder no adecuada.

6.3 Ferrero ha suscrito acuerdos con subprocesadores, a los que ha trasladado la necesidad de implementar las medidas de seguridad técnicas y organizativas necesarias en relación con la protección de datos personales.

7. SEGURIDAD DE RECURSOS HUMANOS

7.1 Previamente a cualquier contratación o selección de personal, de contratistas o de personal temporal, se considerarán las responsabilidades de seguridad de la información (mediante una correcta descripción de los puestos vacantes o de una selección previa) las cuales se incluirán asimismo en los contratos de trabajo o de servicios aplicables (dentro de los términos y condiciones del puesto de trabajo, así como en otros acuerdos firmados que definan los roles y responsabilidades relacionados con la seguridad, mediante obligaciones de cumplimiento, etc.).

7.2 Los directivos de Ferrero deberán asegurarse, durante el transcurso de la relación laboral, de que sus empleados, contratistas y personal temporal conocen y han recibido las instrucciones adecuadas para cumplir con sus obligaciones en cuanto a seguridad de la información, y que han sido informados de la posibilidad de verse expuestos a medidas disciplinarias en caso de provocar incidentes de seguridad de la información.

7.3 Ferrero cuenta con procedimientos disciplinarios que podrán activarse en caso de que sus empleados, contratistas o personal temporal provoque incidentes de seguridad de la información.

7.4 Siempre que una persona abandone Ferrero, o siempre que se produzcan cambios importantes en sus roles y responsabilidades, deberán gestionarse todos los aspectos relacionados con la seguridad, garantizando así la devolución de toda la información y equipos corporativos, la actualización de las autorizaciones/derechos de acceso, así como el recordatorio a todas las personas implicadas de sus obligaciones vigentes en cuanto a privacidad, propiedad intelectual, vigencia de cláusulas contractuales u otras, incluyendo las expectativas éticas.

7.5 Las personas autorizadas recibirán instrucciones específicas sobre cómo eliminar o destruir información contenida en soportes de almacenamiento previamente a su reutilización.

8. GESTIÓN DE ACTIVOS

8.1 Ferrero cuenta con un inventario completo de todos sus activos de información. Asimismo, con el fin de garantizar la responsabilidad de la seguridad de dichos activos, las personas responsables de dichos activos están claramente identificadas. Ferrero ha definido políticas de «uso aceptable» para dichos activos.

8.2 Los soportes de almacenamiento de la información son gestionados, controlados, transportados y eliminados de forma a no comprometer el contenido de la información almacenada.

8.3 Ferrero cuenta con un número adecuado de contenedores seguros, debidamente distribuidos y a disposición de las personas responsables de la custodia (incluso de forma temporal) de datos personales en cualquier formato (formato papel, electrónico u otros).

8.4 Ferrero ha implementado controles para evitar que aquellos documentos que contienen categorías especiales de datos personales queden desatendidos al ser encomendados a personal autorizado y retirados de archivos protegidos.

8.5 El personal autorizado puede acceder fácilmente al uso de destructoras de documentos en papel.

8.6 Ferrero ha implementado una política adecuada sobre el uso, el almacenamiento y la destrucción de documentos en formato papel.

8.7 Previamente a su reutilización, aquellos documentos que contengan categorías especiales de datos personales deberán ser borrados o, preferentemente, destruidos.

9. CONTROL DE ACCESO

9.1 Los requisitos organizativos de Ferrero para el control de acceso a activos de información están claramente documentados en un procedimiento/política de control de acceso, y el acceso a la red y conexiones de Ferrero está limitado.

9.2 Los usuarios tienen conocimiento de sus responsabilidades en relación con el mantenimiento de un control de acceso efectivo, tales como optar por contraseñas seguras y mantenerlas confidenciales.

9.3 El acceso a la información se restringirá de conformidad con el procedimiento/política de control de acceso, mediante, por ejemplo, sistemas de login seguros, una correcta gestión de las contraseñas, controles de acceso especiales y la limitación de acceso a códigos fuentes.

9.4 Ferrero controla los accesos a zonas vulnerables. Todas aquellas personas que deseen acceder a zonas vulnerables deberán obtener una autorización previa.

9.5 Las zonas vulnerables están dotadas con herramientas de control de acceso electrónico o sujetas de cualquier otra forma a una supervisión adecuada.

9.6 Ferrero revisa regularmente los logs de acceso a las zonas vulnerables, tales como salas de servidores, a efectos de detectar accesos no justificados.

10. SEGURIDAD FÍSICA Y MEDIOAMBIENTAL

10.1 Ferrero ha definido claramente barreras y perímetros físicos, con controles físicos de acceso y procedimientos internos para proteger sus instalaciones, oficinas, salas, zonas de carga/descarga, etc. contra cualquier acceso no autorizado (protección contra incendios, inundaciones, terremotos, bombas, etc.).

10.2 Ferrero confirma que no podrá retirarse ni equipos ni información de sus instalaciones sin autorización previa, y que dichos equipos y/o información continuará estando adecuadamente protegida ya esté dentro como fuera de sus instalaciones.

10.3 La información contenida en soportes de almacenamiento de información será destruida antes de eliminar o reutilizar de nuevo dichos soportes de almacenamiento.

10.4 Deberá protegerse cualquier equipo sin vigilancia, y existe un espacio específico y una política de control clara para dicho equipo.

11. SEGURIDAD OPERATIVA

11.1 Se han implementado y se mantienen controles de software malicioso.

11.2 De conformidad con la política de copias de seguridad de Ferrero se llevan a cabo y se mantienen las copias de seguridad necesarias.

11.3 Se procede a la comprobación de dichas copias de seguridad. Los resultados se documentan y registran.

12. AUTENTICACIÓN Y SUPERVISIÓN

12.1 Los sistemas de cronometraje están sincronizados a efectos de garantizar la coherencia temporal del registro de datos.

12.2 Ferrero sigue el principio de privilegios mínimos, permitiendo el acceso autorizado de los usuarios sobre la base de las responsabilidades de su cargo.

13. GESTIÓN DE VULNERABILIDADES TÉCNICAS

13.1 Ferrero puede confirmar el desarrollo de un proceso de gestión de vulnerabilidades a efectos de identificar puntos débiles de seguridad recurriendo a fuentes fiables externas para información sobre vulnerabilidades, y asignando una clasificación de riesgo a las vulnerabilidades de seguridad.

13.2 Las actualizaciones de software y de los componentes del sistema relacionados con la corrección de vulnerabilidades conocidas son evaluadas a efectos de determinar su aplicabilidad. En su caso, serán sometidas a las pruebas necesarias antes de su instalación y se implementarán de la manera oportuna.

13.3 A efectos de impedir nuevas vulnerabilidades, se han implementado normas sobre la instalación de software por parte de los usuarios.

13.4 Ferrero ha definido e implementado un proceso de prueba de penetración tanto a nivel de aplicación como de infraestructura.

14. SEGURIDAD EN LAS COMUNICACIONES

14.1 La seguridad de la red de Ferrero y sus servicios en red están protegidos mediante la segregación de la red.

14.2 Ferrero ha implementado medidas de protección para controlar las comunicaciones tanto en la frontera interna como externa de la infraestructura.

14.3 Ferrero ha implementado políticas, procedimientos y acuerdos (tales como de confidencialidad, de procesamiento de datos personales, etc.) en relación con el traspaso de información a/desde terceros, incluyendo a través de mensajería electrónica.

14.4 Ferrero ha implementado canales seguros (protocolos encriptados en caso de conexión con la red corporativa, y/o accesos VPN en caso de conexiones remotas) para las comunicaciones entre los sistemas de información y la red corporativa.

15. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DEL SISTEMA

15.1 Ferrero analiza y especifica sus requisitos de control de seguridad, incluyendo aquellos referidos a las operaciones y aplicaciones web.

15.2 La normativa que rige el desarrollo de los sistemas de seguridad se ha definido de conformidad con la política interna de Ferrero.

15.3 Previamente a su migración a producción, todos los cambios son gestionados, tramitados, revisados y aprobados (idealmente mediante una herramienta) en un entorno específico.

15.4 Los cambios en la configuración de los parámetros de aplicación deberán autorizarse antes de su implementación y validarse tras haberse implementado.

15.5 Los paquetes de programas no podrán modificarse y deberán respetarse los principios técnicos sobre seguridad de los sistemas.

15.6 Los entornos de desarrollo, prueba y producción deberán segregarse con el fin de evitar accesos no autorizados o cambios en los sistemas de producción y repositorios de códigos.

15.7 Todos los datos para las pruebas son cuidadosamente seleccionados, generados y controlados.

16. RELACIONES CON PROVEEDORES

16.1 Ferrero ha implementado políticas, procedimientos y actividades de concienciación para proteger aquella información organizativa que sea accesible a subcontratistas u otros proveedores externos (sean o no subprocesadores) en toda la cadena de suministro. Dichas acciones se recogen en los acuerdos escritos firmados con estos.

17. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

17.1 Ferrero ha implementado procedimientos y responsabilidades para gestionar (informar, evaluar, responder y aprender de) temas de seguridad de la información, incidentes y vulnerabilidades, incluyendo fallos de datos personales, de forma coherente y efectiva para permitir su debida comunicación al responsable del tratamiento, así como la recogida de las pruebas periciales necesarias, en su caso.

18. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN RELACIÓN CON LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

18.1 Ferrero considera la planificación de la continuidad, implementación, pruebas y revisión de la seguridad de la información como parte fundamental de los sistemas de gestión de la continuidad de su negocio.

18.2 Ferrero cuenta con la redundancia suficiente para cumplir los requisitos de disponibilidad.

19. CUMPLIMIENTO

19.1 Ferrero tiene identificadas y ha documentado sus obligaciones de seguridad de la información frente a las autoridades (tales como las autoridades de control) y terceros, incluyendo en relación con la propiedad intelectual, corporativa u otros registros, la privacidad y la encriptación.

Última actualización: junio de 2018