Declaración de Aplicabilidad

SMARTME ANALYTICS

La organización se dedica a la investigación de mercados usando como herramienta una tecnología observacional propietaria. Nuestra fuente de datos es el BIG DATA generado obtenido por medio de nuestra tecnología observacional de nuestro panel – comunidad de usuarios que tienen instalada nuestra APP que contiene la tecnología extractora de data. La data obtenida se procesa, se filtra, se analiza y estructura por medio de procesos de la ciencia de los datos, por medio de KPIs de negocio, generando información útil para nuestros clientes.

Nuestros clientes son empresas de diferentes sectores o verticales (banca y seguros, retail, restaurant & delivery, redes sociales, deportes, y así hasta 12), que tengan una alto grado de digitalización o pretendan alcanzarlo, entrando sobre todo por departamentos de marketing, departamentos de data y departamentos de investigación, cuya necesidad es información sobre el comportamiento y las pautas de conducta de sus propios clientes, y/o de los de la competencia, generalmente usuarios y consumidores finales de productos y servicios, y del mercado competitivo en el que se enmarca su actividad.

"Nuestras soluciones ofrecen a nuestros clientes insights de negocio sobre el buyer persona y el panorama competitivo en el medio digital de su sector".

Además, la tecnología y solución de SMARTME permite medir la audiencia de canales digitales y off line, y la eficacia publicitaria cross media.

El negocio de SMARTME en B2B (business to business).

SMARTME también tiene como línea de negocio licenciar su modelo tecnológico y de negocio a nivel internacional, permitiendo a sus licenciatarios utilizar su tecnología y su Know how para extractar data, procesarla por medio de la ciencia de los datos recogida en los algoritmos de Smartme, y ofrecerla al mercado.

ALCANCE DEL SISTEMA

El alcance del sistema es la investigación de mercados mediante tecnología observacional propietaria.

La organización ha decidido incluir los servicios de CONSUMER PERSONA, COMPETITOR LANDSCAPE y CROSS MEDIA MONITOR dentro del alcance del sistema de acuerdo al anexo D, de observación digital, en su totalidad, y a los anexos A, B, C, E y F parcialmente, de la norma ISO 20252:2019 sobre la Investigación de Mercados. De igual forma, la organización ha decidido seguir el esquema ISO 27001:2013 sobre la Gestión de la Seguridad de la Información. Ambas normas son de obligado cumplimiento por todos los empleados de SMARTME ANALYTICS.

Requisitos de APLICABILIDAD

ISO 27001. Anexo A. Objetivos de control y controles de referencia

Nivel 1	Nivel 2	Requisito	Aplica	Aplicabilidad	Responsables	Medidas de Seguridad
A.5. Políticas de seguridad	**A.5.1. Directrices de gestión de la seguridad de la información**	A.5.1.1. Políticas para la seguridad de la información. Un conjunto de políticas para la seguridad de la información debe ser definido, aprobado por la Dirección, publicado y comunicado a los empleados y partes externas relevantes.	Sí	La organización necesita definir una política que sirva como marco normativo y de establecimiento de objetivos en términos de seguridad de la información. SMARTME ANALYTICS ha desarrollado una política de seguridad de la información, que tiene una aplicabilidad global para todo el SGSI.	Dirección	PSI - Política de Seguridad de la Información
A.5. Políticas de seguridad	**A.5.1. Directrices de gestión de la seguridad de la información**	A.5.1.2. Revisión de las políticas para la seguridad de la información. Las políticas de seguridad de la información deben revisarse a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.	Sí	La política se revisa según la metodología establecida en la ficha de proceso FP-20 Revisión del Sistema y esta revisión queda evidenciada en la fecha de aprobación registrada en la misma política, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia..	Dirección	FP-20 - Revisión del Sistema PSI - Política de Seguridad de la Información
A.6. Organización de la seguridad de la Información	**A.6.1. Organización interna**	A.6.1.1. Roles y responsabilidades en seguridad de la información. Todas las responsabilidades en seguridad de la información deben ser definidas y asignadas.	Sí	La determinación de roles y responsabilidades es necesaria para la especialización y delegación de tareas y la involucración de todo el equipo. SMARTME ANALYTICS ha definido y entregado perfiles a sus empleados en los que se describen las competencias técnicas, sociales y organizativas, y la formación necesaria para el puesto incluida la referente a la seguridad de la información. La relación de subordinación de responsabilidades entre los perfiles queda establecida en el organigrama de la organización.	Dirección	RE-04 - Perfil OR - Organigrama
A.6. Organización de la seguridad de la Información	**A.6.1. Organización interna**	A.6.1.2. Segregación de tareas. Las funciones y áreas de responsabilidad deben segregarse para reducir la posibilidad de que se produzcan modificaciones no autorizadas o no intencionadas o usos indebidos de los activos de la organización.	Sí	La definición de responsables entre diferentes miembros del equipo permite disminuir el riesgo de uso inadecuado de los activos de información. La responsabilidad de las tareas y los procesos de la organización quedan definidos y comunicados en los perfiles entregados a los empleados. Por otro lado, estas mismas responsabilidades quedan asociadas a cada proceso y tarea en las fichas de proceso donde se describen.	Dirección	RE-04 - Perfil
A.6. Organización de la seguridad de la Información	**A.6.1. Organización interna**	A.6.1.3. Contacto con las autoridades. Deben mantenerse los contactos apropiados con las autoridades pertinentes.	Sí	La responsabilidad de la comunicación queda definida en el perfil correspondiente. Dicha comunicación se garantiza mediante la ficha de proceso que establece la sistemática y el cuadro que enumera todos los mensajes a comunicar.	Dirección Responsable del Sistema	RE-04 - Perfil FP-13 - Comunicación RE-29 - Cuadro de Comunicación
A.6. Organización de la seguridad de la Información	**A.6.1. Organización interna**	A.6.1.4. Contacto con grupos de interés especial. Deben mantenerse los contactos apropiados con grupos de interés especial, u otros foros y asociaciones profesionales especializados en seguridad.	Sí	La organización identifica sus partes interesadas que se evidencian en el registro correspondiente y mantiene el contacto pertinente con cada una de ellas para garantizar el cumplimiento de sus requisitos en cuanto a seguridad de la información. Así mismo, está	Dirección Responsable del Sistema	FP-13 - Comunicación RE-29 - Cuadro de Comunicación RE-40 - Requisitos de las Partes Interesadas

				adherida a diferentes foros especializados también en la seguridad de la información para mantenerse actualizada con los avances del sector. La comunicación se garantiza mediante la ficha de proceso que establece la sistemática y el cuadro que enumera todos los mensajes a comunicar.		
A.6. Organización de la seguridad de la Información	**A.6.1. Organización interna**	A.6.1.5. Seguridad de la información en la gestión de proyectos. La seguridad de la información debe tratarse dentro de la gestión de proyectos, independientemente de la naturaleza del proyecto.	Sí	La organización diseña y desarrolla las herramientas con las que trabaja y lo hace según las buenas prácticas establecidas en su protocolo para el Desarrollo Seguro. Esto es fundamental para garantizar la seguridad de la información de todo el servicio que se le presta al cliente. El equipo de data scientists y data analysts trabaja posteriormente, según el código interno de las mejores prácticas comunicado por la propia organización y de obligado cumplimiento.	Tecnología, Procesos, Herramientas	IT-11-01 - Buenas Prácticas de Desarrollo Seguro 22 - Acceso a CPD 70 - Acceso ETHERNET a LAN 21 - Seguridad de oficinas 20 - Tarjeta de acceso al edificio y a las oficinas 64 - Acceso a ordenador personal 28 - Acceso a SMARTME DASHBOARDS integrado en la herramienta de usuario 24 - Accesos a base de datos Data Warehouse 23 - Accesos a base de datos Transaccional (AMAZON) 67 - Accesos a BITRIX 33 - Accesos a la red VPN (DOMINION) 31 - Accesos a la red WI-FI (DOMINION) 66 - Accesos a TRELLO
A.6. Organización de la seguridad de la Información	**A.6.2. Los dispositivos móviles y el teletrabajo**	A.6.2.1. Política de dispositivos móviles. Se debe adoptar una política y unas medidas de seguridad adecuadas para la protección contra los riesgos de la utilización de dispositivos móviles.	Sí	SMARTME ANALYTICS cuenta con un conjunto de smartphones y portátiles identificados en su inventario de equipos y ha desarrollado un protocolo de seguridad para dispositivos móviles que ha distribuido y ha formado en él a todos los empleados con móvil de empresa. El protocolo y la formación quedan evidenciados mediante la instrucción técnica y la acción formativa respectivas.	Responsable del Sistema	IT-70-01 - Protocolo de Seguridad de la Información RE-08 - Acción formativa RE-10 - Inventario de Equipos
A.6. Organización de la seguridad de la Información	**A.6.2. Los dispositivos móviles y el teletrabajo**	A.6.2.2. Teletrabajo. Se debe implementar una política y unas medidas de seguridad adecuadas para proteger la información accedida, tratada o almacenada en emplazamientos de teletrabajo.	Sí	La organización admite el teletrabajo cuando las condiciones de los proyectos resultan óptimas, por lo tanto es necesario contar con las medidas y elementos adecuados para garantizar la seguridad de la información tratada registrados en el inventario de equipos. La organización ha desarrollado y comunicado un protocolo de obligado cumplimiento por sus empleados evidenciado mediante las correspondientes instrucción técnica y acción formativa.	Responsable del Sistema	IT-70-01 - Protocolo de Seguridad de la Información RE-08 - Acción formativa RE-10 - Inventario de Equipos 64 - Acceso a ordenador personal 33 - Accesos a la red VPN (DOMINION) 69 - Cuentas de usuario de Microsoft
A.7. Seguridad relativa a los recursos humanos	**A.7.1. Antes del empleo**	A.7.1.1. Investigación de antecedentes. La comprobación de los antecedentes de todos los candidatos al puesto de trabajo se debe llevar a cabo de acuerdo con las leyes, normativa y códigos éticos que sean de aplicación y debe ser proporcional a las necesidades del negocio, la clasificación de la información a la que se accede y los riesgos percibidos.	Sí	Para prevenir riesgos de violación de las políticas y procedimientos establecidos en cuanto a la seguridad de la información, la organización cuenta con una ficha de personal completada con los currículum vitae de todos los empleados y la formación en seguridad de la información recibida en SMARTME ANALYTICS. Por otro lado, todos los empleados firman el compromiso de cumplimiento del protocolo de seguridad de la información, que se adjunta a su misma ficha de personal.	Responsable del Sistema	RE-06 - Ficha de Personal IT-70-01 - Protocolo de Seguridad de la Información
A.7. Seguridad relativa a los recursos humanos	**A.7.1. Antes del empleo**	A.7.1.2. Términos y condiciones del empleo. Como parte de sus obligaciones contractuales, los empleados y contratistas deben establecer los términos y condiciones en su contrato de trabajo en lo que respecta a la seguridad de la información, tanto hacia el empleado como hacia la organización.	Sí	Previamente a la incorporación al equipo, los candidatos deben ser y son informados como parte de sus obligaciones contractuales para con la organización sobre los procedimientos que le afecten relacionados con la seguridad de la información. Compromiso evidenciado con la firma del protocolo de seguridad de la información desarrollado y entregado por SMARTME ANALYTICS.	Responsable del Sistema	IT-70-01 - Protocolo de Seguridad de la Información
A.7. Seguridad relativa a los recursos humanos	**A.7.2. Durante el empleo**	A.7.2.1. Responsabilidades de gestión. La dirección debe exigir a los empleados y contratistas, que apliquen la seguridad de la información de acuerdo con las políticas y procedimientos establecidos en la organización.	Sí	La organización debe garantizar que las políticas y procedimientos relacionados con la seguridad de la información se cumplen y por ello organiza acciones formativas y de concienciación periódicamente. Evidenciado mediante los protocolos para empleados y para colaboradores entendidos, aceptados y firmados por los mismos.	Responsable del Sistema	IT-70-01 - Protocolo de Seguridad de la Información IT-70-02 - Protocolo de Seguridad de la Información para colaboradores RE-07 - Plan de Formación
A.7. Seguridad relativa a los recursos humanos	**A.7.2. Durante el empleo**	A.7.2.2. Concienciación, educación y capacitación en seguridad de la información. Todos los empleados de la organización y, cuando corresponda, los contratistas, deben recibir una adecuada educación, concienciación y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según corresponda a su puesto de trabajo.	Sí	Es necesario que los empleados tengan una formación adecuada y actualizada respecto de los últimos cambios en el sistema de gestión de la seguridad de la información. Evidenciadas mediante las acciones formativas correspondientes y los resultados de la evaluación del desempeño realizadas a todos los empleados.	Responsable del Sistema	RE-08 - Acción formativa RE-09 - Evaluación
A.7. Seguridad relativa a los recursos humanos	**A.7.2. Durante el empleo**	A.7.2.3. Proceso disciplinario. Debe existir un proceso disciplinario formal que haya sido comunicado a los empleados, que recoja las acciones a tomar ante aquellos que hayan provocado una brecha de seguridad.	Sí	Con el objetivo de garantizar el cumplimiento de la política y los procedimientos establecidos, se han redactado las medidas disciplinarias que se han considerado adecuadas y se evidencian mediante la instrucción técnica que establece el protocolo de seguridad de la información	Responsable del Sistema	IT-70-01 - Protocolo de Seguridad de la Información

				comunicada y firmada por todos los empleados de SMARTE ANALYTICS.		
A.7. Seguridad relativa a los recursos humanos	**A.7.3. Finalización del empleo o cambio en el puesto de trabajo**	A.7.3.1. Responsabilidades ante la finalización o cambio. Las responsabilidades en seguridad de la información y obligaciones que siguen vigentes después del cambio o finalización del empleo se deben definir, comunicar al empleado o contratista y se deben cumplir.	Sí	Una vez finalizada la relación contractual con SMARTME, los empleados y colaboradores mantienen las obligaciones de confidencialidad y otros criterios que puedan afectar a la seguridad de la información de la organización. Las responsabilidades a la finalización del contrato quedan detalladas en la instrucción técnica de seguridad de la información entregada y firmada por cada empleado.	Dirección Responsable del Sistema	IT-70-02 - Protocolo de Seguridad de la Información para colaboradores
A.8. Gestión de activos	**A.8.1. Responsabilidad sobre los activos**	A.8.1.1. Inventario de activos. La información y otros activos asociados a la información y a los recursos para el tratamiento de la información deben estar claramente identificados y debe elaborarse y mantenerse un inventario.	Sí	Con el fin de tenerlos controlados, la organización ha desarrollado y mantiene un inventario de activos de la información y un diagrama de la configuración en los que se establecen las relaciones de dependencia existentes entre ellos. Así mismo, mantiene un inventario de equipos detallado en el que cada elemento está relacionado con el activo correspondiente.	Responsable del Sistema	RE-723 - Listado de Activos RE-10 - Inventario de Equipos RE-701 - Diagrama de Configuración
A.8. Gestión de activos	**A.8.1. Responsabilidad sobre los activos**	A.8.1.2. Todos los activos que figuran en el inventario deben tener un propietario.	Sí	Para facilitar su control y garantizar su seguridad, los activos de información de la organización deben asociarse a un propietario que se compromete a cumplir el protocolo de seguridad correspondiente. El propietario de cada activo queda identificado en el inventario de equipos.	Responsable del Sistema	RE-10 - Inventario de Equipos IT-70-01 - Protocolo de Seguridad de la Información
A.8. Gestión de activos	**A.8.1. Responsabilidad sobre los activos**	A.8.1.3. Uso aceptable de los activos. Se deben identificar, documentar e implementar las reglas de uso aceptable de la información y de los activos asociados con los recursos para el tratamiento de la información.	Sí	Los activos de información de la organización suponen un recurso que debe utilizarse para los fines y condiciones para los que se adquirió. El uso aceptable de los activos se establece en la instrucción técnica de seguridad de la información que se entrega y firman todos los empleados.	Responsable del Sistema	IT-70-01 - Protocolo de Seguridad de la Información
A.8. Gestión de activos	**A.8.1. Responsabilidad sobre los activos**	A.8.1.4. Devolución de los activos. Todos los empleados y terceras partes deben devolver todos los activos de la organización que estén en su poder al finalizar su empleo, contrato o acuerdo.	Sí	Una vez finalizado el uso del activo, su propietario debe devolverlo a la organización cumpliendo las medidas de seguridad establecidas. La devolución de los activos se produce tal y como se define en las instrucciones técnicas entregadas y firmadas por los empleados y otros colaboradores y queda evidenciada en el registro de propiedad de activos.	Responsable del Sistema	RE-10 - Inventario de Equipos IT-70-01 - Protocolo de Seguridad de la Información
A.8. Gestión de activos	**A.8.2. Clasificación de la información**	A.8.2.1. Clasificación de la información. La información debe ser clasificada en términos de la importancia de su revelación frente a requisitos legales, valor, sensibilidad y criticidad ante revelación o modificación no autorizadas.	Sí	Con el objetivo de equilibrar la confidencialidad y la agilidad en la gestión SMARTME clasifica su información documentada estableciendo diferentes niveles de seguridad para cada tipo de documento. La información se clasifica según la sistemática establecida en la ficha de proceso para la seguridad de la información y queda evidenciada en registro de clasificación de la información.	Responsable del Sistema	FP-70 - Seguridad de la Información RE-01 - Listado de Documentos del Sistema
A.8. Gestión de activos	**A.8.2. Clasificación de la información**	A.8.2.2. Etiquetado de la información. Debe desarrollarse e implantarse un conjunto adecuado de procedimientos para etiquetar la información, de acuerdo con el esquema de clasificación por la organización.	Sí	Para garantizar que cada destinatario de la documentación conoce el nivel de clasificación de la misma, el listado de información documentada aparece clasificado en la distribución de dichos documentos, al igual que aparecen clasificados los mensajes del cuadro de comunicación. La información clasificada se etiqueta según la sistemática establecida en la ficha de proceso para la seguridad de la información y queda evidenciada en registro de clasificación de la información.	Responsable del Sistema	FP-70 - Seguridad de la Información RE-01 - Listado de Documentos del Sistema RE-29 - Cuadro de Comunicación
A.8. Gestión de activos	**A.8.2. Clasificación de la información**	A.8.2.3. Manipulación de la información. Debe desarrollarse e implantarse un conjunto adecuado de procedimientos para la manipulación de la información, de acuerdo con el esquema de clasificación adoptado por la organización.	Sí	Con el fin de garantizar la manipulación adecuada de la información, además de su etiquetado se han desarrollado los procedimientos pertinentes y se ha formado a los empleados en ello. El procedimiento para la manipulación de la información queda definido en la ficha de proceso y las instrucciones técnicas para la seguridad de la información.	Responsable del Sistema	FP-70 - Seguridad de la Información IT-70-01 - Protocolo de Seguridad de la Información IT-70-02 - Protocolo de Seguridad de la Información para colaboradores RE-07 - Plan de Formación
A.8. Gestión de activos	**A.8.3. Manipulación de los soportes**	A.8.3.1. Gestión de soportes extraíbles. Se deben implementar procedimientos para la gestión de los soportes extraíbles, de acuerdo con el esquema de clasificación adoptado por la organización.	Sí	La organización prohíbe el uso de soportes extraíbles salvo en casos de autorización expresa por la Dirección, en cuyo caso se aplicará el protocolo correspondiente al tipo de clasificación de los documentos extraídos. El procedimiento para la gestión de los soportes extraíbles queda definido en la ficha de proceso y en los protocolos (instrucciones técnicas) entregados a empleados y colaboradores para la seguridad de la información.	Responsable del Sistema	FP-70 - Seguridad de la Información IT-70-02 - Protocolo de Seguridad de la Información para colaboradores IT-70-01 - Protocolo de Seguridad de la Información
A.8. Gestión de activos	**A.8.3. Manipulación de los soportes**	A.8.3.2. Eliminación de soportes. Los soportes deben eliminarse de forma segura cuando ya no vayan a ser	Sí	El uso de soportes de información está expresamente prohibido por la Dirección, salvo en casos puntuales y autorizados. Los soportes se eliminan	Responsable del Sistema	FP-70 - Seguridad de la Información IT-70-02 - Protocolo de Seguridad de la Información para colaboradores

		necesarios, mediante procedimientos formales.		cuando proceden según la sistemática establecida en la ficha de proceso y las instrucciones técnicas entregadas para la seguridad de la información y la eliminación queda evidenciada en el registro de gestión de activos.		IT-70-01 - Protocolo de Seguridad de la Información
A.8. Gestión de activos	**A.8.3. Manipulación de los soportes**	A.8.3.3. Soportes físicos en tránsito. Durante el transporte fuera de los límites físicos de la organización, los soportes que contengan información deben estar protegidos contra accesos no autorizados, usos indebidos o deterioro.	Sí	Los soportes de información físicos están expresamente prohibidos por la Dirección, salvo en caso de necesidad excepcional y con autorización expresa. El procedimiento de uso de los soportes físicos en tránsito queda establecido en las instrucciones técnicas entregadas a empleados y colaboradores.	Responsable del Sistema	IT-70-02 - Protocolo de Seguridad de la Información para colaboradores IT-70-01 - Protocolo de Seguridad de la Información
A.9. Control de acceso	**A.9.1. Requsitos de negocio para el control de acceso**	A.9.1.2. Acceso a las redes y a los servicios de red. Únicamente se debe proporcionar a los usuarios el acceso a las redes y a los servicios en red para cuyo uso hayan sido específicamente autorizados.	Sí	El equipo de SMARTME trabaja en red compartiendo archivos y aplicaciones, por ello es necesario controlar los accesos a la misma cuidando que cada persona acceda exclusivamente a aquella información a la que se le ha concedido permiso. Los permisos de acceso a las redes y servicios de red se evidencian en el registro de Control de Acceso a los activos de la información. Este control se audita al menos una vez al año.	Responsable del Sistema	RE-733 - Control de Accesos 70 - Acceso ETHERNET a LAN 65 - Acceso único SMARTME APP - BBDD Transaccional (AMAZON) 23 - Accesos a base de datos Transaccional (AMAZON) 67 - Accesos a BITRIX 25 - Accesos a GestNear (DOMINION) 33 - Accesos a la red VPN (DOMINION) 31 - Accesos a la red WI-FI (DOMINION) 26 - Accesos a Microsoft Dynamics CRM 68 - Accesos a TQNET 66 - Accesos a TRELLO 69 - Cuentas de usuario de Microsoft
A.9. Control de acceso	**A.9.2. Gestión de acceso de usuario**	A.9.2.1. Registro y baja de usuario. Debe implantarse un procedimiento formal de registro y retirada de usuarios que haga posible la asignación de los derechos de acceso.	Sí	Al trabajar en red y utilizar servicios de red resulta imprescindible que la organización mantenga un registro de altas y bajas de acceso a los mismos. En el Control de Acceso a los activos de la información se registran las altas y bajas de los usuarios. Este control se audita al menos una vez al año.	Responsable del Sistema	RE-733 - Control de Accesos
A.9. Control de acceso	**A.9.2. Gestión de acceso de usuario**	A.9.2.2. Provisión de acceso de usuario. Debe implantarse un procedimiento formal para asignar o revocar los derechos de acceso para todos los tipos de usuario de todos los sistemas y servicios.	Sí	Como parte del control de accesos a sus activos de la información, la organización requiere de un procedimiento formal para la asignación y desasignación de los permisos. El procedimiento queda establecido en la instrucción técnica que describe el Protocolo para la Seguridad de la Información.	Responsable del Sistema	IT-70-01 - Protocolo de Seguridad de la Información RE-723 - Listado de Activos
A.9. Control de acceso	**A.9.2. Gestión de acceso de usuario**	A.9.2.3. Gestión de privilegios de acceso. La asignación y el uso de privilegios de acceso debe estar restringida y controlada.	Sí	Para todos los activos inventariados en la organización, tanto físicos como virtuales, es necesario establecer niveles de permiso según el nivel de responsabilidad del usuario. El procedimiento para la asignación y el uso de privilegios de acceso se establece en la instrucción técnica para el Protocolo de Seguridad de la Información y dichos privilegios quedan evidenciados en el registro del Control de Acceso.	Responsable del Sistema	IT-70-01 - Protocolo de Seguridad de la Información RE-733 - Control de Accesos RE-723 - Listado de Activos
A.9. Control de acceso	**A.9.2. Gestión de acceso de usuario**	A.9.2.4. Gestión de la información secreta de autenticación de los usuarios. La asignación de la información secreta de autenticación debe ser controlada a través de un proceso formal de gestión.	Sí	Para garantizar la confidencialidad de la información es necesario que la organización desarrolle un procedimiento para la comunicación de las credenciales de acceso a los diferentes activos. El procedimiento para la gestión de la asignación de la información secreta de autenticación de los usuarios queda establecido en la instrucción técnica del Protocolo para la Seguridad de la Información.	Responsable del Sistema	IT-70-01 - Protocolo de Seguridad de la Información RE-723 - Listado de Activos
A.9. Control de acceso	**A.9.2. Gestión de acceso de usuario**	A.9.2.5. Revisión de los derechos de acceso de usuario. Los propietarios de los activos deben revisar los derechos de acceso de usuario a intervalos regulares.	Sí	La organización revisa los derechos de acceso de los usuarios a los activos de la información y registra los resultados de dicha revisión en informes de auditoría del control de acceso.	Responsable del Sistema	RE-733 - Control de Accesos
A.9. Control de acceso	**A.9.2. Gestión de acceso de usuario**	A.9.2.6. Retirada o reasignación de los derechos de acceso. Los derechos de acceso de todos los empleados y terceras partes, a la información y a los recursos de tratamiento de la información deben ser retirados a la finalización del empleo, del contrato o del acuerdo, o ajustados en caso de cambio.	Sí	Es necesario para garantizar la confidencialidad de la información contar con un procedimiento para la retirada de permisos a los empleados y otros colaboradores cuando finalice la actividad que motivó su asignación. Los derechos de acceso se retiran a empleados y colaboradores, tal y como se establece en los protocolos de Seguridad de la Información para empleados y colaboradores, que han sido comunicados y entregados a estos con su consentimiento firmado.	Responsable del Sistema	IT-70-01 - Protocolo de Seguridad de la Información IT-70-02 - Protocolo de Seguridad de la Información para colaboradores RE-723 - Listado de Activos
A.9. Control de acceso	**A.9.3. Responsabilidades del usuario**	A.9.3.1. Uso de la información secreta de autenticación. Se debe requerir a los usuarios que sigan las prácticas de la organización en el uso de la información secreta de autenticación.	Sí	Es necesario para garantizar la confidencialidad de la información que los usuarios de la misma cumplan la normativa establecida por la organización. La organización ha formado y concienciado a los empleados en el uso secreto de la autenticación a los sistemas. La concienciación se evidencia mediante la correspondiente acción formativa y los protocolos de seguridad de la información.	Responsable del Sistema	IT-70-02 - Protocolo de Seguridad de la Información para colaboradores IT-70-01 - Protocolo de Seguridad de la Información RE-07 - Plan de Formación
A.9. Control de acceso	**A.9.4. Control de acceso a sistemas y**	A.9.4.1. Restricción del acceso a la información. Se debe restringir el	Sí	Al igual que el acceso a los activos, es necesario gestionar los permisos dentro	Responsable del Sistema	RE-733 - Control de Accesos RE-723 - Listado de Activos

	aplicaciones	acceso a la información y a las funciones de las aplicaciones, de acuerdo con la política de control de acceso definida.		de las diferentes herramientas de información y los permisos de acceso a la diferente documentación de la organización. Estas herramientas se identifican como SOFTWARE en el listado de activos y en el inventario de elementos de infraestructura. El acceso a la información se restringe en base a la clasificación de la propia información y al registro de Control de Accesos.		RE-10 - Inventario de Equipos
A.9. Control de acceso	**A.9.4. Control de acceso a sistemas y aplicaciones**	A.9.4.2. Procedimientos seguros de inicio de sesión. Cuando así se requiera en la política de control de acceso a los sistemas y aplicaciones se debe controlar por medio de un procedimiento seguro de inicio de sesión.	Sí	Los procedimientos seguros de inicio de sesión se establecen en el Protocolo para la Seguridad de la Información.	Responsable del Sistema	IT-70-01 - Protocolo de Seguridad de la Información
A.9. Control de acceso	**A.9.4. Control de acceso a sistemas y aplicaciones**	A.9.4.3. Sistema de gestión de contraseñas. Los sistemas para la gestión de contraseñas deben ser interactivos y establecer contraseñas seguras y robustas.	Sí	SMARTME cuenta con unos sistemas de información totalmente informatizados, por lo que toda la información que maneja se realiza a través de una aplicación. Cada una de estas aplicaciones cuenta con la funcionalidad de gestión de usuarios para controlar su acceso y los permisos dentro de la misma. En el inventario de equipos se listan todos los accesos a las mismas.	Responsable del Sistema	RE-10 - Inventario de Equipos 64 - Acceso a ordenador personal 27 - Acceso a SMARTME APP integrado en la aplicación 28 - Acceso a SMARTME DASHBOARDS integrado en la herramienta de usuario 65 - Acceso único SMARTME APP - BBDD Transaccional (AMAZON) 24 - Accesos a base de datos Data Warehouse 23 - Accesos a base de datos Transaccional (AMAZON) 67 - Accesos a BITRIX 25 - Accesos a GestNear (DOMINION) 33 - Accesos a la red VPN (DOMINION) 31 - Accesos a la red WI-FI (DOMINION) 26 - Accesos a Microsoft Dynamics CRM 68 - Accesos a TQNET 66 - Accesos a TRELLO 69 - Cuentas de usuario de Microsoft
A.9. Control de acceso	**A.9.4. Control de acceso a sistemas y aplicaciones**	A.9.4.4. Uso de utilidades con privilegios del sistema. Se debe restringir y controlar rigurosamente el uso de utilidades que puedan ser capaces de invalidar los controles del sistema y de la aplicación.	Sí	Todas las herramientas, incluidas las utilidades con privilegios del sistema, quedan inventariadas en el Listado de Activos y en el Inventario de Equipos. La organización no permite el uso de herramientas que no estén incluidas en estos listados. Sólo el administrador del sistema (Responsable del Sistema) puede instalar aplicaciones en los equipos.	Responsable del Sistema	RE-723 - Listado de Activos RE-10 - Inventario de Equipos 78 - Acceso de administrador del sistema
A.9. Control de acceso	**A.9.4. Control de acceso a sistemas y aplicaciones**	A.9.4.5. Control de acceso al código fuente de los programas. Se debe restringir el acceso al código fuente de los programas.	Sí	Sólo los data analysts y los data scientists deben tener acceso al código fuente de los programas, en el caso de SMARTME, a los scripts y tablas de base de datos. Los permisos de acceso a los códigos fuente de los programas se establecen y quedan registrados en el Control de Accesos.	Responsable del Sistema	RE-733 - Control de Accesos 23 - Accesos a base de datos Transaccional (AMAZON) 69 - Cuentas de usuario de Microsoft
A.10. Criptografía	**A.10.1. Controles criptográficos**	A.10.1.1. Política de uso de los controles criptográficos. Se debe desarrollar e implementar una política sobre el uso de los controles criptográficos para proteger las información.	Sí	La Organización hace uso de controles criptográficos cuando transmite información clasificada como corporativa o confidencial, según lo establece en su Política de Controles Criptográficos.		IT-70-03 - Política de Controles Criptográficos 94 - Cifrado de VPN 92 - Protocolo HTTPS para aplicaciones web 93 - Protocolo HTTPS para servicio web 91 - Protocolo SSL/TLS para correo electrónico
A.10. Criptografía	**A.10.1. Controles criptográficos**	A.10.1.2. Gestión de claves. Se debe desarrollar e implementar una política sobre el uso, la protección y la duración de las claves de cifrado a lo largo de todo su ciclo de vida.	No	La Organización hace uso de criptografía a través del uso de aplicaciones estándares del mercado, a las que exige el uso de estos controles. La Organización no tiene el control de las claves de cifrado.		
A.11. Seguridad física y del entorno	**A.11.1. Áreas seguras**	A.11.1.1. Perímetro de seguridad física. Se deben utilizar perímetros de seguridad para proteger las áreas que contienen información sensible así como los recursos de tratamiento de la información.	Sí	Todas las zonas desde las que resulta accesible la información de la organización deben tener las medidas de seguridad adecuadas. La Organización cuenta con un plano de las instalaciones con el perímetro y los elementos de seguridad identificados. Estos elementos forman parte del inventario de elementos de infraestructura y están marcados como elementos de seguridad. Las medidas de seguridad asociadas a cada activo se evidencian en el diagrama de configuración.	Responsable del Sistema	RE-10 - Inventario de Equipos RE-701 - Diagrama de Configuración 76 - Grupo Electrógeno (DOMINION) 17 - Protección Contra Incendios 80 - Puerta de seguridad de entrada a las plantas 81 - Puerta de seguridad de entrada al CPD 75 - Sistema de Baterías (DOMINION) 79 - Torno de acceso a los ascensores
A.11. Seguridad física y del entorno	**A.11.1. Áreas seguras**	A.11.1.2. Controles físicos de entrada. Las áreas seguras deben estar protegidas mediante controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado.	Sí	Sólo las personas autorizadas para ello deben tener acceso físico a las zonas desde las que resulta accesible la información de la organización. La Organización cuenta con controles físicos de entrada identificados como elementos de seguridad en el Inventario de Equipos. Las medidas de seguridad asociadas a cada activo se evidencian en el diagrama de configuración.	Responsable del Sistema	RE-10 - Inventario de Equipos RE-701 - Diagrama de Configuración 22 - Acceso a CPD 21 - Seguridad de oficinas 20 - Tarjeta de acceso al edificio y a las oficinas 64 - Acceso a ordenador personal
A.11. Seguridad física y del entorno	**A.11.1. Áreas seguras**	A.11.1.3. Seguridad de oficinas, despachos y recursos. Para las oficinas, despachos y recursos, se debe diseñar y aplicar la seguridad física.	Sí	SMARTME desarrolla su actividad desde sus oficinas situadas en el Edificio Ática de Pozuelo de Alarcón. Los elementos de seguridad de las oficinas, despachos y recursos están identificados en el Inventario de Equipos y se gestionan según la sistemática establecida en la ficha de procesos para las	Responsable del Sistema	FP-03 - Infraestructuras RE-10 - Inventario de Equipos RE-701 - Diagrama de Configuración 76 - Grupo Electrógeno (DOMINION) 17 - Protección Contra Incendios 80 - Puerta de seguridad de entrada a las plantas 81 - Puerta de seguridad de entrada al

				Infraestructuras. Las medidas de seguridad asociadas a cada activo se evidencian en el diagrama de configuración.		CPD 21 - Seguridad de oficinas 75 - Sistema de Baterías (DOMINION) 79 - Torno de acceso a los ascensores
A.11. Seguridad física y del entorno	**A.11.1. Áreas seguras**	A.11.1.4. Protección contra las amenazas externas y ambientales. Se debe diseñar y aplicar una protección física contra desastres naturales, ataques provocados por el hombre o accidentes.	Sí	SMARTME desarrolla su actividad en la segunda planta de un edificio inteligente dentro del municipio de Pozuelo de Alarcón. La Organización cuenta con un sistema de protección física cuyos elementos están identificados en el Inventario de Equipos diseñado en base a un análisis exhaustivo de los riesgos asociados a los activos de la información. Las medidas de seguridad asociadas a cada activo se evidencian en el diagrama de configuración.	Responsable del Sistema	RE-10 - Inventario de Equipos RE-727 - Tabla de riesgos RE-701 - Diagrama de Configuración 76 - Grupo Electrógeno (DOMINION) 17 - Protección Contra Incendios 80 - Puerta de seguridad de entrada a las plantas 81 - Puerta de seguridad de entrada al CPD 21 - Seguridad de oficinas 75 - Sistema de Baterías (DOMINION) 79 - Torno de acceso a los ascensores
A.11. Seguridad física y del entorno	**A.11.1. Áreas seguras**	A.11.1.5. El trabajo en áreas seguras. Se deben diseñar e implementar procedimientos para trabajar en las áreas seguras.	Sí	Sólo se identifica un área segura en las instalaciones de SMARTME y es el cuarto que aloja el CPD en el edificio. El mantenimiento de esta sala y el del propio CPD está externalizado a la empresa DOMINION, que son los actuales propietarios del edificio y del grupo de empresas del que forma parte SMARTME. Ninguna persona de SMARTME tiene acceso a esta sala.	Responsable del Sistema	IT-70-01 - Protocolo de Seguridad de la Información IT-70-02 - Protocolo de Seguridad de la Información para colaboradores 22 - Acceso a CPD 81 - Puerta de seguridad de entrada al CPD
A.11. Seguridad física y del entorno	**A.11.1. Áreas seguras**	A.11.1.6. Áreas de carga y descarga. Deben controlarse los puntos de acceso tales como las áreas de carga y descarga y otros puntos, donde pueda acceder personal no autorizado a las instalaciones, y, si es posible, aislar dichos puntos de los recursos de tratamiento de la información para evitar accesos no autorizados.	Sí	Las áreas de carga y descarga del edificio pertenecen y están controladas por DOMINION, que es el propietario del grupo de empresas al que pertenece SMARTME. La organización tiene identificados y controlados los puntos de acceso a sus instalaciones en un Plano de las Instalaciones y en el Inventario de Equipos. Las medidas de seguridad asociadas a cada activo se evidencian en el diagrama de configuración.	Responsable del Sistema	RE-10 - Inventario de Equipos RE-701 - Diagrama de Configuración
A.11. Seguridad física y del entorno	**A.11.2. Seguridad de los equipos**	A.11.2.1. Emplazamiento y protección de equipos. Los equipos deben situarse o protegerse de forma que se reduzcan los riesgos de las amenazas y los riesgos ambientales, así como las oportunidades de que se produzcan accesos no autorizados.	Sí	Los activos de la información de SMARTME se localizan en la segunda planta del Edificio Ática de Pozuelo de Alarcón, propiedad de DOMINION. Existen medidas de seguridad de acceso al edificio y a la planta. El emplazamiento de los equipos se ha diseñado teniendo en cuenta un análisis de riesgos de los activos de información y queda identificado en el Plano de las Instalaciones.	Responsable del Sistema	RE-727 - Tabla de riesgos RE-10 - Inventario de Equipos 76 - Grupo Electrógeno (DOMINION) 17 - Protección Contra Incendios 80 - Puerta de seguridad de entrada a las plantas 81 - Puerta de seguridad de entrada al CPD 21 - Seguridad de oficinas 75 - Sistema de Baterías (DOMINION) 79 - Torno de acceso a los ascensores
A.11. Seguridad física y del entorno	**A.11.2. Seguridad de los equipos**	A.11.2.2. Instalaciones de suministro. Los equipos deben estar protegidos contra fallos de alimentación y otras alteraciones causadas por fallos en las instalaciones de suministro.	Sí	Las instalaciones de suministro son un activo para la organización y, tal y como se describe en la tabla de riesgos, un fallo en el mismo supondría una contingencia que poner en marcha. La protección de los equipos contra fallos de alimentación se define mediante el análisis de riesgos de los activos de información y se identifican en el Inventario de Equipos.	Responsable del Sistema	RE-727 - Tabla de riesgos RE-10 - Inventario de Equipos RE-723 - Listado de Activos 75 - Sistema de Baterías (DOMINION) 76 - Grupo Electrógeno (DOMINION)
A.11. Seguridad física y del entorno	**A.11.2. Seguridad de los equipos**	A.11.2.3. Seguridad del cableado. El cableado eléctrico y de telecomunicaciones que transmite datos o que sirve de soporte a los servicios de información debe estar protegido frente a interceptaciones, interferencias o daños.	Sí	SMARTME desarrolla su actividad en el Edificio Ática de Pozuelo de Alarcón, que cuenta con suelo sobreelevado y techo técnico para las canalizaciones de suministros eléctricos, de comunicaciones, de aire y de PCI. La organización ha establecido su localización basándose en el análisis de riesgos de los activos de la información.	Responsable del Sistema	RE-10 - Inventario de Equipos RE-727 - Tabla de riesgos 83 - Techo técnico 82 - Pavimento sobre elevado
A.11. Seguridad física y del entorno	**A.11.2. Seguridad de los equipos**	A.11.2.4. Mantenimiento de los equipos. Los equipos deben recibir un mantenimiento correcto que asegure su disponibilidad y su integridad continuas.	Sí	Los equipos que son susceptibles de mantenimiento para la Organización son los servidores que alojan aplicaciones y bases de datos, como son AMAZON y el CPD de DOMINION, ambos casos externalizados. El mantenimiento de otros dispositivos de hardware o smartphones no se realiza, directamente se destruyen los antiguos y se sustituyen por nuevos equipos. En el caso de realizarse algún tipo de mantenimiento, se registraría como mantenimiento preventivo o correctivo cuando es necesario, según el procedimiento establecido es su ficha de proceso para las Infraestructuras.	Responsable del Sistema	FP-03 - Infraestructuras RE-11 - Control de Mantenimiento Preventivo RE-12 - Operaciones de mantenimiento correctivo
A.11. Seguridad física y del entorno	**A.11.2. Seguridad de los equipos**	A.11.2.4. Retirada de materiales propiedad de la empresa. Sin autorización previa, los equipos, la información o el software no deben sacarse de las instalaciones.	Sí	La Organización cuenta con ordenadores portátiles y smartphones susceptibles de salir físicamente de sus instalaciones. La Organización ha desarrollado y comunicado a sus empleados y colaboradores las condiciones de salida de equipos e información de sus instalaciones incluidas en el protocolo para la Seguridad de la Información.	Responsable del Sistema	IT-70-01 - Protocolo de Seguridad de la Información IT-70-02 - Protocolo de Seguridad de la Información para colaboradores
A.11. Seguridad física y del entorno	**A.11.2. Seguridad de los equipos**	A.11.2.6. Seguridad de los equipos fuera de las instalaciones. Deben aplicarse medidas de seguridad a los equipos situados fuera de las instalaciones de la organización, teniendo en cuenta los diferentes	Sí	Para el caso en que ordenadores portátiles y smartphones salgan de las instalaciones de la Organización y basadas en un análisis de riesgos de sus activos de información, la Organización cuenta con medidas de seguridad identificadas en el Inventario	Responsable del Sistema	RE-10 - Inventario de Equipos RE-727 - Tabla de riesgos IT-70-01 - Protocolo de Seguridad de la Información IT-70-02 - Protocolo de Seguridad de la Información para colaboradores 64 - Acceso a ordenador personal

		riesgos que conlleva trabajar fuera de dichas instalaciones.		de Equipos y un protocolo de Seguridad de la Información comunicado a sus empleados y colaboradores.		33 - Accesos a la red VPN (DOMINION) 69 - Cuentas de usuario de Microsoft
A.11. Seguridad física y del entorno	**A.11.2. Seguridad de los equipos**	A.11.2.7. Reutilización o eliminación segura de equipos. Todos los soportes de almacenamiento deben ser comprobados para confirmar que todo dato sensible y software bajo licencia se ha eliminado de manera segura antes de deshacerse de ellos.	Sí	La retirada de los equipos obsoletos se realiza por el Responsable del Sistema, quien deja constancia de la comprobación de la eliminación de toda la información sensible en el Listado de Activos y en el Inventario de Equipos. Los equipos son formateados en el momento en que dejan de ser operativos.	Responsable del Sistema	RE-723 - Listado de Activos RE-10 - Inventario de Equipos
A.11. Seguridad física y del entorno	**A.11.2. Seguridad de los equipos**	A.11.2.8. Equipo de usuario desatendido. Los usuarios deben asegurarse que el equipo desatendido tiene la protección adecuada.	Sí	Para aquellos momentos en que los usuarios no ocupan sus puestos de trabajo con el ordenador o el smartphone, la Organización establece mediante sus protocolos de Seguridad de la Información la protección de los equipos desatendidos. Esta protección se basa en la suspensión de las sesiones de usuario tanto en los dispositivos, ordenador o smartphone, como en las aplicaciones de software, obligando al usuario a introducir las credenciales de acceso de nuevo al reanudar sus tareas. También realiza y registra acciones formativas para sus empleados en este sentido.	Responsable del Sistema	IT-70-01 - Protocolo de Seguridad de la Información RE-07 - Plan de Formación 85 - Cierre de sesión en aplicaciones web 84 - Suspensión de sesión de ordenador
A.11. Seguridad física y del entorno	**A.11.2. Seguridad de los equipos**	A.11.2.9. Política de puesto de trabajo despejado y pantalla limpia. Debe adoptarse una política de puesto de trabajo despejado de papeles y medios de almacenamiento desmontables y una política de pantalla limpia para los recursos de tratamiento de la información.	Sí	Es imprescindible para garantizar la seguridad de la información que todos los soportes de información estén custodiados bajo control del propietario del mismo, por ello son básicos el orden y limpieza de los puestos de trabajo. La Organización establece mediante sus protocolos de Seguridad de la Información la política de puesto de trabajo despejado y pantalla limpia. También realiza y registra acciones formativas para sus empleados en este sentido.	Responsable del Sistema	IT-70-01 - Protocolo de Seguridad de la Información RE-07 - Plan de Formación
A.12. Seguridad de las operaciones	**A.12.1. Procedimientos y responsabilidades operacionales**	A.12.1.1. Documentación de procedimientos operacionales. Deben documentarse y mantenerse procedimientos operacionales y ponerse a disposición de todos los usuarios que los necesiten.	Sí	Documentar los procedimientos operacionales es una labor fundamental en todo sistema de gestión. La Organización tiene implantado un sistema integrado de gestión según las normas ISO27001 para la Seguridad de la Información e ISO20252 para la Investigación de Mercados, que es su actividad principal. Cuenta con fichas de proceso que sistematizan todas las tareas operacionales. Las fichas de proceso y las relaciones entre sí quedan establecidas en el mapa de Interacción de Procesos y en el listado de documentación del sistema y en el Organigrama corporativo se establecen los responsables de estos procesos.	Dirección	IP - Interacción de Procesos OR - Organigrama RE-01 - Listado de Documentos del Sistema
A.12. Seguridad de las operaciones	**A.12.1. Procedimientos y responsabilidades operacionales**	A.12.1.2. Gestión de cambios. Los cambios en la organización, los procesos de negocio, instalaciones de tratamiento de la información y los sistemas de que afectan a la seguridad de la información deben ser controlados.	Sí	En SMARTME se planifican los cambios necesarios para el mantenimiento y la mejora del sistema. La Organización cuenta con una ficha de proceso que documenta el procedimiento para la gestión de los cambios identificada en el sistema como Mejora y Cambio. Estos cambios se registran y controlan desde el registro de informes de mejora.	Responsable del Sistema	FP-16 - Mejora y Cambio RE-34 - Informe de Mejora
A.12. Seguridad de las operaciones	**A.12.1. Procedimientos y responsabilidades operacionales**	A.12.1.3. Gestión de capacidades. Se debe supervisar y ajustar la utilización de los recursos, así como realizar proyecciones de los requisitos futuros de capacidad, para garantizar el rendimiento requerido del sistema.	Sí	Con el objetivo de garantizar la prestación de sus servicios la organización gestiona la capacidad de sus activos, según la sistemática establecida en su ficha de proceso para la Seguridad de la Información. La organización registra la planificación de la capacidad para facilitar su control y seguimiento.	Dirección Responsable del Sistema	FP-70 - Seguridad de la Información RE-713 - Capacidad de los Activos
A.12. Seguridad de las operaciones	**A.12.1. Procedimientos y responsabilidades operacionales**	A.12.1.4. Separación de los recursos de desarrollo, prueba y operación. Deben separarse los recursos de desarrollo, pruebas y operación, para reducir los riesgos de acceso no autorizado o los cambios del sistema en producción.	Sí	SMARTME cuenta con entornos independientes de desarrollo, consolidación y producción para el despliegue de sus sistemas. Estos entornos figuran en el Inventario de Equipos para su gestión según la sistemática establecida en la ficha de proceso para las Infraestructuras. Las medidas de seguridad asociadas a cada activo se evidencian en el diagrama de configuración.	Responsable del Sistema	FP-03 - Infraestructuras RE-10 - Inventario de Equipos RE-701 - Diagrama de Configuración 86 - Entorno de desarrollo y pruebas
A.12. Seguridad de las operaciones	**A.12.2. Protección contra el software malicioso (malware)**	A.12.2.1. Controles contra el código malicioso. Se deben implementar los controles de detección, prevención y recuperación que sirvan como protección contra el código malicioso, así como procedimientos adecuados de concienciación al usuario.	Sí	La Organización ha implantado un sistema de corta fuegos y anti virus que mantiene actualizado, registrado en el Inventario de Equipos. En caso de incidencia de seguridad grave, aplicará el plan de contingencia y restaurará las copias de seguridad si es necesario. Al mismo tiempo, planifica y realiza acciones formativas de concienciación evidenciadas en el Plan de Formación.	Responsable del Sistema	RE-10 - Inventario de Equipos RE-07 - Plan de Formación RE-703 - Plan de Continuidad 88 - Firewall NGFW 87 - Trend Micro Antivirus 71 - Copia de seguridad servidor CPD
A.12. Seguridad de las operaciones	**A.12.3. Copias de seguridad**	A.12.3.1. Copias de seguridad de la información. Se deben realizar copias de seguridad de la información, del	Sí	Las copias de seguridad se incluyen en el inventario de activos del sistema y se planifica su verificación con la	Tecnología, Procesos, Herramientas	RE-10 - Inventario de Equipos RE-11 - Control de Mantenimiento

		software y del sistema y se deben verificar periódicamente de acuerdo a la política de copias de seguridad acordada.		frecuencia establecida en el registro de mantenimiento preventivo de los activos. Se realizan copias de seguridad de los sistemas alojados en el CDP. Las copias de seguridad del resto de sistemas son automáticas en los diferentes entornos cloud.		Preventivo 71 - Copia de seguridad servidor CPD
A.12. Seguridad de las operaciones	**A.12.4. Registros y supervisión**	A.12.4.1. Registro de eventos. Se deben registrar, proteger y revisar periódicamente las actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información.	Sí	Las excepciones y fallos de seguridad de la información se recogen y tratan como incidencias relacionadas con el proceso de Seguridad de la Información.	Responsable del Sistema	RE-716 - Incidencias
A.12. Seguridad de las operaciones	**A.12.4. Registros y supervisión**	A.12.4.2. Protección de la información del registro. Los dispositivos de registro y la información del registro deben estar protegidos contra manipulaciones indebidas y accesos no autorizados.	Sí	Se registra información a través de las aplicaciones de gestión, de operación y de soporte al sistema, que queda guardada en las respectivas bases de datos. Todos los sistemas cuentan con gestión de accesos registrados en el Inventario de Equipos.	Responsable del Sistema	RE-10 - Inventario de Equipos 22 - Acceso a CPD 70 - Acceso ETHERNET a LAN 64 - Acceso a ordenador personal 27 - Acceso a SMARTME APP integrado en la aplicación 28 - Acceso a SMARTME DASHBOARDS integrado en la herramienta de usuario 78 - Acceso de administrador del sistema 65 - Acceso único SMARTME APP - BBDD Transaccional (AMAZON) 24 - Accesos a base de datos Data Warehouse 23 - Accesos a base de datos Transaccional (AMAZON) 67 - Accesos a BITRIX 25 - Accesos a GestNear (DOMINION) 33 - Accesos a la red VPN (DOMINION) 31 - Accesos a la red WI-FI (DOMINION) 26 - Accesos a Microsoft Dynamics CRM 68 - Accesos a TQNET 66 - Accesos a TRELLO
A.12. Seguridad de las operaciones	**A.12.4. Registros y supervisión**	A.12.4.3. Registros de administración y operación. Se deben registrar, proteger y revisar regularmente las actividades del administrador del sistema y del operador del sistema.	Sí	Toda la documentación relevante que maneja la Organización se encuentra inventariada y controlada en el Listado de Documentos del Sistema, incluidos los registros operacionales. Las tareas operacionales realizadas por todo el equipo, incluido el administrador, se registran como Planificación de Tareas en la herramienta de gestión corporativa, mientras que las tareas propias del sistema de gestión se registran en la plataforma que contiene el Sistema de Gestión.	Responsable del Sistema	RE-01 - Listado de Documentos del Sistema RE-106 - Planificación de Tareas RE-736 - Listado de Tareas Planificadas
A.12. Seguridad de las operaciones	**A.12.4. Registros y supervisión**	A.12.4.4. Sincronización del reloj. Los relojes de todos los sistemas de tratamiento de la información dentro de una organización o de un dominio de seguridad, deben estar sincronizados con una única fuente de tiempo precisa y acordada.	Sí	La hora oficial de SMARTME ANALYTICS y de todos sus sistemas es la establecida para España por el servidor NTP de Microsoft (time.windows.com). Todos los equipos que funcionan dentro de España, se sincronizan con este servicio. Para los datos con un origen internacional, como desarrollos o de la SMARTME APP, la organización cuenta con un algoritmo de conversión que aplica en sus procesos ETL identificados en el diagrama de configuración y en el inventario de equipos (activos de la información).	Tecnología, Procesos, Herramientas	RE-701 - Diagrama de Configuración RE-10 - Inventario de Equipos 89 - Algoritmo de conversión horaria
A.12. Seguridad de las operaciones	**A.12.5. Control del software en explotación**	A.12.5.1. Instalación del software en explotación. Se deben implementar procedimientos para controlar la instalación del software en explotación.	Sí	La Organización utiliza la Apple y la Play Stores para la distribución e instalación de la SMARTME APP de los usuarios panelistas y ha desarrollado los procedimientos necesarios plasmados en la ficha de proceso de Diseño y Desarrollo y en la ficha de subproceso para el desarrollo tecnológico para asegurar su éxito. Por otro lado, ha desarrollado otro procedimiento documentado con la ficha de proceso para el Delivery de los DASHBOARDS entregados a los clientes.	Tecnología, Procesos, Herramientas	FP-09 - Delivery FP-11 - Diseño y Desarrollo FP-11-01 - Desarrollo tecnológico 86 - Entorno de desarrollo y pruebas
A.12. Seguridad de las operaciones	**A.12.6. Gestión de la vulnerabilidad técnica**	A.12.6.1. Gestión de las vulnerabilidades técnicas. Se debe obtener información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información utilizados, evaluar la exposición de la organización a dichas vulnerabilidades y adoptar las medidas adecuadas para afrontar el riesgo asociado.	Sí	La Organización realiza un análisis de riesgos continuo relacionados con sus activos de información y basados en una matriz de impactos que tiene en cuenta las vulnerabilidades del sistema.	Responsable del Sistema	RE-726 - Matriz de impactos RE-727 - Tabla de riesgos
A.12. Seguridad de las operaciones	**A.12.6. Gestión de la vulnerabilidad técnica**	A.12.6.2. Restricción en la instalación de software. Se deben establecer y aplicar reglas que rijan la instalación de software por parte de los usuarios.	Sí	Los usuarios no pueden instalar software en ningún equipo propiedad de SMARTME ANALYTICS, sólo el usuario Administrador puede realizar instalaciones. La seguridad se aplica a todos los activos de la información inventariados, tal y como se establece en la ficha de proceso para la Seguridad de la Información.	Responsable del Sistema	RE-10 - Inventario de Equipos IT-70-01 - Protocolo de Seguridad de la Información 78 - Acceso de administrador del sistema
A.12. Seguridad de las operaciones	**A.12.7. Consideraciones sobre la auditoría de sistemas de información**	A.12.7.1. Controles de auditoría de sistemas de información. Los requisitos y las actividades de auditoría que impliquen comprobaciones en los sistemas operativos deben ser cuidadosamente planificados y acordados para minimizar el riesgo de	Sí	La organización realiza auditorías del sistema programadas. Ha desarrollado para ello un procedimiento para la realización de auditorías de los sistemas documentado como la ficha de proceso de auditorías.	Responsable del Sistema	FP-14 - Auditorías

		interrupciones en los procesos de negocio.				
A.13. Seguridad de las comunicaciones	**A.13.1. Gestión de la seguridad de las redes**	A.13.1.1. Controles de red. Las redes deben ser gestionadas y controladas para proteger la información en los sistemas y aplicaciones.	Sí	La organización desarrolla su actividad en las instalaciones del grupo DOMINION al que pertenece y la administración de la intranet depende de ellos. En cuanto a las aplicaciones cloud, SMARTME mantiene contratos con los proveedores a los que subcontrata la gestión de redes en los que se evidencian las medidas de seguridad de la información aplicadas.	Dirección	RE-17 - Contrato con Proveedor
A.13. Seguridad de las comunicaciones	**A.13.1. Gestión de la seguridad de las redes**	A.13.1.2. Seguridad de los servicios de red. Se deben identificar los mecanismos de seguridad, los niveles de servicio, y los requisitos de gestión de todos los servicios de red y se deben incluir en cualquier acuerdo de servicios de red, tanto si estos servicios se prestan dentro de la organización como si se subcontratan.	Sí	SMARTME identifica los mecanismos de seguridad implantados en su diagrama de la configuración. También mantiene contratos con los proveedores a los que subcontrata la gestión de redes en los que se evidencian las medidas de seguridad de la información aplicadas y se establecen los niveles de servicio (SLA). En el caso especial de la intranet de DOMINION, la medida de control utilizada para los accesos a la red es el firewall.	Dirección Responsable del Sistema	RE-17 - Contrato con Proveedor RE-701 - Diagrama de Configuración 88 - Firewall NGFW
A.13. Seguridad de las comunicaciones	**A.13.1. Gestión de la seguridad de las redes**	A.13.1.3. Segregación en redes. Los grupos de servicios de información, los usuarios y los sistemas de información deben estar segregados en redes distintas.	Sí	SMARTME mantiene 3 entornos independientes: desarrollo, consolidacion y producción. El primero se divide a su vez en el interno en el que trabaja el equipo de Data Scientists y Data Analysts, y en el externo en el que trabajan los colaboradores de desarrollo. Al entorno de consolidación tiene acceso el equipo de Testing y el de producción se divide en la SMARTME APP y la SMARTME DASHBOARDS. Todos los entornos quedan reflejados en el Diagrama de la Configuración.	Responsable del Sistema	RE-701 - Diagrama de Configuración 86 - Entorno de desarrollo y pruebas
A.13. Seguridad de las comunicaciones	**A.13.2. Intercambio de información**	A.13.2.1. Políticas y procedimientos de intercambio de información. Deben establecerse políticas, procedimientos y controles formales que protejan el intercambio de información mediante el uso de todo tipo de recursos de comunicación.	Sí	Todo el intercambio de información permitido en SMARTME es a través de correo electrónico con clientes y proveedores, TABLEAU DASHBOARDS para clientes y la SMARTME APP para usuarios panelistas. La Organización ha desarrollado y comunicado un protocolo de Seguridad de la Información en el que se hace referencia a los procedimientos de intercambio de la información para sus empleados y colaboradores.	Responsable del Sistema	IT-70-02 - Protocolo de Seguridad de la Información para colaboradores IT-70-01 - Protocolo de Seguridad de la Información
A.13. Seguridad de las comunicaciones	**A.13.2. Intercambio de información**	A.13.2.2. Acuerdos de intercambio de información. Deben establecerse acuerdos para el intercambio seguro de información del negocio y software entre la organización y terceros.	Sí	Todo el intercambio de información permitido en SMARTME es a través de correo electrónico con clientes y proveedores, TABLEAU DASHBOARDS para clientes y la SMARTME APP para usuarios panelistas. SMARTME establece canales por defecto en su protocolo de seguridad de la información para colaboradores o acuerdos específicos en los contratos con terceros.	Dirección	IT-70-02 - Protocolo de Seguridad de la Información para colaboradores RE-17 - Contrato con Proveedor
A.13. Seguridad de las comunicaciones	**A.13.2. Intercambio de información**	A.13.2.3. Mensajería electrónica. La información que sea objeto de mensajería electrónica debe estar adecuadamente protegida.	Sí	La Organización cuenta con un protocolo para la Seguridad de la Información en el que se establecen las medidas de protección para la mensajería electrónica, que ha comunicado a sus empleados y colaboradores. En el protocolo se establece la política de uso del correo y en especial para el intercambio de información clasificada como CONFIDENCIAL, que debe comunicarse utilizando contraseña, la cual debe ser comunicada por otro canal diferente.	Responsable del Sistema	IT-70-02 - Protocolo de Seguridad de la Información para colaboradores IT-70-01 - Protocolo de Seguridad de la Información 90 - Contraseña de seguridad para información CONFIDENCIAL
A.13. Seguridad de las comunicaciones	**A.13.2. Intercambio de información**	A.13.2.4. Acuerdos de confidencialidad o no revelación. Deben identificarse, documentarse y revisarse regularmente los requisitos de los acuerdos de confidencialidad o no revelación.	Sí	La Organización cuenta con empleados y colaboradores externos con los que comparte información por las necesidades del negocio. La Organización ha desarrollado sendas fichas de proceso para la gestión de los Recursos Humanos y los Externos en las que se establece la sistemática de documentación y revisión de los contratos laborales y de colaboración en los que se firman cláusulas de confidencialidad.	Responsable del Sistema	FP-04 - Recursos Externos RE-17 - Contrato con Proveedor FP-02 - Recursos Humanos RE-17 - Contrato con Proveedor
A.14. Adquisición, desarrollo y mantenimiento de los sistemas de información	**A.14.1. Requisitos de seguridad en los sistemas de información**	A.14.1.1. Análisis de requisitos y especificaciones de seguridad de la información. Los requisitos relacionados con la seguridad de la información deben incluirse en los requisitos para los nuevos sistemas de información o mejoras a los sistemas de información existentes.	Sí	Los requisitos de la seguridad de la información de los nuevos activos o cuando se aplican mejoras a los existentes, se tienen en cuenta tal y como se establece en las fichas de proceso para las Infraestructuras y para la Mejora y el Cambio respectivamente. Los nuevos sistemas de información son considerados activos de la información y, como tal, tratados en el análisis de riesgos de la seguridad de la información, según se describe en la ficha de proceso para la Seguridad de la Información.	Responsable del Sistema	FP-70 - Seguridad de la Información FP-03 - Infraestructuras FP-16 - Mejora y Cambio
A.14. Adquisición, desarrollo y mantenimiento de	**A.14.1. Requisitos de seguridad en los**	A.14.1.2. Asegurar los servicios de aplicaciones en redes públicas. La información involucrada en	Sí	La organización utiliza diferentes aplicaciones en modo cloud para sus tareas de gestión, de soporte al	Responsable del Sistema	RE-10 - Inventario de Equipos

los sistemas de información	**sistemas de información**	aplicaciones que pasan a través de redes públicas debe ser protegida de cualquier actividad fraudulenta, disputa de contrato, revelación y modificación no autorizadas.		sistema, incluso para la operación. Todas estas aplicaciones deben utilizar un protocolo seguro de transferencia HTTPS para sus comunicaciones y están listadas en inventario de equipos dentro de la familia SOFTWARE.		
A.14. Adquisición, desarrollo y mantenimiento de los sistemas de información	**A.14.1. Requisitos de seguridad en los sistemas de información**	A.14.1.3. Protección de las transacciones de servicios de aplicaciones. La información involucrada en las transacciones de servicios de aplicaciones debe ser protegida para prevenir la transmisión incompleta, errores de enrutamiento, alteración no autorizada del mensaje, revelación, duplicación o reproducción de mensaje no autorizadas.	Sí	El requisito aplica a los desarrollos propios de la Organización, en concreto a la transmisión de datos entre la SMARTME APP y la base de datos Transaccional y a los procesos ETL que dan lugar a los ficheros CSV origen de los DASHBOARDS. La Organización cuenta con una instrucción técnica comunicada a los equipos de desarrollo interno y externo que describe la metodología para un desarrollo seguro.	Responsable del Sistema	IT-11-01 - Buenas Prácticas de Desarrollo Seguro
A.14. Adquisición, desarrollo y mantenimiento de los sistemas de información	**A.14.2. Seguridad en el desarrollo y en los procesos de soporte**	A.14.2.1. Política de desarrollo seguro. Se deben establecer y aplicar reglas dentro de la organización para el desarrollo de aplicaciones y sistemas.	Sí	El requisito aplica a los desarrollos externos de la SMARTME APP y a los scripts de los procesos ETL de los data scientists. La Organización cuenta con una instrucción técnica comunicada a los equipos de desarrollo interno y externo que describe la metodología para un desarrollo seguro.	Responsable del Sistema	IT-11-01 - Buenas Prácticas de Desarrollo Seguro IT-09-01 - Delivery
A.14. Adquisición, desarrollo y mantenimiento de los sistemas de información	**A.14.2. Seguridad en el desarrollo y en los procesos de soporte**	A.14.2.2. Procedimiento de control de cambios en sistemas. La implantación de cambios a lo largo del ciclo de vida del desarrollo debe controlarse mediante el uso de procedimientos formales de control de cambios.	Sí	El requisito aplica por un lado al desarrollo externalizado de la SMARTME APP, para lo cual la Organización cuenta con una ficha de proceso para el Desarrollo de nuevos servicios y otra ficha de subproceso para el Desarrollo Tecnológico de mejoras en los sistemas en el que se establece el uso de entornos de desarrollo y pruebas y la subida a producción desde las APPLE y PLAY stores. Por otro lado, a cualquier cambio o mejora realizado en el sistema, para lo cual la organización cuenta con una ficha de proceso que establece la sistemática que se debe seguir en este caso.	Responsable del Sistema	FP-11-01 - Desarrollo tecnológico FP-11 - Diseño y Desarrollo 86 - Entorno de desarrollo y pruebas
A.14. Adquisición, desarrollo y mantenimiento de los sistemas de información	**A.14.2. Seguridad en el desarrollo y en los procesos de soporte**	A.14.2.3. Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo. Cuando se modifiquen los sistemas operativos, las aplicaciones de negocio críticas deben ser revisadas y probadas para garantizar que no existen efectos adversos en las operaciones o la seguridad de la organización.	Sí	La Organización realiza los cambios en los sistemas operativos en un entorno de preproducción previo al cambio del entorno de producción, tal y como se describe en la ficha de proceso de Diseño y Desarrollo. Si alguna actualización automática provocara algún fallo en el sistema, se procederá según lo descrito en la contingencia correspondiente del plan de continuidad.	Responsable del Sistema	FP-11-01 - Desarrollo tecnológico RE-703 - Plan de Continuidad FP-11 - Diseño y Desarrollo
A.14. Adquisición, desarrollo y mantenimiento de los sistemas de información	**A.14.2. Seguridad en el desarrollo y en los procesos de soporte**	A.14.2.4. Restricciones a los cambios en los paquetes de software. Se deben desaconsejar las modificaciones en los paquetes de software, limitándose a los cambios necesarios, y todos los cambios deben ser objeto de un control riguroso.	Sí	El requisito no afecta al software de los ordenadores personales, ya que las instalaciones son exclusividad del administrador del sistema. En cuanto a los servidores internos, la administración corresponde a DOMINION. El requisito aplica sobre todo a las modificaciones en la SMARTME APP desarrollada por INITIUM y que está controlado directamente por el Responsable del Sistema. Las modificaciones son planificadas y pasan previamente por el entorno de Pruebas.	Responsable del Sistema	FP-11-01 - Desarrollo tecnológico 86 - Entorno de desarrollo y pruebas
A.14. Adquisición, desarrollo y mantenimiento de los sistemas de información	**A.14.2. Seguridad en el desarrollo y en los procesos de soporte**	A.14.2.5. Principios de ingeniería de sistemas seguros. Principios de ingeniería de sistemas seguros se debe establecer, documentar, mantener y aplicarse a todos los esfuerzos de implementación de sistemas de información.	Sí	Los principio de ingeniería de sistemas seguros aplican al desarrollo de la SMARTME APP externalizado con INITIUM y a los scripts desarrollados por los data scientists y analysts para los procesos de extracción (ETL). La Organización cuenta con instrucciones técnicas comunicadas a los equipos de desarrollo interno y externo que describe la metodología para un desarrollo seguro y de buenas prácticas de desarrollo.	Responsable del Sistema	IT-11-01 - Buenas Prácticas de Desarrollo Seguro IT-09-01 - Delivery
A.14. Adquisición, desarrollo y mantenimiento de los sistemas de información	**A.14.2. Seguridad en el desarrollo y en los procesos de soporte**	A.14.2.6. Entorno de desarrollo seguro. Las organizaciones deben establecer y proteger adecuadamente los entornos de desarrollo seguro para el desarrollo del sistema y los esfuerzos de integración que cubren todo el ciclo de vida de desarrollo del sistema.	Sí	Los entornos de desarrollo seguros aplican al desarrollo de la SMARTME APP externalizado con INITIUM y al desarrollo de los procesos de extracción por parte de los analistas y científicos de datos. Los accesos a estos entornos se listan en el inventario de equipos. La Organización cuenta con una instrucción técnica comunicada a los equipos de desarrollo interno y externo que describe la metodología para un desarrollo seguro.	Responsable del Sistema	IT-11-01 - Buenas Prácticas de Desarrollo Seguro RE-10 - Inventario de Equipos 23 - Accesos a base de datos Transaccional (AMAZON) 86 - Entorno de desarrollo y pruebas
A.14. Adquisición, desarrollo y mantenimiento de los sistemas de información	**A.14.2. Seguridad en el desarrollo y en los procesos de soporte**	A.14.2.7. Externalización del desarrollo de software. El desarrollo de software externalizado debe ser supervisado y controlado por la organización.	Sí	La Organización mantiene externalizado el desarrollo de la SMARTME APP. El desarrollo lo supervisa directamente el Responsable del Sistema, que se encarga de realizar las pruebas oportunas antes de subir a producción los cambios. La Organización controla y supervisa el desarrollo externalizado, tal y como se describe en su ficha de proceso de Diseño y Desarrollo. El Protocolo de Desarrollo Seguro también se le ha	Responsable del Sistema	FP-11-01 - Desarrollo tecnológico IT-11-01 - Buenas Prácticas de Desarrollo Seguro 86 - Entorno de desarrollo y pruebas

				hecho llegar al equipo de desarrollo del proveedor.		
A.14. Adquisición, desarrollo y mantenimiento de los sistemas de información	**A.14.2. Seguridad en el desarrollo y en los procesos de soporte**	A.14.2.8. Pruebas funcionales de seguridad de sistemas. Se deben llevar a cabo pruebas de la seguridad funcional durante el desarrollo.	Sí	El requisito aplica tanto al desarrollo externo de la SMARTME APP por parte de INITIUM, como al desarrollo interno de procesos de extracción por parte de analistas y científicos de datos. La Organización prueba funcionalmente la seguridad de los nuevos desarrollos, tal y como se establece en sus fichas de proceso de Diseño y Desarrollo.	Responsable del Sistema	FP-11 - Diseño y Desarrollo FP-11-01 - Desarrollo tecnológico 86 - Entorno de desarrollo y pruebas
A.14. Adquisición, desarrollo y mantenimiento de los sistemas de información	**A.14.2. Seguridad en el desarrollo y en los procesos de soporte**	A.14.2.9. Pruebas de aceptación de sistemas. Se deben establecer programas de pruebas de aceptación y criterios relacionados para nuevos sistemas de información, actualizaciones y nuevas versiones.	Sí	El requisito aplica tanto al desarrollo externo de la SMARTME APP por parte de INITIUM, como al desarrollo interno de procesos de extracción por parte de analistas y científicos de datos. La Organización cuenta con una ficha de proceso de Diseño y Desarrollo que establece la sistemática de las pruebas de aceptación y verificación de los nuevos desarrollo.	Responsable del Sistema	FP-11 - Diseño y Desarrollo FP-11-01 - Desarrollo tecnológico 86 - Entorno de desarrollo y pruebas
A.14. Adquisición, desarrollo y mantenimiento de los sistemas de información	**A.14.3. Datos de prueba**	A.14.3.1. Protección de los datos de prueba. Los datos de prueba se deben seleccionar con cuidado y deben ser protegidos y controlados.	Sí	El requisito aplica tanto al desarrollo externo de la SMARTME APP por parte de INITIUM, como al desarrollo interno de procesos de extracción por parte de analistas y científicos de datos. La Organización cuenta con una instrucción técnica comunicada a los equipos de desarrollo interno y externo que describe la metodología para un desarrollo seguro, que tiene en cuenta el control de los datos de prueba.	Responsable del Sistema	IT-11-01 - Buenas Prácticas de Desarrollo Seguro
A.15. Relación con proveedores	**A.15.1. Seguridad en las relaciones con proveedores**	A.15.1.1. Política de seguridad de la información en las relaciones con los proveedores. Los requisitos de seguridad de la información para la mitigación de los riesgos asociados con el acceso del proveedor a los activos de la organización deben acordarse con el proveedor y quedar documentados.	Sí	El requisito aplica a todos los proveedores identificados en el listado de proveedores homologados. La Organización firma contratos y acuerdos de colaboración con proveedores que incluyen requisitos de seguridad. Cuando procede, se les hace entrega del Protocolo de Seguridad de la Información para colabores solicitándoles su firma.	Responsable del Sistema	IT-70-02 - Protocolo de Seguridad de la Información para colaboradores RE-17 - Contrato con Proveedor RE-13 - Listado de Proveedores Homologados
A.15. Relación con proveedores	**A.15.1. Seguridad en las relaciones con proveedores**	A.15.1.2. Requisitos de seguridad en contratos con terceros. Todo los requisitos relacionados con la seguridad de la información deben establecerse y acordarse con cada proveedor que puede acceder, tratar. almacenar, comunicar o proporcionar componentes de la infraestructura de Tecnología de la Información.	Sí	En este caso, el requisito aplica a DOMINION y a AMAZON, como provedores de infraestructura. La Organización firma contratos y acuerdos de colaboración con proveedores que incluyen requisitos de seguridad y requiere la firma del protocolo de seguridad de la información a todos los colaboradores.	Responsable del Sistema	RE-17 - Contrato con Proveedor IT-70-02 - Protocolo de Seguridad de la Información para colaboradores
A.15. Relación con proveedores	**A.15.1. Seguridad en las relaciones con proveedores**	A.15.1.3. Cadena de suministro de tecnología de la información y de las comunicaciones. Los acuerdos con proveedores deben incluir requisitos para hacer frente a los riesgos de seguridad de la información relacionados con las tecnologías de la información y las comunicaciones y con la cadena de suministro de productos.	Sí	El requisito aplica exclusivamente a DOMINION como suministrador de tecnología de la información y de las comunicaciones. La organización cuenta con un protocolo estándar para garantizar la seguridad de la información con sus colaboradores y firma acuerdos de colaboración en los que evidencia otros requisitos de seguridad cuando procede.	Dirección	IT-70-02 - Protocolo de Seguridad de la Información para colaboradores RE-17 - Contrato con Proveedor
A.15. Relación con proveedores	**A.15.2. Gestión de la provisión de servicios del proveedor**	A.15.2.1. Control y revisión de la provisión de servicios del proveedor. Las organizaciones deben controlar, revisar y auditar regularmente la provisión de servicios del proveedor.	Sí	Aplica a todos los proveedores que aparecen en el listado de proveedores homologados. La organización cuenta con un procedimiento de auditorías en el que se incluyen los servicios del proveedor documentado mediante una ficha de proceso y evidenciado en los informes de auditoría.	Responsable del Sistema	RE-31 - Informe de Auditoría RE-13 - Listado de Proveedores Homologados FP-14 - Auditorías
A.15. Relación con proveedores	**A.15.2. Gestión de la provisión de servicios del proveedor**	A.15.2.2. Gestión de cambios en la provisión del servicio del proveedor. Se deben gestionar los cambios en la provisión del servicio, incluyendo el mantenimiento y la mejora de las políticas, los procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de los procesos y sistemas de negocio afectados así como la reapreciación de los riesgos.	Sí	Aplica a los cambios en el servicio proporcionado por cualquiera de los proveedores. La organización cuenta con metodología para gestión de los cambios descrita en la ficha de proceso para la Mejora y el Cambio. Estos cambios se registrarán y controlarán mediante los informes de mejora.	Responsable del Sistema	FP-16 - Mejora y Cambio RE-34 - Informe de Mejora
A.16. Gestión de incidentes de seguridad de la información	**A.16.1. Gestión de incidentes de seguridad de la información y mejoras**	A.16.1.1. Responsabilidades y procedimientos. Se deben establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, efectiva y adecuada a los incidentes de seguridad de la información.	Sí	La organización cuenta con un procedimiento de Seguridad de la Información en el que se establece la sistemática de gestión del registro de incidencias de Seguridad de la Información. En dicho procedimiento se establecen las responsabilidades de cada componente del equipo a la hora de gestionar una incidencia de seguridad de la información. En el Protocolo de Seguridad de la Información comunicado a los empleados y en Plan de Continuidad se hace referencia al registro de las incidencias cuando procede.	Responsable del Sistema	FP-70 - Seguridad de la Información RE-716 - Incidencias IT-70-01 - Protocolo de Seguridad de la Información RE-703 - Plan de Continuidad
A.16. Gestión de incidentes de seguridad de la información	**A.16.1. Gestión de incidentes de seguridad de la información y mejoras**	A.16.1.2. Notificación de los eventos de seguridad de la información. Los eventos de seguridad de la información se deben notificar por los canales de gestión adecuados lo antes posible.	Sí	Aplica a todos los empleados y a los colaboradores. La Organización cuenta con un cuadro de comunicación en el que se registran todos los mensajes intercambiados en el ámbito del sistema, incluidos los eventos de seguridad, los emisores, los receptores	Responsable del Sistema	RE-29 - Cuadro de Comunicación IT-70-01 - Protocolo de Seguridad de la Información IT-70-02 - Protocolo de Seguridad de la Información para colaboradores

				y los canales adecuados. Este cuadro de comunicación y el Protocolo de Seguridad de la Información se han comunicado al conjunto de empleados y colaboradores para garantizar que todos conocen el procedimiento a seguir con las incidencias de Seguridad de la Información.		
A.16. Gestión de incidentes de seguridad de la información	**A.16.1. Gestión de incidentes de seguridad de la información y mejoras**	A.16.1.3. Notificación de puntos débiles de la seguridad. Todos los empleados, contratistas, terceras partes usuarias de los sistemas y servicios de información deben ser obligados a anotar y notificar cualquier punto débil que observen o que sospechen que exista en los sistemas o servicios.	Sí	El requisito aplica a los empleados y a los colaboradores de SMARTME. La organización comunica esta obligación a empleados y colaboradores en sus respectivos protocolos de Seguridad de la Información.	Responsable del Sistema	IT-70-01 - Protocolo de Seguridad de la Información IT-70-02 - Protocolo de Seguridad de la Información para colaboradores
A.16. Gestión de incidentes de seguridad de la información	**A.16.1. Gestión de incidentes de seguridad de la información y mejoras**	A.16.1.4. Evaluación y decisión sobre los eventos de seguridad de la información. Los eventos de seguridad de la información deben ser evaluados y debe decidirse si se clasifican como incidentes de seguridad de la información.	Sí	Aplica a todas las incidencias de Seguridad de la Información comunicadas por los canales establecidos para ello. La organización ha desarrollado un procedimiento para la evaluación y clasificación de los eventos y las incidencias de Seguridad de la Información. Las incidencias se registran y clasifican en la aplicación de soporte del Sistema de Gestión.	Responsable del Sistema	FP-70 - Seguridad de la Información RE-716 - Incidencias
A.16. Gestión de incidentes de seguridad de la información	**A.16.1. Gestión de incidentes de seguridad de la información y mejoras**	A.16.1.5. Respuesta a incidentes de seguridad de la información. Los incidentes de seguridad de la información deben ser respondidos de acuerdo con los procedimientos documentados.	Sí	El requisito aplica a todas las incidencias de Seguridad de la Información registradas en el sistema. Los incidentes de Seguridad de la Información se responden y quedan evidenciados en el registro de incidencias, según la sistemática establecida en el procedimiento de Seguridad de la Información.	Responsable del Sistema	FP-70 - Seguridad de la Información RE-716 - Incidencias
A.16. Gestión de incidentes de seguridad de la información	**A.16.1. Gestión de incidentes de seguridad de la información y mejoras**	A.16.1.6. Aprendizaje de los incidentes de seguridad de la información. El conocimiento obtenido a partir del análisis y la resolución de incidentes de seguridad de la información debe utilizarse para reducir la probabilidad o el impacto de los incidentes en el futuro.	Sí	El requisito aplica a todas incidencias de Seguridad de la Información notificadas, registradas y resueltas en el sistema. El registro de las incidencias y su resolución conforman una base de datos de conocimiento que la organización aprovecha para reducir los eventos y sus efectos.	Responsable del Sistema	FP-70 - Seguridad de la Información RE-716 - Incidencias
A.16. Gestión de incidentes de seguridad de la información	**A.16.1. Gestión de incidentes de seguridad de la información y mejoras**	A.16.1.7. Recopilación de evidencias. La organización debe definir y aplicar procedimientos para la identificación recogida, adquisición y preservación de la información que puede servir de evidencia.	Sí	Aplica a todas las incidencias de Seguridad de la Información registradas. La organización guarda un registro de evidencias relacionadas con las incidencias de la Seguridad de la Información. Este registro cuenta con la funcionalidad de poder guardar toda la documentación relacionada con las evidencias y asociarla con cada evidencia.	Responsable del Sistema	RE-716 - Incidencias
A.17. Aspectos de seguridad de la información para la gestión de la continuidad de negocio	**A.17.1. Continuidad de la seguridad de la información**	A.17.1.1. Planificación de la continuidad de la seguridad de la información. La organización debe determinar sus necesidades de seguridad de la información y de continuidad para la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	Sí	La determinación de necesidades de seguridad y continuidad aplica a todos los activos de información de la Organización. Por ello, la Organización realiza un análisis de los riesgos asociados y aplicados a todos sus activos, según la valoración de los mismos. Basado en el análisis de riesgos, desarrolla un plan de continuidad del negocio de acuerdo a las posibles contingencias.	Responsable del Sistema	RE-726 - Matriz de impactos RE-727 - Tabla de riesgos RE-703 - Plan de Continuidad RE-723 - Listado de Activos
A.17. Aspectos de seguridad de la información para la gestión de la continuidad de negocio	**A.17.1. Continuidad de la seguridad de la información**	A.17.1.2. Implementar la continuidad de la seguridad de la información. La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel requerido de continuidad de la seguridad de la información durante una situación adversa.	Sí	El requisito aplica a la continuidad de la seguridad de la información de todos los activos de la Organización. La organización cuenta con un plan de continuidad del negocio en el que establece contingencias, desarrollado y revisado con regularidad según lo indicado por la ficha de proceso para la seguridad de la información. La organización cuenta con un plan de continuidad del negocio en el que establece contingencias, desarrollado y revisado con regularidad según lo indicado por la ficha de proceso para la seguridad de la información.	Responsable del Sistema	FP-70 - Seguridad de la Información RE-703 - Plan de Continuidad RE-723 - Listado de Activos
A.17. Aspectos de seguridad de la información para la gestión de la continuidad de negocio	**A.17.1. Continuidad de la seguridad de la información**	A.17.1.3. Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	Sí	La verificación, revisión y evaluación de la continuidad de la seguridad de la información aplica a todo el plan de continuidad, que determina contingencias y establece planes de acción para dichas contingencias. La organización verifica y prueba el plan de continuidad periódicamente, registrando los resultados de dichas pruebas.	Responsable del Sistema	RE-703 - Plan de Continuidad
A.17. Aspectos de seguridad de la información para la gestión de la continuidad de negocio	**A.17.2. Redundancias**	A.17.2.1. Disponibilidad de los recursos de tratamiento de la información. Los recursos de tratamiento de la información deben ser implementados con la redundancia suficiente para satisfacer los requisitos de disponibilidad.	Sí	El requisito de disponibilidad de los recursos de tratamiento de la información aplica a todos los activos de la Organización. La organización gestiona la necesidad de redundancia de sus recursos basándose en el registro de la capacidad de sus activos, en el conocimiento del consumo de estos recursos durante la prestación de sus servicios y en el análisis de la demanda de los mismos, según la sistemática establecida en la ficha de	Dirección Responsable del Sistema	RE-713 - Capacidad de los Activos FP-70 - Seguridad de la Información

				proceso para la Seguridad de la Información.		
A.18. Cumplimiento	**A.18.1. Cumplimiento de los requisitos legales y contractuales**	A.18.1.1. Identificación de la legislación aplicable y de los requisitos contractuales.	Sí	El requisito aplica a toda la normativa aplicable identificada y a los contratos con las partes interesadas. La organización revisa la legislación aplicable y los requisitos contractuales de las partes interesadas con la frecuencia y la metodología establecida en la ficha de proceso para la revisión del sistema y evidencia dicha revisión en el registro de normativa aplicable.	Dirección Responsable del Sistema	FP-20 - Revisión del Sistema RE-21 - Normativa aplicable RE-28 - Acta de Revisión del Sistema
A.18. Cumplimiento	**A.18.1. Cumplimiento de los requisitos legales y contractuales**	A.18.1.2. Derechos de Propiedad Intelectual (DPI). Deben implementarse procedimientos adecuados para garantizar el cumplimiento de los requisitos legales, regulatorios y contractuales sobre el uso de materiales, con respecto a los cuales puedan existir derechos de propiedad intelectual y sobre el uso de productos de software patentados.	Sí	Aplica a las licencias de uso de las diferentes aplicaciones de software que utiliza la Organización. El software no propietario está registrado en el inventario de equipos como SOFTWARE. La organización garantiza la legalidad de las aplicaciones inventariadas en su listado y prohibe y controla la instalación de software no autorizado fuera del inventario en su Protocolo de Seguridad de la Información.	Responsable del Sistema	RE-723 - Listado de Activos IT-70-01 - Protocolo de Seguridad de la Información RE-10 - Inventario de Equipos
A.18. Cumplimiento	**A.18.1. Cumplimiento de los requisitos legales y contractuales**	A.18.1.3. Protección de los registros de la organización. Los registros deben estar protegidos contra la pérdida, destrucción, falsificación, revelación o acceso no autorizados de acuerdo con los requisitos legales, regulatorios, contractuales y de negocio.	Sí	Aplica a todos los registros inventariados en el listado de documentos del sistema. Los registros están protegidos mediante controles de acceso y copias de seguridad. La organización garantiza las medidas de seguridad de la información adecuadas, evidenciadas en el inventario de elementos de infraestructura identificadas como MEDIDAS DE SEGURIDAD y en el diagrama de la configuración.	Responsable del Sistema	RE-10 - Inventario de Equipos RE-701 - Diagrama de Configuración RE-01 - Listado de Documentos del Sistema 28 - Acceso a SMARTME DASHBOARDS integrado en la herramienta de usuario 65 - Acceso único SMARTME APP - BBDD Transaccional (AMAZON) 23 - Accesos a base de datos Transaccional (AMAZON) 67 - Accesos a BITRIX 25 - Accesos a GestNear (DOMINION) 26 - Accesos a Microsoft Dynamics CRM 68 - Accesos a TQNET 66 - Accesos a TRELLO 69 - Cuentas de usuario de Microsoft 71 - Copia de seguridad servidor CPD
A.18. Cumplimiento	**A.18.1. Cumplimiento de los requisitos legales y contractuales**	A.18.1.4. Protección y privacidad de la información de carácter personal. Debe garantizarse la protección y la privacidad de los datos, según se requiera en la legislación y reglamentación aplicables.	Sí	La legislación aplicable son el Reglamento General y la Ley de Protección de Datos identificados en el listado de normativa aplicable. La organización tiene implantado un protocolo para la protección de los datos personales tal y como marca la ley.	Dirección	RE-21 - Normativa aplicable PD - Documento de seguridad
A.18. Cumplimiento	**A.18.1. Cumplimiento de los requisitos legales y contractuales**	A.18.1.5. Regulación de los controles criptográficos. Los controles criptográficos se deben utilizar de acuerdo con todos los contratos, leyes y regulaciones pertinentes.	Sí	Los controles criptográficos utilizados son protocolos de cifrado de aplicaciones estándares del mercado. La Organización cuida que los proveedores de estas aplicaciones cumplan la legislación vigente.		94 - Cifrado de VPN 92 - Protocolo HTTPS para aplicaciones web 93 - Protocolo HTTPS para servicio web 91 - Protocolo SSL/TLS para correo electrónico
A.18. Cumplimiento	**A.18.2. Revisiones de la seguridad de la información**	A.18.2.1. Revisión independiente de la seguridad de la información. El enfoque de la organización para la gestión de la seguridad de la información y su implantación, es decir, objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información, debe someterse a una revisión independiente a intervalos planificados o siempre que se produzcan cambios significativos en la implantación de la seguridad.	Sí	El requisito aplica a la totalidad del Sistema de Gestión. La Organización ha desarrollado una ficha de proceso para la realización de auditorías objetivas e independientes, que se evidencia mediante el Plan de Auditorías y los informes de auditoría derivados.	Responsable del Sistema	FP-14 - Auditorías RE-30 - Plan de Auditorías RE-31 - Informe de Auditoría
A.18. Cumplimiento	**A.18.2. Revisiones de la seguridad de la información**	A.18.2.2. Cumplimiento de las políticas y normas de seguridad. Los directivos deben asegurarse que todos los procedimientos de seguridad dentro de su área de responsabilidad se realizan correctamente con el fin de cumplir las políticas y normas de seguridad y cualquier otro requisito de seguridad aplicable.	Sí	Aplica a todos los empleados y responsables de procesos de la Organización. La Dirección de SMARTME ANALYTICS impulsa la implantación de la norma de Seguridad de la Información y evidencia de ello es la publicación de su política, la concienciación de los empleados mediante el plan de formación y el nombramiento de responsables de los diferentes procesos y tareas a través de la comunicación de perfiles y organigrama. Las políticas y normas de seguridad se comunican a los empleados y su cumplimiento es una competencia que se incluye en los perfiles de puesto. El grado de cumplimiento queda registrado en las evaluaciones del desempeño que realizan los responsables a sus equipos.	Dirección	PSI - Política de Seguridad de la Información OR - Organigrama RE-04 - Perfil RE-07 - Plan de Formación RE-02 - Control de la Distribución RE-09 - Evaluación
A.18. Cumplimiento	**A.18.2. Revisiones de la seguridad de la información**	A.18.2.3. Comprobación del cumplimiento técnico. Debe comprobarse periódicamente que los sistemas de información cumplen las políticas y normas de seguridad de la información de la organización.	Sí	El requisito aplica a todos los activos de la información de la Organización. La Organización planifica auditorías internas periódicas con la finalidad de comprobar el cumplimiento del sistema de seguridad de la información implantado.	Responsable del Sistema	RE-30 - Plan de Auditorías RE-31 - Informe de Auditoría
A.9. Control de acceso	**A.9.1. Requsitos de negocio para el control de acceso**	A.9.1.1. Política de control de acceso. Se debe establecer, documentar y revisar una política de control de acceso basada en los requisitos de negocio y de seguridad de la información.	Sí	El requisito aplica al acceso de los activos de la información inventariados en SMARTME. Para establecer los procedimientos de acceso a estos activos, la organización ha elaborado una ficha de proceso para la Seguridad de la Información, una instrucción	Responsable del Sistema	FP-70 - Seguridad de la Información IT-70-01 - Protocolo de Seguridad de la Información IT-70-02 - Protocolo de Seguridad de la Información para colaboradores

				técnica como Protocolo para la Seguridad de la Información que la desarrolla y que se comunica a sus empleados y colaboradores y cuenta con un registro en el que se listan los accesos permitidos por activo y persona.		

ISO 20252. Anexo D. Observación digital

Nivel 1	Nivel 2	Requisito	Aplica	Aplicabilidad	Responsables	Documentos
D.1. General	**D.1. General**	El proveedor del servicio que oferta recopilación de datos utilizando metodologías pasivas, directamente o a través de subcontratación del servicio, debe adecuarse al Anexo D.	Sí	SMARTME ANALYTICS desarrolla su actividad en base al big data registrado desde su aplicación para smartphones SMARTME APP, una herramienta de tecnología observacional propietaria. Por lo tanto, la Organización se ajustará principalmente al Anexo D de la norma ISO 20252 y así queda reflejado en su Declaración de Aplicabilidad.	Responsable del Sistema	RE-900 - Declaración de Aplicabilidad
D.2. Propuestas y ofertas	**D.2.1. Propuestas y licitaciones del proveedor del servicio a los clientes.**	Las propuestas, las ofertas o licitaciones deben realizarse por escrito, online u offline, y deben describir claramente las responsabilidades del cliente y del proveedor del servicio, así como las herramientas utilizadas y la implementación de los resultados. Las propuestas deben el contenido mínimo que establece la norma.	Sí	La Organización realiza y entrega las propuestas de servicio, según la sistemática descrita en la ficha del proceso Comercial y utilizando un formato preestablecido de forma que se garantice el contenido mínimo de estas.	Ventas y Marketing Dirección	RE-19 - Propuesta FP-07 - Comercial
D.2. Propuestas y ofertas	**D.2.2. Otros aspectos a establecer por los proveedores del servicio**	D.2.2.1. General. Para facilitar la transparencia y el entendimiento del proyecto y sus capacidades y limitaciones, el proveedor del servicio debe tener preparada y disponible la exposición para los clientes de los puntos D.2.2.2., D.2.2.3. y D.2.2.4. del Anexo D.	Sí	La Organización ha desarrollado Fichas Técnicas para cada uno de los servicios, que forman parte de su Catálogo, orientadas al mejor entendimiento posible por parte de los clientes de cuáles son las características de sus servicios.	Ventas y Marketing Dirección Gestión Comunidad	RE-35 - Ficha técnica RE-42 - Catálogo de Productos
D.2. Propuestas y ofertas	**D.2.2. Otros aspectos a establecer por los proveedores del servicio**	D.2.2.2. Limpieza y edición de los datos. El proveedor del servicio debe documentar los procesos de limpieza de los datos relevantes para el propósito del estudio y mantener esta documentación disponible para su explicación a los clientes.	Sí	La organización cuenta con sendas fichas de procesos para el Diseño y Desarrollo y el Delivery de los proyectos realizados, así como de una instrucción técnica de buenas prácticas para los científicos y analistas de datos.	Tecnología, Procesos, Herramientas	FP-11 - Diseño y Desarrollo FP-09 - Delivery IT-09-01 - Delivery
D.2. Propuestas y ofertas	**D.2.2. Otros aspectos a establecer por los proveedores del servicio**	D.2.2.3. Análisis de texto y/o emoción. Cuando proceda, el proveedor del servicio debe preparar y tener disponible para el cliente aspectos como el tipo de datos analizado, si el análisis ha sido manual o automático, la metodología, medidas de calidad, y otros.	Sí	La organización cuenta con sendas fichas de procesos para el Diseño y Desarrollo y el Delivery de los proyectos realizados, así como de una instrucción técnica de buenas prácticas para los científicos y analistas de datos.	Tecnología, Procesos, Herramientas	FP-09 - Delivery FP-11 - Diseño y Desarrollo IT-09-01 - Delivery
D.2. Propuestas y ofertas	**D.2.2. Otros aspectos a establecer por los proveedores del servicio**	D.2.2.4. Analítica web. El proveedor del servicio debe preparar y tener disponible documentación sobre el tipo de datos que recopila, visitas y visitantes, navegadores, usuarios únicos o múltiples, y otros.	Sí	La organización cuenta con sendas fichas de procesos para el Diseño y Desarrollo y el Delivery de los proyectos realizados, así como de una instrucción técnica de buenas prácticas para los científicos y analistas de datos.	Tecnología, Procesos, Herramientas	FP-09 - Delivery FP-11 - Diseño y Desarrollo IT-09-01 - Delivery
D.3. Ejecución de proyectos	**D.3.1. Recopilación de datos del análisis web y análisis digital**	D.3.1.1. Metodología de recopilación de datos. El proveedor del servicio debe documentar la metodología utilizada para recopilar datos de sitios web o redes sociales y la metodología para observar y medir la conducta del público objetivo.	Sí	La organización cuenta con sendas fichas de procesos para el Diseño y Desarrollo y el Delivery de los proyectos realizados, así como de una instrucción técnica de buenas prácticas para los científicos y analistas de datos.	Tecnología, Procesos, Herramientas	FP-09 - Delivery FP-11 - Diseño y Desarrollo IT-09-01 - Delivery
D.3. Ejecución de proyectos	**D.3.1. Recopilación de datos del análisis web y análisis digital**	D.3.1.2. Validación del proceso de recogida de datos. Deben documentarse los detalles de cómo se monitoriza el proceso de recogida de datos para asegurar que se lleva a cabo según lo previsto y cómo se llega a la conclusión de su impacto en la consistencia y fiabilidad de los datos.	Sí	La organización detalla la metodología y validación de la recogida de datos en su ficha de proceso para el Delivery.	Tecnología, Procesos, Herramientas	FP-09 - Delivery
D.3. Ejecución de proyectos	**D.3.1. Recopilación de datos del análisis web y análisis digital**	D.3.1.3. Salvaguardia de los participantes. Cuando se recluten participantes, debe informárseles con una breve descripción de los principios de confidencialidad, de los objetivos generales del estudio, de la identidad del proveedor del servicio y de la voluntariedad de la participación.	Sí	La organización comunica a los participantes la Política de Confidencialidad, que estos deben aceptar antes de finalizar la instalación de la aplicación SMARTME APP.	Dirección	PCO - Política de Cookies PIN - Política de Incentivos PPR - Política de Privacidad
D.3. Ejecución de proyectos	**D.3.1. Recopilación de datos del análisis web y análisis digital**	D.3.1.4. Ponderación. Si fuera necesario aplicar alguna ponderación a los resultados del análisis web y digital, esta ponderación debe ser registrada.	Sí	La organización cuenta con sendas fichas de procesos para el Diseño y Desarrollo y el Delivery de los proyectos realizados, así como de una instrucción técnica de buenas prácticas para los científicos y analistas de datos.	Tecnología, Procesos, Herramientas	FP-09 - Delivery FP-11 - Diseño y Desarrollo IT-09-01 - Delivery
D.3. Ejecución de proyectos	**D.3.2. Protección de los individuos**	Para garantizar hasta donde sea posible el anonimato de los individuos, los datos deben anonimizarse en los resultados hasta no sea posible identificarlos. El proveedor del servicio debe cuidar por que los datos recogidos de los usuarios no resulten en su perjuicio.	Sí	La organización cuenta con sendas fichas de procesos para el Diseño y Desarrollo y el Delivery de los proyectos realizados, así como de una instrucción técnica de buenas prácticas para los científicos y analistas de datos. Los datos son anónimos desde el momento en que son registrados.	Tecnología, Procesos, Herramientas	FP-11 - Diseño y Desarrollo FP-09 - Delivery IT-09-01 - Delivery
D.3. Ejecución de proyectos	**D.3.3. Monitorización de**	El proveedor del servicio debe asegurarse de que cuenta con una	Sí	La actividad que desarrolla SMARTME está basada en el análisis del BIG DATA	Tecnología, Procesos, Herramientas	FP-09 - Delivery

	dispositivos	razón justa para recoger datos mediante la monitorización de dispositivos y con el consentimiento de los usuarios. Estos datos incluyen navegación web, geolocalización, llamadas, audio ambiental, etc.		generado por los usuarios panelistas. Sin la recogida de estos datos, los servicios que presta la organización se perderían sus fundamentos. Así se describe en la ficha de proceso para el Delivery.		

ISO 20252. Anexo F. Gestión de datos y procesamiento

Nivel 1	Nivel 2	Requisito	Aplica	Aplicabilidad	Responsables	Documentos
F.3. Fiabilidad de las bases de datos que no requieren entrada de datos manual	**F.3.2. Recogida de datos electrónica**	El proveedor del servicio debe definir y documentar procedimientos para asegurar la fiabilidad de las tablas de datos creadas. Debe validar y probar el diseño y la implementación del el proceso de entradas automáticas para cada proyecto fase.	Sí	El requisito aplica al proceso de carga de la base de dato Transaccional cargada desde la aplicación SMARTME APP. La Organización cuenta con una ficha de proceso para el Diseño y Desarrollo de nuevos KPIs o indicadores para sus clientes y una instrucción técnica para sus científicos de datos que establecen la sistemática a seguir para validar y probar los modelos de datos y los resultados de los scripts.	Tecnología, Procesos, Herramientas	FP-11 - Diseño y Desarrollo IT-09-01 - Delivery IT-11-01 - Buenas Prácticas de Desarrollo Seguro