A.5 Controles Organizacionales

A.5.1 Políticas para la seguridad de la información

Con el objetivo de garantizar la confidencialidad, integridad y disponibilidad de la información propia o de terceros que ostenta nuestra organización para efecto de llevar a cabo sus operaciones, los usuarios de todos los niveles tienen el deber de ejecutar las medidas pertinentes que sean definidas por el responsable de Seguridad de Información, en representación operativa del Comité del SGI y la Alta Dirección.

Estas medidas deberán aplicarse a todos los sistemas de información que procesan, almacenan, transmiten y acceden a datos personales y datos sensibles, equipos electrónicos y accesos físicos que sean administrados por MEDMarketing, de forma que garanticen la protección contra toda clase de amenaza que comprometa la información hacia una actividad diferente para la que se tiene disponible, a excepción de lo que esté administrado directamente por el cliente.

Estas políticas de seguridad tienen el objetivo principal de cumplir con la norma ISO/IEC 27001:2022 y con la Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP), la dirección se compromete a revisar al menos una vez al año previo al evento de auditoría, revisión y certificación, para mejorar los controles y procesos del Sistema de Gestión Integral mediante la actualización de la valoración de riesgos y de los planes de tratamiento de riesgos, el establecimiento de políticas para la mejora continua, la realización de auditorías internas, revisiones por la dirección y la implementación de acciones de mejora.

La política deberá ser revisada al menos una vez al año previo al evento de auditoría, revisión y certificación para su actualización y autorización de cambios por el Comité del SGI, en caso de que se requiera, el responsable de Seguridad de Información podrá presentar sus sugerencias de mejora en cualquier momento a la Alta Dirección.

Contratistas, Proveedores y Terceros

Los contratistas, proveedores y terceros que tengan acceso a los activos de información, están obligados a cumplir las políticas de Seguridad de la información.

A.5.10 Uso aceptable de la información y otros activos asociados

En el caso de que los proveedores requieran acceso a la información de la organización o del cliente y adicional a otros activos asociados son conscientes de los requisitos de seguridad de la información para protegerla de acuerdo a la política de uso aceptable de la información.

El equipo de cómputo de proveedor que permanezca dentro de las instalaciones de MEDMarketing por tiempo indefinido deberá integrarse al dominio y apegarse a las políticas de la empresa.

Es responsabilidad del proveedor, activar el protector de pantalla con protección de contraseña de su computadora, cuando no se encuentre en su lugar de trabajo y no dejar archivos confidenciales a la vista.

A.5.19 Seguridad de la información para la relación con proveedores

La organización identifica y establece diferentes controles de seguridad para tratar de forma adecuada el acceso a la información de los proveedores de la organización a través de una política donde se especifican los requisitos a cumplir, la mitigación de riesgos y el acceso controlado a los activos de la organización.

El tipo de acceso requerido (físico/lógico y a qué recurso)

- Los motivos para los cuales se solicita el acceso.
- El valor de la información. o Los controles colaboradores por la tercera parte.
- La incidencia de este acceso en la seguridad de la información de la empresa.

En todos los contratos cuyo objeto sea la prestación de servicios a título personal bajo cualquier modalidad jurídica que deban desarrollarse dentro de la organización, se establecerán los controles, requerimientos de seguridad y compromisos de confidencialidad aplicables al caso, restringiendo al mínimo necesario, los permisos a otorgar.

En ningún caso se otorgará acceso a terceros a la información, a las instalaciones de procesamiento u otras áreas de servicios críticos, hasta tanto se hayan implementado los controles apropiados y se haya firmado un contrato o acuerdo que defina las condiciones para la conexión o el acceso.

A.5.20 Abordar la seguridad dentro de los acuerdos con proveedores

La organización establece todos los requisitos de seguridad de la información relevantes de acuerdo a cada proveedor que proporciona un producto o servicio a la organización que pueda acceder, procesar, almacenar, comunicar o proporcionar componentes de la infraestructura de TI o cualquier otro activo de la organización.

A.5.21 Gestión de la seguridad de la información en la cadena de suministro de las TIC

La organización establece acciones y requisitos diseñados a través del procedimiento de Gestión de riesgos en la cadena de suministro, para identificar, evaluar, mitigar y controlar los riesgos de seguridad de la información asociados a los sistemas que procesan, almacenan, transmiten y acceden a información del cliente, datos sensibles y datos personales que pueden afectar la cadena de suministro de la organización.

El Control de acceso a información es restringida a terceros
Una vez realizado el plan de riesgos sobre la información para terceras partes, se deberá registrar en una bitácora:

- Nombre del tercero.
- Fecha y hora de ingreso.
- Personal/Área que visita.
- Motivo de la visita.

Equipo de cómputo en caso de ingresarlo.

- Al momento de abandonar las instalaciones deberá registrar su salida indicando:
- Hora de salida.
- Validación del equipo de cómputo en caso de haberlo ingresado.

A.5.22 Gestión de monitoreo, revisión y cambios a los servicios de proveedores

La organización monitorea, revisa, evalúa y audita la entrega de los productos y servicios de los proveedores conforme a lo establecido en los acuerdos contractuales. Esto se realiza a través de la Subdirección de Administración y Finanzas para confirmar el cumplimiento y abordar cualquier incidente o problema de seguridad que puedan surgir.

A.5.23 Seguridad de la información para uso de servicios de la nube

La organización actualmente no cuenta con los servicios de nube para proveer el servicio de Telemarketing o soluciones de terceros que tengan una conexión a servicios de la nube.

Cuando sea necesario tener un servicio en la nube dicho proveedor se apegará a los requisitos para tratar de forma adecuada el acceso a la información y el acceso controlado a los activos de la organización.

A.5.24 Gestión, previsión y preparación contra incidentes de seguridad de la información

La organización establece roles, responsabilidades y procedimientos de gestión para garantizar una rápida, eficaz y ordenada respuesta a los incidentes de seguridad de la información en los sistemas de información que procesan, almacenan, transmiten y acceden a información del cliente, datos sensibles y datos personales.
Ver documentos: Procedimiento de Incidentes de Seguridad (MED-A05-PR-05).

A.5.29 Seguridad de la información durante interrupciones

La organización determina los requisitos necesarios de seguridad de la información y la continuidad de la gestión de seguridad de la información en situaciones adversas como crisis o desastres que puedan afectar el servicio de Telemarketing.
Se tienen establecidos, documentados e implementados los procedimientos y controles para asegurar el nivel adecuado de seguridad de la información en el caso donde se requiera la aplicación de un Plan de Continuidad del Negocio o Plan de Recuperación de Desastres.
Ante cualquier eventualidad que afecte la continuidad del negocio MEDMarketing deberá ejecutar el Plan de Continuidad del Negocio con la finalidad de identificar, establecer y notificar los recursos humanos y materiales, así como las actividades que le permitirán a MEDMarketing responder ante un evento disruptivo que pudiera poner en riesgo la continuidad de cualquier proceso crítico.

En el caso de causas naturales que afecten la continuidad del negocio el proceso puede iniciar por instrucción de Dirección General de acuerdo a lo establecido en el Plan de Continuidad del Negocio y Plan de Recuperación de Desastres.

La organización lleva a cabo la comprobación de los controles establecidos e implementados en intervalos planificados de al menos una vez al año previo al evento de auditoría, revisión y certificación para asegurar su continuidad, vigencia, adecuación y eficacia en ambientes controlados con escenarios apegados a la realidad de la operación del negocio.

A.5.34 Privacidad y protección de información de identificación personal

En la organización se brinda la protección y privacidad de los datos personales de acuerdo a la Ley Federal de Protección de Datos Personales en Posesión de Particulares. Esto se logra a través de los responsables de gestión de datos personales apegados a los principios de privacidad.

A.6 Controles de Personas

A.6.7 Trabajo remoto

Para la organización es importante el control de todos los activos de información por lo que considera necesario mantener el control adecuado, es por eso que adopta una política de trabajo remoto donde se especifica de forma clara que no se cuenta con este esquema de trabajo para brindar el servicio de Telemarketing.

A.7 Controles Físicos

A.7.3 Aseguramiento de oficinas, salas e instalaciones

En la organización se cuenta con las siguientes medidas de seguridad física para asegurar las oficinas de procesamiento de información sensible:

- Las instalaciones se encuentran situadas de manera estratégica en diferentes ubicaciones en caso de redundancia por lo que, si ocurre un incidente, la operación puede continuar brindando el servicio de telemarketing a los clientes.
- Los procesos más críticos y sensibles relacionados a la información del cliente se encuentran aislados de la comunicación al exterior, por lo que no sería posible que de forma visual o auditiva pudieran conocer información completa o parcial sobre el tratamiento de los datos.
- Los controles físicos que robustecen el acceso a estas áreas sensibles son dispositivos biométricos, CCTV de vigilancia, alarmas en puertas, oficial de seguridad, arcos detectores de metales, garret y validación de identidad en las entradas de la organización.
- En caso de ser una visita de un proveedor por única ocasión o de no estar dado de alta como proveedor de MEDMarketing, ningún visitante podrá estar solo durante su estancia en las instalaciones, sin excepción, deberá ser supervisado o acompañado en todo momento por una persona designada por el responsable del área que visita.

A.7.5 Protección contra amenazas externas y ambientales

La organización cuenta con un programa de protección civil especializado sobre cómo evitar, actuar y reestablecer el orden después de una situación por fuego, inundación, terremoto, explosión, revueltas sociales y otras formas de desastres naturales o provocados por el hombre.

En el caso de algún incidente dentro de las instalaciones de la empresa y no conocer el plan de protección civil, contamos con brigadas de seguridad que dará las instrucciones pertinentes, siempre salvaguardando la seguridad física de todos los colaboradores que se encuentren en las instalaciones. El proveedor se compromete a hacer del conocimiento de esto a todo su personal o subcontratistas que visiten las instalaciones de MEDMarketing.

A.7.7 Pantalla y escritorio limpio

En caso de que el proveedor desempeñe sus funciones dentro de las instalaciones de MEDMarketing, deberá apegarse a los controles de pantalla y escritorio limpio de acuerdo a la clasificación de información, nivel de sensibilidad y ejecución de procesos con la finalidad de no comprometer ningún activo de la organización.

No debe colocar archivos de carácter confidencial en el escritorio del equipo de cómputo, ni aquellos que puedan comprometer la confidencialidad de la información.

- Todos los archivos confidenciales, deben guardarse con contraseña.
- Conserve sobre su escritorio sólo las cosas que necesita para su día de trabajo. Organizar los documentos que necesita para el trabajo inmediato. Archive cualquier otra carpeta o documento.
- De tener que abandonar su escritorio para asistir a reuniones o tomarse un descanso, verifique si hay información sensible sobre su escritorio y colóquela dentro de una carpeta fuera de su escritorio. Asegúrese de activar el protector de pantalla con protección de contraseña de su computadora.
- Cuando abandone su escritorio al final del día, no deje documentos sobre él. Es fundamental que archive sus documentos y en el caso de documentos restringidos o confidenciales guárdelos bajo llave. Despejar la superficie de su escritorio todos los días antes de irse.

Todos los cajones y puertas de los muebles deberán permanecer cerrados cuando no lo ocupes.

A.7.10 Medios de almacenamiento

El puerto USB se encuentra deshabilitado en todos los equipos de la empresa y de proveedores para protección contra uso de medios de almacenamiento.

En el caso requerirlo, se aplica el manejo de excepción correspondiente, con las siguientes restricciones:

- Debe ser utilizado con cifrado AES de 128 bits o superior.
- Solo debe ser utilizado para fines laborales.

En la organización se controla el acceso a los diferentes medios de almacenamiento que representan un riesgo a la operación del servicio de Telemarketing, se tienen implementadas políticas y procedimientos establecidos sobre la transportación segura de información, el acceso no autorizado, el mal uso que le puedan dar, la corrupción de los paquetes, el robo de información y cuando la información ya concluyo su utilidad se realiza un procedimiento de borrado seguro.

En el caso que la organización solicite la destrucción de cierta información a su proveedor, se deberá llevar a cabo iniciando la petición por escrito por parte de MEDMarketing, la identificación de la información que será destruida y soporte técnico será quien gestione con los responsables las actividades correspondientes.

De manera lógica se realiza una técnica de borrado seguro que se determine en el momento, apegándose al procedimiento de Seguro.

A.8 Controles Tecnológicos

A.8.1 Dispositivos de punto final de usuario

La organización adopta una política y medidas de seguridad para controlar y gestionar los riesgos introducidos por el uso de dispositivos de punto final.
En el caso de los proveedores no pueden acceder con cualquier dispositivo móvil (tabletas, teléfonos inteligentes, lap top, relojes inteligentes, dispositivos inteligentes portátiles, altavoces inteligentes) a la red o correo electrónico de MEDMarketing.

En caso de que el proveedor requiera utilizar equipo laptop que no sea proporcionado por MEDMarketing para facilitar sus servicios, debe de cumplir con las siguientes políticas:

- Instalar y configurar un antivirus.
- Configurar el cifrado de disco y comunicaciones.
- Utilizar canales cifrados seguros de comunicación VPN - Red privada virtual o algún otro tipo de cifrado punto a punto, como los sitios web con protocolo SSL (Secure Sockets Layer) y certificado.

Esta protección es para mantener la confidencialidad y seguridad de los sistemas de información que procesan, almacenan transmiten y acceden a información del cliente, datos sensibles y datos personales.

El sistema operativo del equipo de cómputo de MEDMarketing o proveedor y Servidores (a nivel consola) deberá realizar un bloqueo de sesión por inactividad a los 5 minutos de la misma.

A.8 Controles Tecnológicos

A.8.7 Protección contra malware

La organización ha implementado los controles necesarios de detección, prevención y recuperación para protegerse contra malware, basándose en la detección y reparación del software, la concientización de seguridad y controles para el acceso al sistema, y gestión del cambio apropiado.

A.8.20 Controles de red

Las redes de la organización son gestionadas y controladas por el especialista en redes y telecomunicaciones para proteger la información en los sistemas de información que procesan, almacenan, transmiten y acceden a información del cliente, datos sensibles y datos personales frente a accesos no autorizados, considerando los siguientes aspectos:

- Las redes son gestionadas por el especialista en redes con el apoyo del equipo de infraestructura a través de diferentes mecanismos y herramientas.
- Se cuenta con una segmentación de red inalámbrica en donde se tiene una red de invitados la cual no tiene acceso a sistemas de información productivos.
- Únicamente se le da acceso a la red a invitados que lo solicitan como clientes y proveedores.
- La red productiva no se encuentra en un segmento inalámbrico por lo que no hay riesgo de acceso no autorizado.

- Se cuenta con un cifrado WPA configurado para cifrar la comunicación entre laptop y el punto de acceso.
- Todos los usuarios que se conectan a la red inalámbrica de invitados es necesario dar acceso desde Fortinet a través de la dirección IP y dirección MAC, de lo contrario no podrán iniciar una navegación.
- El acceso a internet se encuentra restringido principalmente a páginas relacionadas con los siguientes temas: juegos, películas, videos no relacionados con el desempeño de sus funciones, redes sociales, casas de apuestas, pornografía, erotismo, música, video juegos y páginas que el responsable de la seguridad indique para su bloqueo.
- El proveedor reconoce que toda la información proporcionada por MEDMarketing es propiedad de la empresa.
- Es responsabilidad de la empresa y del proveedor el resguardo y confidencialidad de la información de proyectos, estudios, folletos, publicaciones, manuales, presentaciones, dibujos, diagramas, propuestas, diseños, código, configuración, planos, memorándums, correspondencia y cualquier otro documento o información relativos a procedimientos y normas de las mismas, los cuales tienen carácter estrictamente confidencial y, todos los documentos e información escrita y verbal a que tenga acceso o se le proporcionen durante la prestación de sus servicios.
- El proveedor se compromete a no revelar a ninguna persona física o moral, la información confidencial de la empresa, de sus clientes o de terceros que sea de su conocimiento, a menos de que tal comunicación o uso sea en función directa de las actividades laborales que así le correspondan, lo anterior incluye cualquier información confidencial que haya sido adquirida, obtenida o desarrollada por el proveedor.

A.8.24 Uso de criptografía

En la organización se tiene establecida una política sobre la especificación de controles criptográficos para la protección de los sistemas de información que procesan, almacenan, transmiten y acceden a la información del cliente, datos sensibles y datos personales considerando el uso, protección y tiempo de vida de las llaves criptográficas, a través de todo su ciclo de vida incluyendo la generación, almacenamiento, archivo, recuperación, distribución, retirada y destrucción de las mismas.

EL PROVEEDOR SE OBLIGA A CUMPLIR CON TODAS Y CADA UNA DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN QUE SE DICTEN Y PUBLIQUEN POR MEDMARKETING, MISMAS QUE TENDRÁN EL CARÁCTER OBLIGATORIO Y DE OBSERVANCIA GENERAL. EL DESCONOCIMIENTO DE LAS MISMAS NO EXIME DE SU CUMPLIMIENTO Y RESPONSABILIDAD.