Política de Seguridad

Índice

Propósito de la Política

Esta Política de Seguridad de la Información expresa el compromiso de Sondeos para gestionar eficaz y eficientemente los riesgos de seguridad de la información, coordinados a nivel global y en cumplimiento con las regulaciones aplicables dondequiera que realice negocios. Esta Política es la base de todas las actividades de seguridad de la información. Se centra no solo en la tecnología para el almacenamiento, procesamiento y transmisión de información, sino también en las prácticas administrativas y operativas para la protección de toda la información, datos, archivos y recursos de procesamiento propios y de terceros gestionadas por **Sondeos.** La intención de esta Política es facilitar el intercambio de información y recursos informáticos, equilibrando la necesidad de proteger la información con el costo de implementación. Esta Política es propiedad de **Sondeos** y está destinada a ser distribuida a todos los empleados y usuarios de sistemas de gestión de seguridad de la información en las ubicaciones de **Sondeos**.

Alcance de la Política

Esta Política se aplica a todos los empleados, proveedores, contratistas y consultores que crean, distribuyen, acceden o gestionan información a través de los sistemas de tecnología de la información de **Sondeos**, Incluidos los activos corporativos (celulares, notebooks, etc), redes y servicios de comunicación a los que están conectados. También se aplica por igual a individuos y empresas que, debido a su relación con **Sondeos**, están confiados con información confidencial o sensible. Esta Política aborda todos los aspectos de la seguridad de la información y la continuidad desde el diseño inicial de un sistema hasta la implementación y operación. También aborda cualquier dispositivo utilizado para almacenar, procesar o comunicar información protegida u otra información propiedad de **Sondeos**.

Alcance asociado al SGSI

Prestación del Servicio de plataforma Multichannel de Omnicanalidad en la Modalidad Software As a Service (SaaS).

Definiciones

Propietario de la Información

Sondeos designa propietarios para cada tipo de información, tanto la propia como la gestionada en nombre de los clientes o partes interesadas, con el fin de garantizar su adecuada protección y uso. El propietario de la información es responsable de:

- Determinar y documentar la clasificación de sensibilidad y el nivel de criticidad de la información.
- Establecer los criterios de acceso y aprobar qué usuarios o roles podrán utilizarla.
- Autorizar el uso, procesamiento, transmisión, almacenamiento o eliminación de la información en función de su clasificación.
- Asegurar que se cumplan los requisitos legales, contractuales y de seguridad aplicables a dicha información.

Esta responsabilidad aplica tanto a la información generada internamente como a la de terceros, preservando en todos los casos su confidencialidad, integridad y disponibilidad.

Custodios

Los Custodios están en posesión física o lógica de la información de Sondeos o de la información que se ha confiado a Sondeos. Mientras que los Administradores de Sistema son Custodios, cuando la información se mantiene solo en una computadora personal, el Usuario también es un Custodio. Los Custodios son responsables de salvaguardar la información, incluida la

implementación de sistemas de control de acceso para evitar la divulgación inapropiada y realizar copias de seguridad para que la información crítica no se pierda. Los Custodios también están obligados a implementar, operar y mantener las medidas de seguridad definidas por los Propietarios de la Información.

Política Marco de Seguridad de la Información

Proteger la Información: Protegemos la información asegurando la confidencialidad, integridad y disponibilidad de toda la información que gestionamos en la organización.

Gestionar los Riesgos: Gestionamos los riesgos identificando, evaluando y mitigando aquellos relacionados con la seguridad de la información, a través de una metodología establecida.

Brindar respuesta a incidentes: Respondemos a incidentes mediante procedimientos eficaces para la detección, notificación y gestión de incidentes de seguridad de la información.

Formar y concienciar: Aseguramos que todos los empleados comprendan y cumplan con las políticas y procedimientos de seguridad de la información a través de la formación y concientización continua.

Mantener la continuidad del negocio: Implementamos y mantenemos planes de continuidad del negocio y recuperación ante desastres para minimizar el impacto de interrupciones y asegurar la disponibilidad de la información.

Fomentar la mejora Continua: Revisamos y mejoramos continuamente el sistema de gestión de seguridad de la información para adaptarnos a los cambios en el entorno, las tecnologías y las amenazas.

Usuarios de la Información

Los Usuarios de la Información incluyen a todos los empleados de Sondeos que acceden o reciben información producida, almacenada o comunicada por los sistemas de tecnología de la información de Sondeos. Los Usuarios también incluyen a todas las personas que, debido a su relación con Sondeos (por ejemplo, contratistas, proveedores, proveedores de servicios, consultores, etc.), están confiadas con información sensible o confidencial. Los Usuarios son responsables de cumplir con la Política de Seguridad de la Información y con Normas y Procedimientos individuales.

Requisitos de la Política

Si alguno de los siguientes requisitos de esta política no puede cumplirse, entonces esa exención de seguridad debe documentarse y registrarse. Las exenciones deben ser reportadas al Information Security Analyst.

Gestión de Seguridad

La seguridad de la información corporativa, aplicaciones, sistemas y redes es fundamental para el éxito continuo de Sondeos. La gestión de seguridad busca establecer controles y medidas para minimizar el riesgo de pérdida de información y recursos del sistema, corrupción de datos, interrupción del acceso a los datos y divulgación no autorizada de información. La gestión de seguridad se logra mediante políticas, normas y procedimientos efectivos que asegurarán la confidencialidad, integridad y disponibilidad de la información, aplicaciones, sistemas y redes de Sondeos para usuarios autorizados.

Confidencialidad

La confidencialidad se refiere a la protección de la información contra el acceso no autorizado, independientemente de dónde resida o cómo esté almacenada. La información que es sensible o propietaria debe ser protegida a un nivel más alto que otra información. Consulta la Política de Clasificación y Manejo de la Información para obtener más orientación.

Integridad

La integridad es la protección de la información, aplicaciones, sistemas y redes contra cambios intencionales, no autorizados o accidentales. También es importante proteger los procesos o programas utilizados para manipular datos. Los usuarios que acceden a información sensible, aplicaciones, sistemas y redes deben ser identificados y autenticados.

Disponibilidad

La disponibilidad es la garantía de que la información y los recursos de Sondeos estén accesibles para usuarios autorizados según sea necesario. Hay dos problemas relativos a la disponibilidad: la negación de servicios causada por la falta de controles de seguridad (por ejemplo, destrucción de datos o equipos, virus informático) y la pérdida de servicios de los recursos de información debido a desastres naturales (por ejemplo, tormentas, inundaciones, incendios). Consulta el Proceso de Planificación de Continuidad del Negocio para obtener más información sobre cómo abordar esto.

Autenticación

La autenticación requiere que se identifique correctamente el origen de un mensaje con la garantía de que no es una identidad falsa o falsificada. Las contraseñas se utilizan para autenticar a un usuario basándose en el hecho de que solo el usuario debe conocer la contraseña. Se utilizarán contraseñas fuertes que deben cumplir con varias reglas, como combinaciones de letras y números con mayúsculas y minúsculas. Además del uso de contraseñas, siempre que sea posible, se implementará la Autenticación Multifactor.

Activos de Información

Toda la información, datos, aplicaciones, redes y equipos son propiedad de Sondeos y se proporcionan a sus empleados para que puedan llevar a cabo sus responsabilidades laborales de manera efectiva. Estos activos deben tratarse con privacidad y confidencialidad de acuerdo con la Política de Clasificación y Manejo de la Información al realizar negocios y no deben ponerse a disposición

o ser accesibles para nadie fuera de la empresa sin el permiso específico por escrito de la Alta Dirección.

La información de Sondeos y la infraestructura de procesamiento de información son activos vitales que requieren protección acorde con su valor. La información organizativa, aplicaciones, sistemas y redes deben ser gestionados activamente para garantizar la seguridad, confidencialidad, integridad y disponibilidad.

Responsabilidad

Los entornos administrativos e informáticos de Sondeos mantendrán estándares consistentes para establecer la responsabilidad y autenticidad de los usuarios del sistema, los cuales serán compatibles con las Políticas internas de Sondeos.

Para mantener la responsabilidad del acceso al sistema, Sondeos implementará lo siguiente:

- Todas las personas con acceso a los sistemas utilizarán un ID de usuario autorizado por la dirección de la empresa y asignado específicamente a esa persona. Se prohíbe compartir IDs de usuario, excepto en situaciones específicas y aprobadas.
- Todas las personas con IDs de usuario de red, sistema y aplicación retendrán una contraseña confidencial que se utilizará para autenticar la identidad de la persona. Se prohíbe la divulgación intencional o el intercambio de contraseñas.

Acceso a la Información

Todo acceso a la información debe ser autorizado por el propietario de la información, con el acceso otorgado o revocado sólo según los requisitos comerciales. El acceso a datos administrativos se otorgará solo a los empleados de Sondeos. Las personas fuera de Sondeos pueden recibir autorización para acceder a los datos de Sondeos solo si esa autorización es otorgada por el Propietario de la Información.

Las capacidades/restricciones de acceso y actualización se aplicarán a todos los datos de Sondeos, almacenados en las instalaciones informáticas de la empresa. Las medidas de seguridad se aplican a todos los sistemas desarrollados y/o mantenidos por Sondeos.

El Jefe de la Unidad de Negocios apropiada y el Administrador del Sistema son responsables de autorizar el acceso a sistemas e información, verificar la integridad de la información y controlar la información extraída. La dirección es responsable de desarrollar sistemas de procesamiento seguros y operar estos sistemas en un entorno controlado. Se requiere que los empleados cumplan con las instrucciones de la dirección para el uso y protección de los sistemas de procesamiento de tecnología de la información y la información.

Los empleados deben estar al tanto de la importancia de la seguridad de la información. Todos los gerentes y empleados deben actuar con urgencia y diligencia para cumplir con estos requisitos.

Se deben llevar a cabo evaluaciones de riesgos y se deben evaluar los riesgos identificados para determinar el nivel óptimo de control requerido para cada tipo de sistema de tecnología de la información. Se deben incluir controles adecuados para garantizar que se logre la seguridad de la información, la confidencialidad, la integridad y la disponibilidad.

Responsabilidades de la Política

Information Security Analyst

El Information Security Analyst tiene la responsabilidad general de los asuntos de seguridad de la información. Estas responsabilidades son:

- Asegurar que los controles de acceso y autenticación del usuario estén en su lugar.
- Asegurar que las políticas, normas y procedimientos de seguridad documentados sean revisados, actualizados y mantenidos periódicamente por las personas apropiadas.

- Evaluación de Exposiciones de Seguridad, Uso Incorrecto o Situaciones de No Cumplimiento.
- Garantizar que los empleados cumplan con sus responsabilidades de seguridad de acuerdo con las políticas, normas y procedimientos relacionados.
- Desarrollar e implementar el Programa de Concientización en Seguridad.

Recursos de Información

Los recursos de información, incluido el software y los sistemas de soporte informático, deben protegerse adecuadamente para mantener la sensibilidad y la naturaleza crítica de la información que se procesa, almacena o comunica. Los sistemas de información deben protegerse de manera que las personas no autorizadas no puedan acceder directamente al dispositivo y causar daños físicos o modificar componentes internos que podrían afectar los resultados de los procesos informáticos u otros procesos.

Los controles ambientales y de seguridad deben ser apropiados para el nivel de riesgo. Se debe realizar una evaluación que equilibre el riesgo con el costo de implementar el control al determinar qué controles de seguridad y ambientales son apropiados.

Los usuarios son responsables de cumplir con las leyes de copyright, patentes y acuerdos de licencia para propiedad intelectual.

Las instalaciones y equipos de comunicación deben protegerse contra modificaciones y manipulaciones no autorizadas para garantizar que los mensajes en tránsito no sean modificados o recibidos por partes no deseadas, o que los servicios de comunicación no se vean interrumpidos. Las instalaciones de comunicación pueden incluir todas las salas de equipos y armarios de cableado y pueden incluir instalaciones y recursos proporcionados por proveedores de servicios externos.

Las preguntas sobre la adecuación de los controles físicos y ambientales deben dirigirse al Oficial de Seguridad.

Propiedad de Sistemas e Información

Sondeos es propietaria de toda la información, aplicaciones, sistemas y software que se desarrollan, utilizan o distribuyen a empleados o representantes designados de entidades que operan como socios comerciales. Aunque Sondeos mantiene la responsabilidad de propiedad última, ciertos gerentes son responsables de ejecutar esta responsabilidad.

Los propietarios de sistemas e información son responsables de identificar y gestionar los riesgos relacionados con la seguridad, integridad y continuidad de la información, así como de los procesos comerciales y funciones del sistema que crean, modifican, eliminan o utilizan esta información. Son responsables de evaluar el nivel de riesgo para Sondeos al proporcionar acceso a la información, así como de determinar el impacto para la organización si la información, los procesos comerciales o las funciones del sistema no estuvieran disponibles o se usaran incorrectamente.

El nivel de riesgo de seguridad, integridad y continuidad debe comunicarse al propietario a las personas o grupos responsables de implementar los controles de seguridad y continuidad comercial de Sondeos.

Periódicamente, el Propietario de la Información y el Oficial de Seguridad revisarán el conjunto actual de accesos y capacidades de actualización otorgadas a cada individuo en el sistema para garantizar que se haya otorgado el nivel apropiado de acceso y que no sean necesarios cambios.

Las evaluaciones de riesgos deben presentarse al Oficial de Seguridad.

Acceso a Sistemas e Información

Sondeos se compromete al principio de privilegio mínimo y, como tal, llevará a cabo revisiones de acceso para asegurar que los Custodios de la Información no tengan acceso excesivo.

Todo acceso a sistemas e información se proporciona en función de la necesidad comercial. Los propietarios de la información, como parte de su responsabilidad de gestión, deben autorizar solicitudes de acceso a información o sistemas, y verificar que dicho acceso satisfaga una necesidad comercial legítima antes de que se implemente.

Se completará un Formulario de Solicitud de Acceso que indicará el acceso al sistema o la información que se debe permitir al Usuario. Este formulario será autorizado por un Jefe de Unidad de Negocios o el Propietario de la Información según sea necesario.

El acceso a información sensible debe restringirse. Los propietarios también pueden designar un período de retención durante el cual se puede autorizar la información o el acceso y después del cual se revocará todo acceso.

Cuando se otorga la aprobación para el acceso externo a la información de Sondeos, se deben proporcionar instrucciones al destinatario notificándoles cualquier requisito de seguridad, incluida la necesidad de mantener la confidencialidad de la información, los requisitos para la distribución de la información dentro de su organización y los procedimientos para la destrucción o devolución de la información después del período de acceso. Todos los empleados firmarán un Acuerdo de No Divulgación.

Todos los ID de Usuario de empleados, contratistas, proveedores y consultores deben desactivarse de inmediato al abandonar la empresa. Cuando un Jefe de Unidad de Negocios recibe notificación de una terminación/resignación de un empleado, debe revisar la disposición de los datos y archivos del Usuario con el Usuario antes de la separación de Sondeos.

Monitoreo y Aplicación de la Seguridad

Es responsabilidad del Oficial de Seguridad implementar medidas apropiadas para detectar intentos de comprometer la seguridad o integridad de la información o sistemas de tecnología de la información. Al implementar capacidades de monitoreo, se debe considerar qué situaciones se deben monitorear según la extensión del riesgo, los medios más efectivos para monitorear actividades de seguridad, los recursos disponibles para el monitoreo y las limitaciones del sistema que limitan la capacidad de monitorear eventos de seguridad. Si no están disponibles medidas adecuadas dentro de un entorno del sistema para monitorear efectivamente eventos de seguridad, se deben implementar controles adicionales para mitigar los riesgos de seguridad.

Cuando ocurre actividad que está en conflicto con las políticas y normas de seguridad, los Jefes de Unidades de Negocios deben tomar las medidas apropiadas para hacer cumplir las prácticas de seguridad deseadas. Las medidas involucradas van desde la capacitación de los Usuarios, revocar el acceso, alterar los parámetros de seguridad y posiblemente acciones disciplinarias.

Debido a la probabilidad de daño y destrucción de información resultante de código malicioso, incluidos virus, las capacidades de detección deben incluir software de detección de malware dentro del entorno de la red de área local, así como en sistemas que estén en alto riesgo de infección.

Programa de Concienciación en Seguridad

Es responsabilidad de la dirección asegurarse de que todos los Usuarios de la información comprendan cómo proteger los activos de la empresa, incluida la información y los recursos de información, y cumplan con las políticas, normas y procedimientos de seguridad. Los supervisores y gerentes deben asegurarse de que las personas que trabajan dentro de su departamento comprendan los requisitos generales de seguridad de la información y tengan suficiente conocimiento sobre las políticas, normas y procedimientos de seguridad de la

tecnología de la información para reconocer la necesidad de proteger la información y los requisitos de los que son específicamente responsables.

El Oficial de Seguridad es responsable de desarrollar e implementar un Programa de Concientización en Seguridad de la Información que respalde la conciencia de los empleados. Los gerentes deben estar al tanto del desempeño del Usuario en esta área, fomentar buenas prácticas de seguridad y abordar comportamientos inapropiados.

Respuesta a Incidentes de Seguridad Informática

Sondeos desarrollará planes y procedimientos efectivos para responder a incidentes de seguridad de la información sospechosos que afecten la confidencialidad, integridad o disponibilidad de datos procesados o propiedad de Sondeos o para los cuales Sondeos sirve como custodio.

Estos planes y procedimientos abordarán las siguientes etapas de respuesta a incidentes:
a. Preparación
b. Detección e Informe
c. Análisis
d. Contención
e. Recuperación
f. Actividades Posteriores al Incidente

Los hechos que rodean una intrusión, infección o compromiso del sistema deben documentarse, informarse al Oficial de Seguridad e incluir las circunstancias que llevaron al descubrimiento del incidente, las acciones que se tomaron inmediatamente, los nombres de las personas involucradas en la investigación del incidente y observaciones detalladas sobre lo que ocurrió, qué daño se causó y qué sistemas o archivos se comprometieron.

Planificación de la Continuidad del Negocio/Recuperación ante Desastres

Si la confidencialidad, integridad o disponibilidad de sistemas o información se ve afectada por un incidente, es responsabilidad de la dirección asegurarse de

que se realice una planificación y preparación para minimizar pérdidas, reducir el impacto y garantizar la continuidad de las funciones y el flujo de ingresos de la organización. Se desarrollará y probará un Plan de Continuidad del Negocio (BCP) para evaluar su efectividad. El BCP abordará el control de riesgos en la planificación previa, la gestión de crisis y la recuperación empresarial.

Cumplimiento

Sondeos cumple con todas las regulaciones federales, estatales, provinciales, locales, de la industria y contractuales aplicables.

Cualquier incumplimiento o violación de esta política debe ser llevado de inmediato a la atención del Oficial de Seguridad. El Oficial de Seguridad trabajará con la dirección de la empresa y los Administradores del Sistema para garantizar que el problema se resuelva y abordar los pasos necesarios para eliminar futuras violaciones. Un proceso de escalada definirá el curso de acción para todas las violaciones, consistente con la gravedad de la violación.

Sondeos se reserva el derecho de disciplinar, terminar, suspender o procesar legalmente, a su discreción, a las personas que violen la Política de Seguridad de la Información.

Entrega de Servicios

Sondeos promueve prácticas seguras en la entrega de sus productos y servicios a través de la conciencia, la formación y las mejores prácticas de la industria.

Seguridad Física y Ambiental

Sondeos mantiene controles para limitar el acceso a activos físicos y mitigar los riesgos asociados con problemas ambientales (incendios, inundaciones, pérdida de energía) para garantizar la protección de datos y la disponibilidad del sistema.

Gestión de Socios de Entrega

Sondeos asegura que existan procesos para evaluar la capacidad de servicio de posibles socios comerciales a través de:

- Acuerdos de No Divulgación.
- Debida diligencia, incluidas referencias, acreditaciones, etc.

Sondeos evalúa a proveedores para garantizar que se cumplan los objetivos de servicio definidos. Asimismo, se asegura de que existan procesos para la terminación de proveedores que proporcionen interrupciones mínimas y mantengan la confidencialidad de los datos.

Información del Cliente como Activo

La información del cliente es reconocida como un **activo estratégico fundamental** tanto para Sondeos como para nuestros clientes. Nos comprometemos a proteger la **confidencialidad, integridad y disponibilidad** de esta información con el mismo rigor y prioridad que la información propia de Sondeos.

Naturaleza Dual del Activo

La información del cliente, que incluye datos personales, comerciales y de uso de servicios, es considerada un activo con **doble titularidad**:

- **Propiedad de Sondeos**: En la medida en que esta información es utilizada para la prestación del servicio de plataforma Multichannel de Omnicanalidad en la modalidad SaaS, para el cumplimiento de obligaciones contractuales, para la mejora de nuestros servicios y para fines analíticos internos, siempre bajo el amparo de la legislación aplicable y los acuerdos con el cliente. Sondeos ejerce la **custodia** y el **tratamiento** de esta información.
- **Propiedad del Cliente**: El cliente mantiene la **propiedad original y principal** de su información. Sondeos actúa como **encargado del tratamiento** de dicha información en nombre del cliente, y está obligada

a protegerla y a utilizarla únicamente según las instrucciones y el consentimiento explícito del cliente, y en cumplimiento con todas las leyes y regulaciones de protección de datos aplicables.

Responsabilidades Compartidas

La protección de la información del cliente es una **responsabilidad compartida** que involucra a Sondeos y a nuestros clientes:

- **Responsabilidades de Sondeos**: Nos comprometemos a implementar y mantener controles de seguridad robustos, incluyendo medidas técnicas, organizativas y administrativas, para proteger la información del cliente contra accesos no autorizados, divulgación, alteración o destrucción. Esto incluye la aplicación de esta Política de Seguridad de la Información a todos los procesos y sistemas que manejan información del cliente.
- **Responsabilidades del Cliente**: Los clientes son responsables de la información que nos confían, incluyendo la legalidad de su obtención, su exactitud y su clasificación. Se espera que los clientes cumplan con sus propias obligaciones de seguridad y privacidad en relación con la información que comparten con Sondeos, y que nos proporcionen instrucciones claras y precisas sobre el tratamiento de sus datos.

Acceso y Tratamiento de la Información del Cliente

El acceso y el tratamiento de la información del cliente se regirán por los principios de **necesidad de conocer** y **privilegio mínimo**. Solo el personal autorizado de Sondeos, que requiera acceso para el desempeño de sus funciones y para la provisión del servicio, podrá acceder a esta información. Cualquier acceso o tratamiento se realizará en estricto cumplimiento de los acuerdos contractuales con el cliente y la normativa de protección de datos.

Gestión de Riesgos y Cumplimiento Regulatorio

Sondeos gestionará proactivamente los riesgos de seguridad asociados a la información del cliente, incluyendo la realización de **evaluaciones de impacto en la protección de datos (DPIA)** cuando sea requerido. Aseguraremos el cumplimiento con las leyes y regulaciones de protección de datos aplicables, como GDPR, LGPD, o cualquier otra normativa relevante en las jurisdicciones donde operen nuestros clientes, garantizando los derechos de los interesados sobre su información.

Revisión de la Política

Esta política y las políticas de Seguridad de la Información de apoyo se revisarán anualmente y se actualizarán según sea necesario.

Revisado: 01.07.2025