Política de seguridad de la información

Contenido

1. Introducción

Este documento define la política de seguridad de la información de TIMEWEB LATAM.

Como empresa moderna y con visión de futuro, TIMEWEB LATAM reconoce en los niveles superiores la necesidad de garantizar que su negocio funcione sin problemas y sin interrupciones en beneficio de sus clientes, accionistas y otras partes interesadas.

Con el fin de proporcionar tal nivel de operación continua, TIMEWEB LATAM ha implementado un Sistema de Gestión de Seguridad de la Información (SGSI) en línea con el Estándar Internacional para la Seguridad de la Información, ISO/IEC 27001. Esta norma define los requisitos para un SGSI basado en las mejores prácticas reconocidas internacionalmente.

El funcionamiento del SGSI tiene muchos beneficios para el negocio, entre ellos:

- Protección de los flujos de ingresos y la rentabilidad de la empresa
- Garantizar el suministro de bienes y servicios a los clientes
- Mantenimiento y mejora del valor para los accionistas
- Cumplimiento de los requisitos legales y reglamentarios

TIMEWEB LATAM ha decidido mantener la certificación completa de ISO/IEC 27001 para que la adopción efectiva de las mejores prácticas de seguridad de la información pueda ser validada por un tercero independiente, un Organismo de Certificación Registrado. Además, se han adoptado las directrices contenidas en los códigos de prácticas ISO/IEC 27017 e ISO/IEC 27018, ya que tienen especial relevancia para los proveedores de servicios en la nube.

Esta política se aplica a todos los sistemas, personas y procesos que constituyen los sistemas de información de la organización, incluidos los miembros de la junta, directores, empleados, proveedores y otros terceros que tienen acceso a los sistemas de TIMEWEB LATAM.

Los siguientes documentos de apoyo son relevantes para esta política de seguridad de la información y proporcionan información adicional sobre cómo se aplica:

- Evaluación de riesgos y proceso de tratamiento
- Declaración de aplicabilidad
- Proceso de evaluación de la seguridad de la información de los proveedores
- Política de uso aceptable de Internet
- Política de computación en la nube
- Política de dispositivos móviles
- Política de teletrabajo
- Política de control de acceso

- Proceso de gestión de acceso de usuarios
- Política criptográfica
- Política de Seguridad Física
- Política antimalware
- Política de copia de seguridad
- Política de software
- Política de Gestión de Vulnerabilidades Técnicas
- Política de seguridad de la red
- Política de Mensajería Electrónica
- Política de Desarrollo Seguro
- Política de Seguridad de la Información para las Relaciones con los Proveedores
- Política de administración de disponibilidad
- Política de cumplimiento de la propiedad intelectual y los derechos de autor
- Política de Retención y Protección de Registros
- Política de Privacidad y Protección de Datos Personales
- Política de escritorio y pantalla clara

Los detalles del número de versión más reciente de cada uno de estos documentos están disponibles en la FO-SGI-02 Control de documentos internos.

2. Política de seguridad de la información

2.1 Requisitos de la seguridad de la información

Se acordará y mantendrá una definición clara de los requisitos de seguridad de la información dentro de TIMEWEB LATAM con los clientes y las partes interesadas, que toda la actividad del SGSI se centre en el cumplimiento de esos requisitos, así como también se contribuirá al proceso de planificación del servicio y desarrollo. Los requisitos específicos con respecto a la seguridad de los sistemas o servicios nuevos o modificados se recogerán como parte de la etapa de diseño de cada proyecto.

Es un principio fundamental del Sistema de Gestión de Seguridad de la Información de TIMEWEB LATAM que los controles implementados estén impulsados por las necesidades comerciales y esto se comunicará regularmente a todo el personal a través de reuniones de equipo y documentos informativos.

2.2 Marco para el establecimiento de los objetivos

Se utilizará un ciclo regular para el establecimiento de objetivos de seguridad de la información, que coincidirá con el ciclo de planificación presupuestaria. De este modo se garantizará la obtención de una financiación adecuada para las actividades de mejora identificadas. Estos objetivos se basarán en una comprensión clara de los requisitos del negocio, informada por el proceso de revisión por la dirección durante el cual se pueden obtener las opiniones de las partes interesadas pertinentes.

Los objetivos de seguridad de la información se documentarán durante un período de tiempo acordado, junto con detalles de cómo se lograrán. Estos serán evaluados y monitoreados como parte de las revisiones de la dirección para garantizar que sigan siendo válidos. En caso de que se requieran modificaciones, estas se gestionarán a través del proceso de gestión de cambios.

De acuerdo con la norma ISO/IEC 27001, los controles de referencia detallados en el Anexo A de la norma serán adoptados, cuando proceda, por [Nombre de la organización]. Estos se revisarán periódicamente a la luz de los resultados de las evaluaciones de riesgos y en consonancia con los planes de tratamiento de riesgos para la seguridad de la información. Para obtener más información sobre los controles del anexo A que se han aplicado y los que se han excluido, véase la *declaración de aplicabilidad*.

Además, se adoptarán y aplicarán, cuando proceda, controles mejorados y adicionales de los siguientes códigos de prácticas:

- ISO/IEC 27002 – Código de prácticas para los controles de seguridad de la información
- ISO/IEC 27017 – Código de prácticas para controles de seguridad de la información basados en ISO/IEC 27002 para servicios en la nube
- ISO/IEC 27018 – Código de prácticas para la protección de la información de identificación personal (PII) en nubes públicas que actúan como procesadores de PII
-

La adopción de estos códigos de prácticas proporcionará una garantía adicional a nuestros clientes y ayudará aún más a cumplir con la legislación internacional de protección de datos.

2.3 Mejora continua del SGSI

La política de TIMEWEB LATAM con respecto a la mejora continua es:

- Mejorar continuamente la eficacia del SGSI;
- Mejorar los procesos actuales para alinearlos con las buenas prácticas definidas en la norma ISO/IEC 27001 y normas relacionadas;
- Obtener la certificación ISO/IEC 27001 y mantenerla de forma continua;
- Aumentar el nivel de proactividad (y la percepción de proactividad de los grupos de interés) con respecto a la seguridad de la información;
- Hacer que los procesos y controles de seguridad de la información sean más medibles con el fin de proporcionar una base sólida para tomar decisiones informadas;
- Revisar las métricas relevantes anualmente para evaluar si es apropiado cambiarlas, en función de los datos históricos recopilados;

- Obtener ideas para mejorar a través de reuniones periódicas y otras formas de comunicación con las partes interesadas, incluidos los clientes de servicios en la nube;
- Revisar las ideas de mejora en las reuniones periódicas de la dirección con el fin de priorizar y evaluar los plazos y los beneficios;

Las ideas para mejoras se pueden obtener de cualquier fuente, incluidos empleados, clientes, proveedores, personal de TI, evaluaciones de riesgos e informes de servicio. Una vez identificados, se registrarán y evaluarán como parte de las revisiones de gestión.

2.4 Áreas de políticas de la seguridad de la información

TIMEWEB LATAM define la política en una amplia variedad de áreas relacionadas con la seguridad de la información, que se describen en detalle en un conjunto completo de documentación de política que acompaña a esta política general de seguridad de la información.

Cada una de estas políticas es definida y acordada por una o más personas con competencia en el área relevante y, una vez aprobadas formalmente, se comunican a una audiencia apropiada, tanto dentro como fuera de la organización.

En la siguiente tabla se muestran las políticas individuales dentro del conjunto de documentación y se resume el contenido de cada política y el público objetivo de las partes interesadas.

Política	Áreas abordadas	Aplicación
Política de uso aceptable de Internet	Uso comercial de Internet, uso personal de Internet, administración de cuentas de Internet, seguridad y monitoreo y usos prohibidos del servicio de Internet.	Usuarios del servicio de Internet
Política en la nube	Diligencia debida, registro, configuración, gestión y eliminación de servicios en la nube.	Empleados involucrados en la adquisición y gestión de servicios en la nube.
Política de dispositivos móviles	Cuidado y seguridad de dispositivos móviles como laptops, tabletas y smartphones, ya sean proporcionados por la organización o por el individuo para uso empresarial.	Usuarios de dispositivos móviles proporcionados por la empresa y BYOD (Bring Your Own Device).
Política de teletrabajo	Consideraciones de seguridad de la información en el establecimiento y funcionamiento de un sitio y acuerdo de teletrabajo, por ejemplo, seguridad física, seguros y equipos.	Dirección y empleados implicados en la creación y mantenimiento de un centro de teletrabajo.
Política de control de acceso	Registro y baja de usuarios, provisión de derechos de acceso, acceso externo, revisiones de acceso, política de contraseñas,	Empleados involucrados en la configuración y administración del control de acceso.

Política	Áreas abordadas	Aplicación
	responsabilidades del usuario y control de acceso al sistema y a la aplicación.	
Política criptográfica	Evaluación de riesgos, selección de técnicas, implementación, pruebas y revisión de criptografía y gestión de claves.	Empleados involucrados en la configuración y gestión del uso de la tecnología y las técnicas criptográficas.
Política de Seguridad Física	Áreas seguras, seguridad del papel y de los equipos y gestión del ciclo de vida de los equipos.	Todos los empleados.
Política antimalware	Firewalls, antivirus, filtrado de spam, instalación y análisis de software, gestión de vulnerabilidades, formación de concienciación de usuarios, monitorización y alertas de amenazas, revisiones técnicas y gestión de incidentes de malware.	Empleados responsables de proteger la infraestructura de la organización contra el malware.
Política de copia de seguridad	Ciclos de copia de seguridad, copias de seguridad en la nube, almacenamiento externo, documentación, pruebas de recuperación y protección de medios de almacenamiento.	Empleados responsables de diseñar e implementar regímenes de copia de seguridad.
Política de software	Compra de software, registro, instalación y eliminación de software, desarrollo de software interno y uso de software en la nube.	Todos los empleados.
Política de Gestión de Vulnerabilidades Técnicas	Definición de vulnerabilidades, fuentes de información, parches y actualizaciones, evaluación de vulnerabilidades, endurecimiento y formación de concienciación.	Empleados responsables de proteger la infraestructura de la organización contra el malware.
Política de seguridad de la red	Diseño de seguridad de red, incluida la segregación de red, seguridad perimetral, redes inalámbricas y acceso remoto; Gestión de la seguridad de la red, incluidas las funciones y responsabilidades, el registro, la supervisión y los cambios.	Empleados responsables del diseño, implementación y gestión de redes.
Política de Mensajería Electrónica	Envío y recepción de mensajes electrónicos, supervisión de las instalaciones de mensajería electrónica y uso del correo electrónico.	Usuarios de servicios de mensajería electrónica.
Política de Desarrollo Seguro	Especificación de requisitos de negocio, diseño, desarrollo y pruebas de sistemas y desarrollo de software subcontratado.	Empleados responsables de diseñar, gestionar y escribir código para desarrollos de software a medida.

Política	Áreas abordadas	Aplicación
Política de Seguridad de la Información para las Relaciones con los Proveedores	Diligencia debida, acuerdos con proveedores, seguimiento y revisión de servicios, cambios, disputas y fin de contrato.	Empleados involucrados en el establecimiento y gestión de relaciones con proveedores.
Política de administración de disponibilidad	Requisitos de disponibilidad y diseño, supervisión y generación de informes, no disponibilidad, pruebas de planes de disponibilidad y gestión de cambios.	Empleados responsables del diseño de sistemas y la gestión de la prestación de servicios.
Política de cumplimiento de la propiedad intelectual y los derechos de autor	Protección de la propiedad intelectual, la ley, las sanciones y el cumplimiento de las licencias de software.	Todos los empleados.
Política de retención y protección de Registros	Período de retención para tipos específicos de registros, uso de criptografía, selección de medios, recuperación, destrucción y revisión de registros.	Empleados responsables de la creación y gestión de registros.
Política de Privacidad y Protección de Datos Personales	Legislación, definiciones y requisitos aplicables en materia de protección de datos.	Empleados responsables del diseño y la gestión de sistemas que utilizan datos personales.
Política de escritorio y pantalla limpias	Seguridad de la información mostrada en pantallas, impresa y almacenada en soportes extraíbles.	Todos los empleados.

Tabla 1. Políticas de la seguridad de la información

2.5 Aplicación de las políticas de la seguridad de la información

Las declaraciones de política hechas en este documento y en el conjunto de políticas de apoyo enumeradas en la Tabla 1 han sido revisadas y aprobadas por la alta dirección de TIMEWEB LATAM y deben cumplirse. El incumplimiento por parte de un empleado de estas políticas puede dar lugar a la adopción de medidas disciplinarias de acuerdo con el Proceso Disciplinario del Empleado de la organización.

Las preguntas relacionadas con cualquier política de TIMEWEB LATAM deben dirigirse en primera instancia al gerente de línea inmediata del empleado.

2.6 Publicación de las políticas de la seguridad de la información

TIMEWEB LATAM ha establecido que la política de alto nivel del SGSI se comunicará al personal interno a través de GOOGLE WORKSPACE y para las partes interesadas externas será a través de su página web https://timeweb.com.mx/

Las políticas que respaldan el cumplimiento de la política del SGSI serán comunicadas solo al personal interno y se realizará a través de la plataforma de GOOGLE WORKSPACE en formato electrónico no editable.

2.7 Revisión de la política del SGSI y las políticas de la seguridad de la información

Para asegurarse que las políticas del SGSI y de la SI se mantienen pertinentes e idóneas TIMEWEB LATAM ha establecido que por lo menos una vez al año se revisarán.

3. Control de cambios

Revisión	Fecha	Motivo del cambio
0	04-mar-2025	Documento de nueva creación derivado de la implementación del sistema de gestión de seguridad de la información bajo la norma ISO 27001:2022.