Departamento de Transformación e Innovación Tecnológica

DTI-PE-PL-01

Sistema de Gestión de Seguridad de la Información (SGSI)

Politica

Versión:03

18/03/2026

Estado	Aprobado

REGISTRO DE FIRMAS

Elaborado por	**Revisado por**	**Aprobado por**
Yanick Gomez Mejia	Richard Fernando Lira Miranda	Luis Guillermo Vivar Cortez
		
Fecha: 13/03/2026	Fecha: 13/03/2026	Fecha: 18/03/2026

VERSIÓN	FECHA	MODIFICACIONES
01	11/01/2022	Documento nuevo
02	06/03/2024	- En la politica se cambio las áreas responsables. Dirección de Desarrollo de Negocios a Área de Innovación y Soluciones de Negocios. Área de Innovación y Soluciones de Negocios (AISN) a Departamento de Transformación e Innovación Tecnologica (DTI)
03	18/03/2026	- Se modifico el área responsable: Área de Innovación y Soluciones de Negocios (AISN) a Gerencia Central de Innovación y Soluciones de Negocios - Se agrego la identificación del documento en el encabezado de la Politica.

En caso este documento se encuentra almacenado en un lugar distinto a la Plataforma KM de Tgestiona Servicios Globales SAC, se considera “Copia no controlada”

INDICE

1. OBJETO 4
2. AMBITO DE ALCANCE 4
3. RESPONSABILIDADES 4
4. DEFINICIONES 4
5. DOCUMENTOS DE REFERENCIA 4
6. DESCRIPCIÓN 5
6.1. POLITICA DE SEGURIDAD DE LA INFORMACIÓN 5
6.1.1. Propósito de la organización 5
6.1.2. Objetivos de seguridad de la información 5
6.1.3. Compromisos de la Dirección de la DDN 5
6.1.4. Recursos Humanos 5
6.1.5. Control de Accesos 6
6.1.6. Seguridad en las Operaciones y Comunicaciones 6
6.1.7. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información 7
6.1.8. Relación con Proveedores 7
6.1.9. Gestión de Incidentes de Seguridad 7
6.1.10. Gestión de Continuidad 7
6.1.11. Cumplimiento Normativo 8
6.1.12. Revisión periódica 8
6.1.13. Aprobación 8
6.2. DISPOSICIONES FINALES Y COMPLEMENTARIAS 8
7. FORMATOS 9
8. ANEXOS 9

En caso este documento se encuentra almacenado en un lugar distinto a la Plataforma KM de Tgestiona Servicios Globales SAC, se considera “Copia no controlada”

1. OBJETO

Definir las directrices de la Dirección respecto a la Seguridad de la Información, para la Gestión de Seguridad de la Información (SGSI) en Tgestiona Servicios Globales S.A.C.

2. AMBITO DE ALCANCE

El alcance es el Sistema de Gestión de Seguridad de la información de la plataforma EDI en los servicios de atención de incidencias y requerimientos, gestionados por la Gerencia Central de Innovación y Soluciones de Negocios y el Departamento de Transformación e Innovación Tecnológica (DTI), tal y como está definido en el manual DTI-PE-M-01.

3. RESPONSABILIDADES

Todo el personal: Cumple la Política definida en este documento.

4. DEFINICIONES

Ítem	Concepto	Descripción
1	Evento	Un suceso o serie de sucesos que pueden ser internos o externos a la empresa, originados por la misma causa, que ocurren durante el mismo periodo de tiempo.
2	Incidente de seguridad de información	Evento asociado a una posible falla en la política de seguridad, una falla en los controles, o una situación previamente desconocida relevante para la seguridad, que tiene una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
3	Información	Cualquier forma de registro electrónico, óptico, magnético o en otros medios similares, susceptible de ser procesada, distribuida y almacenada
4	Seguridad de la información:	Característica de la información que se logra mediante la adecuada combinación de políticas, procedimientos, estructura organizacional y herramientas informáticas especializadas a efectos que dicha información cumpla los criterios de confidencialidad, integridad y disponibilidad, definidos de la siguiente manera: I. Confidencialidad: La información debe ser accesible sólo a aquellos que se encuentren debidamente autorizados. II. Integridad: La información debe ser completa, exacta y válida. III. Disponibilidad: La información debe estar disponible en forma organizada para los usuarios autorizados cuando sea requerida.
5	Sistema de Gestión de Seguridad de la Información (SGSI)	Aquella parte del sistema de gestión general, basada en un enfoque de riesgos del negocio, para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información. El sistema de gestión incluye la estructura organizativa, políticas, actividades de panificación, responsabilidades, prácticas, procedimientos, procesos y recursos.

5. DOCUMENTOS DE REFERENCIA

- Estándar de Gestión de la Seguridad de la Información ISO/IEC 27001:2022

6. DESCRIPCIÓN

6.1. POLITICA DE SEGURIDAD DE LA INFORMACIÓN

6.1.1. Propósito de la organización

- La Organización es la Gerencia Central de Innovación y Soluciones de Negocios de la empresa Tgestiona Servicios Globales SAC (Tgestiona).
- Su propósito es brindar el Servicio de Gestión de Incidentes de la Seguridad de la Información a la empresa Tgestiona.

6.1.2. Objetivos de seguridad de la información

- Mejorar la Calidad del Servicio a los clientes.
- La Gerencia Central de Innovación y Soluciones de Negocios demuestra su compromiso con la Gestión de la Seguridad de la información.
- El personal de la Gerencia Central de Innovación y Soluciones de Negocios cumple la Política de Seguridad de la Información
- La organización cumple con los requisitos de la seguridad de la información
- La organización reduce el nivel de riesgos

6.1.3. Compromisos de Gerencia Central de Innovación y Soluciones de Negocios

- Satisfacer los requisitos de Seguridad de la Información de las partes interesadas. Lo cual incluye el cumplir con los requisitos legales aplicables.
- La mejora continua del sistema de gestión de la seguridad de la información.
- Comunicar esta política dentro de la organización por el portal de Recursos Humanos a todo el personal.
- Definir, aprobar, publicar y comunicar a los trabajadores y partes externas involucradas las políticas para la seguridad de la información.

6.1.4. Recursos Humanos

- La seguridad debe contemplarse desde las etapas de selección de personal, durante el desarrollo y al finalizar la relación laboral.
- Tgestiona asegurara que los colaboradores, contratistas y terceros entiendan sus responsabilidades y que éstas sean adecuadas según los roles para los que han sido calificados, reduciendo el riesgo de hurto, fraude o mal uso de los recursos de información, estableciendo para crear conciencias de las

En caso este documento se encuentra almacenado en un lugar distinto a la Plataforma KM de Tgestiona Servicios Globales SAC, se considera “Copia no controlada”

amenazas y riesgos en el ámbito de la seguridad de la información, preparándolos para sostener las Políticas de Seguridad de la empresa.

6.1.5. Control de Accesos

- Los permisos de acceso al sistema de mantenimiento de Edificios – EDI se otorgarán de modo que los usuarios tengan acceso únicamente a los recursos e información necesarios para el desempeño de sus funciones.
- Cualquier concesión de acceso a los recursos o servidores del sistema de Mantenimiento de Edificios – EDI llevará asociado un proceso formal de solicitud y aprobación.
- Todos los colaboradores, personal externo o subcontratado, así como que accedan a los activos de información del sistema de Mantenimiento de Edificios – EDI, deberán registrarse y asociarse a una cuenta única en el sistema.
- Todos los accesos realizados a los recursos o servicios del sistema de Mantenimiento de Edificios – EDI por los usuarios registrados llevarán asociado un proceso de identificación, autenticación de las credenciales de acceso y autorización. Se establecerán mecanismos de registro, monitorización de acceso y uso de los sistemas.
- Las credenciales de acceso de cada usuario serán personales e intransferibles.

6.1.6. Seguridad en las Operaciones y Comunicaciones

- Se establecerán y documentarán procedimientos para la gestión y operación correcta y segura de los recursos o servicios del sistema de Mantenimiento de Edificios – EDI.
- Se establecerán las medidas necesarias para mantener los entornos de Desarrollo y Producción separados e independientes, tanto desde el punto de vista del sistema de Mantenimiento de Edificios – EDI, como de los datos almacenados y procesados y del personal que accede a ellos, todo ello para mantener la seguridad de los datos reales de producción.
- En el caso de servicios externalizados, se impondrán controles técnicos, organizativos y/o contractuales específicos que contemplen los lineamientos expuestos en este documento.
- Se establecerán lineamientos y procedimientos de protección detectivos, preventivos y correctivos contra software malicioso, garantizando la actualización periódica y regular de los mismos.

En caso este documento se encuentra almacenado en un lugar distinto a la Plataforma KM de Tgestiona Servicios Globales SAC, se considera “Copia no controlada”

- Toda información que se transmita a través de redes de comunicaciones, públicas o privadas, deberá ser adecuadamente protegida mediante mecanismos de confidencialidad, autenticación, integridad, no repudio, control de tráfico y estrategias de segmentación y planificación de redes que tengan en cuenta los aspectos relativos a la seguridad de los datos del Sistema de Mantenimiento de Edificios – EDI.

6.1.7. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

- El desarrollo y mantenimiento del sistema de Mantenimiento de Edificios – EDI deberá incluir los controles y registros apropiados que garanticen la correcta implementación de las especificaciones de seguridad y se llevará a cabo teniendo en cuenta las mejores prácticas para el desarrollo seguro de software.

6.1.8. Relación con Proveedores

- Se establecerán acuerdos con los proveedores que permitan hacer frente a los riesgos de seguridad asociados a su contratación.
- Se mantendrá un nivel acordado de seguridad y de prestación de los servicios en concordancia con los acuerdos establecidos con proveedores.

6.1.9. Gestión de Incidentes de Seguridad

- Los eventos y debilidades en la seguridad de la información asociados con los recursos o servicios de información del sistema de Mantenimiento de Edificios – EDI deben ser comunicados oportunamente para que se realicen las acciones correctivas a tiempo.
- Se debe aplicar un proceso de mejora continua en respuesta al monitoreo, evaluación y gestión general de los incidentes en la seguridad de información. En el caso de que se requiera evidencia, ésta debe ser recolectada para asegurar el cumplimiento de los requisitos legales.

6.1.10. Gestión de Continuidad

- Se establecerá un proceso de gestión de continuidad tecnológica para garantizar la recuperación del sistema de Mantenimiento de Edificios – EDI en caso de falla reduciendo el tiempo de indisponibilidad a niveles aceptables desde el punto de vista de negocio mediante la adecuada combinación de controles de carácter organizativo, tecnológico y procedimental tanto preventivos como de recuperación.

En caso este documento se encuentra almacenado en un lugar distinto a la Plataforma KM de Tgestiona Servicios Globales SAC, se considera “Copia no controlada”

- El Plan de Continuidad Tecnológica del sistema de Mantenimiento de Edificios – EDI evaluará el riesgo y el impacto ocasionado por una falla, posibilitando una respuesta uniforme y coordinada, en el plazo previsto, a cualquier interrupción del sistema de Mantenimiento de Edificios – EDI, a fin de conseguir la continuidad esperada por la empresa.
- Los Procedimientos de Recuperación, establecerán las actividades de prevención, ejecución y recuperación.

6.1.11. Cumplimiento Normativo

- Tgestiona adquiere el compromiso de adaptar los recursos o servicios del sistema de Mantenimiento de Edificios – EDI a la normativa legal vigente, adoptando las medidas técnicas y organizativas necesarias, especialmente aquellas regulaciones legales relativas al tratamiento de los datos de carácter personal, registros contables, información privilegiada y el resguardo del secreto profesional.
- Se incluirán cláusulas y garantías en los acuerdos de nivel de servicio con las empresas subcontratadas que garanticen los requerimientos de servicio y seguridad exigidos por Tgestiona.
- Se establecerán las medidas necesarias para evitar la desactivación, accidental o malintencionada, de los mecanismos de seguimiento y auditoría.

6.1.12. Revisión periódica

- Las políticas de seguridad de la información deben ser revisadas anualmente o si ocurren cambios significativos, para garantizar su idoneidad, adecuación y efectividad continuos.

6.1.13. Aprobación

- La Gerencia Central de Innovación y Soluciones de Negocio aprueba la política de seguridad de la información
- Queda disponible como información documentada.

6.2. DISPOSICIONES FINALES Y COMPLEMENTARIAS

- El presente documento rige a partir del día siguiente a su publicación, quedando sin efecto todas las versiones anteriores, su contenido será revisado y/o modificado anualmente o ante un evento significativo.

En caso este documento se encuentra almacenado en un lugar distinto a la Plataforma KM de Tgestiona Servicios Globales SAC, se considera “Copia no controlada”

- Su incumplimiento estará sujeto a sanciones establecidas en el Reglamento Interno de Tgestiona.
- El Responsable de Seguridad es el único encargado de realizar cualquier modificación o cambio a este documento, previa coordinación con las áreas involucradas.

7. FORMATOS

No aplica

8. ANEXOS

No aplica

En caso este documento se encuentra almacenado en un lugar distinto a la Plataforma KM de Tgestiona Servicios Globales SAC, se considera “Copia no controlada”