Contiene los principales lineamientos establecidos por Tu Hogar con Estilo S.A. para ofrecer niveles razonables de protección a su información y sus activos. Este documento debe ser conocido y aplicado por todos los colaboradores que presten sus servicios a la empresa independiente de su modalidad de contratación.

**Modelo de Seguridad de la Información**

Tu Hogar con Estilo S.A.



Nivel de Confidencialidad: Uso Interno

Fecha de Publicación: Marzo de 2014

**Caracterización del Documento**

|  |  |
| --- | --- |
| Nombre del Documento: | Modelo de Seguridad de la Información |
| Nivel de Confidencialidad: | **Uso Interno:** Puede ser distribuido libremente entre los colaboradores de la empresa y no debe ser conocido por personal ajeno a ésta. |
| Codificación: | P-GSI-001 | Versión: | 2.0 |
| Fecha de última modificación: | 20-03-2014 | Fecha de Creación: | 14-04-2013 |
| Responsable del documento: | Oficial de Seguridad de la Información |
| Aprobado por: | Comité de Seguridad de la Información |

**Control de Versiones**

|  |  |  |  |
| --- | --- | --- | --- |
| Versión | Fecha | Elaborador por | Observaciones |
| 1.0 | 31-Oct-2013 | Andrés Augusto Jácome Lobo | Primera versión del documento |
| 1.1 | 31-Dic-2013 | Andrés Augusto Jácome Lobo | Ajustes de forma por revisión anual |
| 2.0 | 20-Mar-2014 | Andrés Augusto Jácome Lobo | Ajustes basados en requisitos de ISO/IEC 27001:2005 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

TABLA DE CONTENIDO

[1. INTRODUCCIÓN AL MODELO DE SEGURIDAD DE LA INFORMACIÓN 3](#_Toc383351176)

[2. ALCANCE DEL SGSI 3](#_Toc383351177)

[3. OBJETIVOS DEL SGSI 3](#_Toc383351178)

[4. CUMPLIMIENTO DE LA POLÍTICA 4](#_Toc383351179)

[5. MANTENIMIENTO DEL DOCUMENTO 4](#_Toc383351180)

[6. ROLES Y RESPONSABILIDADES DE SEGURIDAD DE LA INFORMACIÓN 4](#_Toc383351181)

[7. GOBIERNO DE SEGURIDAD DE LA INFORMACIÓN 6](#_Toc383351182)

[7.1. ESQUEMA DE GOBIERNO 6](#_Toc383351183)

[7.2. CONFORMACIÓN DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN 7](#_Toc383351184)

[8. COMPROMISO DE LA DIRECCIÓN CON LA SEGURIDAD DE LA INFORMACIÓN 8](#_Toc383351185)

[9. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN 8](#_Toc383351186)

[10. APROBACIÓN DEL DOCUMENTO 12](#_Toc383351187)

[ANEXO 1. TÉRMINOS Y DEFINICIONES 13](#_Toc383351188)

# INTRODUCCIÓN AL MODELO DE SEGURIDAD DE LA INFORMACIÓN

El Modelo de Seguridad de la Información es el conjunto de procesos, procedimientos, metodologías, principios, políticas, estándares y controles que Tu Hogar con Estilo S.A. ha adoptado para promover la implementación, mantenimiento y mejora continua de un Sistema de Gestión de Seguridad de la Información, basado en mejores prácticas tendientes a preservar la confidencialidad, integridad y disponibilidad de la información, y que nos permiten contar con lineamientos claros para mantener un entorno razonablemente seguro, apoyando los objetivos estratégicos del negocio.

Este modelo involucra todas las áreas de la organización, donde cada uno de los colaboradores, de acuerdo con sus funciones y rol en el negocio, será responsable en cierta medida por la protección de la información de la empresa y de sus clientes.

# ALCANCE DEL SGSI

La implantación del Sistema de Gestión de Seguridad de la información en la empresa debe ser realizada de forma gradual, acotada inicialmente a los procesos misionales y las sede definidas en el siguiente alcance, incluyendo la tecnología, el personal y los procesos de apoyo asociados:

El Sistema de Gestión de Seguridad de la Información (SGSI) de *Tu Hogar con Estilo S.A.* tiene como alcance los procesos de ***Venta de Productos y Servicios por Internet*** y ***Recibo, alistamiento y despacho de mercancía***, teniendo en cuenta para este último que su implantación se verá acotada al ***Centro de Distribución Principal*** de Costa Rica, ubicado en Alajuela y al ***Almacén Colonia del Rio***, ubicado en San José de Costa Rica.

# OBJETIVOS DEL SGSI

La presente Política tiene como objetivos establecer lineamientos generales en materia de seguridad de la información y declarar el compromiso de la empresa y sus directivos con el diseño, implantación y mantenimiento de un Sistema de Gestión de Seguridad de la Información que permita apalancar el negocio garantizando que la información de la empresa o de sus clientes se encuentre razonablemente protegida.

#

A continuación se presentan los principales objetivos del Sistema de Gestión de Seguridad de la Información, acotados en el alcance definido.

* Brindar niveles razonables de seguridad a la información que los clientes entregan a la empresa al realizar compra de productos o servicios por Internet, reduciendo la materialización de posibles amenazas que conlleven a la divulgación o modificación no autorizada de dicha información.
* Garantizar el cumplimiento de las diferentes normativas nacionales en materia de Seguridad de la información y protección de datos personales en los diferentes países en los que tiene presencia la empresa.
* Asegurar los procedimientos manuales o automatizados que involucran intercambio de información de clientes con los terceros contratados para la prestación del servicio de atención telefónica de quejas y reclamos (Call Center).
* Aumentar las ventas, el posicionamiento de la marca y mejorar la experiencia de compra de los clientes generando una sensación real de seguridad, confianza y respaldo al solicitar productos o servicios de la empresa por canales no presenciales.
* Ofrecer un canal estable y seguro que permita a los clientes relacionarse con la marca “Tu Hogar con Estilo” y adquirir sus productos o servicios a cualquier hora del día, cualquier día del año.

# CUMPLIMIENTO DE LA POLÍTICA

Los lineamientos definidos en la presente Política son de obligatorio cumplimiento y deben ser conocidos por todos los colaboradores que presten sus servicios a *Tu Hogar con Estilo S.A.*, ya sea en almacenes, bodegas como en sedes administrativas; así mismo, se debe aplicar a todos los empleados en modalidad de Outsourcing y demás terceros contratados por la empresa.

Cualquier incumplimiento de dichos lineamientos que resulte en una afectación a la confidencialidad, integridad o disponibilidad de la información será considerado una falta grave que conllevará al establecimiento de procesos disciplinarios o judiciales, y se tomarán las medidas necesarias, de acuerdo con la legislación nacional vigente.

# MANTENIMIENTO DEL DOCUMENTO

Este documento se debe actualizar por lo menos una vez al año o cuando ocurran cambios significativos del negocio o la legislación vigente en cada país donde tiene presencia Tu Hogar con Estilo S.A.

# ROLES Y RESPONSABILIDADES DE SEGURIDAD DE LA INFORMACIÓN

**Rol: Comité de Seguridad de la Información**

|  |
| --- |
| Responsabilidades |
| * Aprobar la Política General de Seguridad de la Información.
* Revisar el modelo de seguridad de la información por lo menos una (1) vez al año y solicitar los ajustes necesarios.
* Velar por la divulgación y actualización del modelo de seguridad de la información, incluyendo las Políticas definidas.
* Proveer de forma razonable los recursos necesarios para implementar, mantener y mejorar el Sistema de Gestión de Seguridad de la Información.
* Analizar y establecer acciones frente a incumplimientos de las políticas definidas.
 |

**Rol: Oficial de Seguridad de la Información**

|  |
| --- |
| Responsabilidades |
| * Mantener actualizado y vigente el modelo de seguridad de la información.
* Velar por la actualización, divulgación y concientización del modelo de seguridad de la información, incluyendo las Políticas definidas.
* Monitorear el nivel de implementación del SGSI y hacer seguimiento a las acciones correctivas y preventivas.
* Apoyar al negocio en la identificación de riesgos de Seguridad de la Información y la generación de los respectivos planes de acción para mitigarlos razonablemente.
* Reportar al Comité de Seguridad de la Información los incidentes y riesgos más relevantes en cuanto a la seguridad de la información.
 |

**Cargo: Todos los colaboradores**

|  |
| --- |
| Responsabilidades |
| * Conocer, cumplir y velar por el cumplimiento de la política de seguridad de la información.
* Velar por la protección de la información que manejan en el desempeño de sus responsabilidades.
* Reportar cualquier incumplimiento de la política de seguridad de la información o cualquier evento o situación relacionada con fuga o modificación no autorizada de información de la empresa o sus clientes.
 |

**Área: Vicepresidencia de Gestión Humana**

|  |
| --- |
| Responsabilidades |
| * Diseñar e implementar programas de capacitación y concientización sobre Seguridad de la Información y el cumplimiento de la política definida.
* Reportar en los tiempos establecidos cualquier novedad relacionada con la contratación del personal de Tu hogar con Estilo S.A., incluyendo vinculación, modificación de cargo, modificación de ubicación y desvinculación.
 |

**Área: Vicepresidencia de Tecnología**

|  |
| --- |
| Responsabilidades |
| * Diseñar, implementar y mantener controles tecnológicos que permitan proteger razonablemente la información de Tu Hogar con Estilo S.A.
* Apoyar la elaboración de las Políticas de Seguridad de la Información.
* Apoyar al Oficial de Seguridad de la Información en la gestión de incidentes de seguridad asociados con sistemas de información y recursos tecnológicos.
 |

**Área: Gerencia de Prevención Fraudes y Pérdidas**

|  |
| --- |
| Responsabilidades |
| * Diseñar, implementar y mantener controles de seguridad física que permitan proteger razonablemente la información y los activos de Tu Hogar con Estilo S.A.
* Apoyar la elaboración de las Políticas de Seguridad de la Información.
* Apoyar al Oficial de Seguridad de la Información en la gestión de incidentes de seguridad asociados con instalaciones y recursos físicos de la empresa.
 |

**Área: Auditoría Interna**

|  |
| --- |
| Responsabilidades |
| * Velar por el cumplimiento de la política de seguridad de la información en la organización.
* Identificar y reportar posibles debilidades en los procesos, procedimientos y recursos tecnológicos que permitan la materialización de riesgos asociados con la información.
 |

# GOBIERNO DE SEGURIDAD DE LA INFORMACIÓN

## ESQUEMA DE GOBIERNO

Tu Hogar con Estilo S.A. ha establecido el siguiente esquema de gobierno para Seguridad de la Información:

Nivel Táctico

Nivel Operativo

Auditoría

Nivel Estratégico

Se observa una pirámide de responsabilidades encabezada por el Comité de Seguridad de la Información en el nivel estratégico, seguida por el rol de Seguridad de la Información, liderado por el Oficial de Seguridad de la Información, con responsabilidades a nivel táctico, estratégico y en menor medida operativo, finalizando con los roles de Seguridad Informática y Seguridad Física, cuyas mayores responsabilidades están asignadas en el nivel táctico y operativo, y en menor medida a nivel estratégico. Todo el esquema de gobierno con sus procesos, roles y áreas involucradas es auditada de forma integral.

## CONFORMACIÓN DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

El Comité de Seguridad de la Información es el principal órgano del gobierno de seguridad de la información, encargado del direccionamiento estratégico de seguridad y de garantizar que la seguridad de la información se encuentra siempre alineada con los objetivos y estrategias del negocio.

Está conformado por miembros permanentes y opcionales, teniendo algunos participación solo en calidad de observadores y garantes de las decisiones tomadas al interior del comité (con voz pero sin voto). El comité sesiona como mínimo 1 vez cada 2 meses en la sede administrativa principal ubicada en Costa Rica y sus miembros corresponden a las cabezas visibles de las principales áreas del negocio y de aquellas encargadas de brindar soporte a la operación, adicionalmente de los encargados de las áreas Jurídicas y de Gestión Humana para velar por el cumplimiento legal y por los derechos y deberes de los colaboradores.

* **Integrantes permanentes**: Miembros con capacidad de toma de decisiones en el comité. Encargados adicionalmente de la concientización de las decisiones tomadas al interior de sus respectivas áreas. Sus miembros son:
* Presidente Corporativo
* Presidente Regional
* Vicepresidente de Operaciones
* Vicepresidente Comercial
* Vicepresidente de Tecnología
* Vicepresidente de Riesgo
* Vicepresidente Financiero
* Vicepresidente Jurídico
* Vicepresidente de Gestión Humana
* Jefe de Seguridad Informática
* **Observadores permanentes**: Miembros con la responsabilidad de asesorar y apoyar la toma de decisiones pero sin voto válido en esta.
* Oficial de Seguridad de la Información
* Auditor General
* Auditor de Sistemas

El Oficial de Seguridad de la Información al ser el encargado de liderar las propuestas y la agenda del Comité no tiene capacidad de voto en el mismo.

* **Invitados opcionales:** Corresponden a los líderes de otras áreas del negocio, consultores, auditores, proveedores y demás expertos requeridos de acuerdo al tema tratado en el comité. Al igual que los observadores están en capacidad de asesorar y apoyar la toma de decisiones pero no pueden participar con su voto en esta.

# COMPROMISO DE LA DIRECCIÓN CON LA SEGURIDAD DE LA INFORMACIÓN

Tu Hogar con Estilo S.A., reconoce que la información es un activo vital para la operación del negocio y por lo se compromete con su protección de acuerdo con su valor y sensibilidad, independientemente del medios en que se encuentre, velando por su confidencialidad, integridad y disponibilidad.

Adicionalmente la empresa:

* Da cumplimiento a todas las regulaciones, leyes y normativas vigentes relacionadas con Seguridad de la Información en cada país donde tiene presencia.
* Asignará razonablemente los recursos requeridos para la concepción, implementación, mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información.
* A través del Comité de Seguridad de la Información evaluará periódicamente el estado general del Sistema de Gestión de Seguridad de la Información, los principales riesgos identificados y hará seguimiento de alto nivel a los correspondientes planes de acción.

# POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

Reconoce como parte integral de la Política de Seguridad de la Información, a las políticas de alto nivel mencionadas a continuación y a todas las políticas de segundo nivel y procedimientos que provengan de éstas[[1]](#footnote-1).

**POLÍTICA 1. Organización de seguridad de la información**

Todos los colaboradores de Tu Hogar con Estilo S.A. y los terceros que presten servicios a ésta, deben conocer sus funciones y responsabilidades asociadas con la seguridad de la información de acuerdo con el rol que desempeñan en la empresa.

Políticas de segundo nivel relacionadas: Ver documento *P-GSI-002 – Detalle de Políticas de Seguridad de la Información*

* + Política 1-1. Comité de Seguridad de la Información
	+ Política 1-2. Revisión por la dirección

**POLÍTICA 2. Protección de la información**

La información y los recursos informáticos del negocio son activos vitales y por lo tanto deben ser identificados, clasificados y protegidos, identificando, evaluando y mitigando los riesgos relacionados con su confidencialidad, integridad y disponibilidad de forma consistente con su valor para el negocio.

Políticas de segundo nivel relacionadas: Ver documento *P-GSI-002 – Detalle de Políticas de Seguridad de la Información*

* + Política 2-1. Uso razonable de los activos de la empresa
	+ Política 2-2. Responsables de la información
	+ Política 2-3. Administración del riesgo en seguridad de la información
	+ Política 2-4. Protección de información confidencial
	+ Política 2-5. Validación de integridad de la información
	+ Política 2-6. Destrucción segura de información
	+ Política 2-7. Escritorio limpio y pantalla despejada
	+ Política 2-8. Segregación de funciones
	+ Política 2-9. Control de dispositivos de almacenamiento extraíble

**POLÍTICA 3. Cumplimiento de regulaciones**

Tu Hogar con Estilo S.A. debe cumplir con las regulaciones nacionales de privacidad, seguridad de la información y propiedad intelectual.

Políticas de segundo nivel relacionadas: Ver documento *P-GSI-002 – Detalle de Políticas de Seguridad de la Información*

* + Política 3-1. Asignación de derechos de propiedad intelectual
	+ Política 3-2. Uso de software e información sujeta a derechos de autor
	+ Política 3-3. Restricción de uso de datos personales

**POLÍTICA 4. Seguridad en el recurso humano**

Tu Hogar con Estilo S.A. debe velar por que los colaboradores conozcan y cumplan con sus responsabilidades en seguridad de la información desde su vinculación.

Políticas de segundo nivel relacionadas: Ver documento *P-GSI-002 – Detalle de Políticas de Seguridad de la Información*

* + Política 4-1. Capacitación y creación de cultura en seguridad de la información
	+ Política 4-2. Acuerdos de confidencialidad
	+ Política 4-3. Requisitos de seguridad en contratos con terceros

**POLÍTICA 5. Control de Acceso**

Los privilegios de acceso de colaboradores o terceros, desde o hacia los recursos informáticos de Tu Hogar con Estilo S.A. deben ser otorgados solo a los usuarios autorizados, concediendo lo mínimo requerido para el cumplimiento de sus responsabilidades con la empresa.

Políticas de segundo nivel relacionadas: Ver documento *P-GSI-002 – Detalle de Políticas de Seguridad de la Información*

* + Política 5-1. Definición de perfiles de acceso, asignación y retiro de privilegios
	+ Política 5-2. Revisión periódica de privilegios de acceso
	+ Política 5-3. Identificación y autenticación de usuarios en recursos informáticos
	+ Política 5-4. Uso personalizado del identificador de usuario
	+ Política 5-5. Usuarios privilegiados y usuarios genéricos
	+ Política 5-6. Acceso remoto
	+ Política 5-7. Conexión segura de terceros a la red
	+ Política 5-8. Acceso restringido a servicios de Internet

**POLÍTICA 6. Plan de contingencia y continuidad**

Todos los procesos críticos y sus recursos informáticos asociados, deben contar con un plan de contingencia y continuidad del negocio de tal forma que se garantice razonablemente su disponibilidad.

Políticas de segundo nivel relacionadas: Ver documento *P-GSI-002 – Detalle de Políticas de Seguridad de la Información*

* + Política 6-1. Seguridad del plan de contingencia y continuidad
	+ Política 6-2. Usuarios de contingencia
	+ Política 6-3. Respaldo de información crítica
	+ Política 6-4. Pruebas sobre el plan de contingencia y continuidad

**POLÍTICA 7. Seguridad Física**

Todas las instalaciones físicas donde se procesa o almacena información de Tu Hogar con Estilo S.A. o de sus clientes, deben tener un nivel de seguridad acorde con su clasificación.

Políticas de segundo nivel relacionadas: Ver documento *P-GSI-002 – Detalle de Políticas de Seguridad de la Información*

* + Política 7-1. Control de acceso y perímetro de las instalaciones
	+ Política 7-2. Gestión de amenazas ambientales
	+ Política 7-3. Manejo de áreas de carga y descarga
	+ Política 7-4. Protección física de equipos de cómputo
	+ Política 7-5. Seguridad en el cableado
	+ Política 7-6. Protección contra fallos del suministro eléctrico

**POLÍTICA 8. Seguridad en Redes y Telecomunicaciones**

Se implementarán razonablemente los controles sobre la red de datos y los enlaces de telecomunicaciones que permitan limitar que los colaboradores solo utilicen aquellos servicios requeridos para el cumplimiento de sus responsabilidades.

Políticas de segundo nivel relacionadas: Ver documento *P-GSI-002 – Detalle de Políticas de Seguridad de la Información*

* + Política 8-1. Segregación de redes y control de enrutamiento en la red
	+ Política 8-2. Intercambio de información con terceros
	+ Política 8-3. Uso de barreras de comunicaciones
	+ Política 8-4. Seguridad en el correo electrónico
	+ Política 8-5. Separación de ambientes de desarrollo, prueba y producción

**POLÍTICA 9. Seguridad en Sistemas de Información**

Durante las etapas de adquisición, desarrollo y mantenimiento de Sistemas de Información se deben incluir los parámetros, lineamientos y estándares definidos por seguridad de la información.

Políticas de segundo nivel relacionadas: Ver documento *P-GSI-002 – Detalle de Políticas de Seguridad de la Información*

* + Política 9-1. Especificación de requisitos de seguridad
	+ Política 9-2. Control de cambios
	+ Política 9-3. Compra o arrendamiento de software o Sistemas de Información
	+ Política 9-4. Validación de datos de entrada en los sistemas de información
	+ Política 9-5. Controles criptográficos en los sistemas
	+ Política 9-6. Protección del código fuente
	+ Política 9-7. Gestión de vulnerabilidades de los sistemas
	+ Política 9-8. Respaldo de información

**POLÍTICA 10. Gestión de Incidentes de Seguridad de la Información**

Todo incidente o alerta de seguridad debe ser tratado de principio a fin, hasta su solución definitiva.

Políticas de segundo nivel relacionadas: Ver documento *P-GSI-002 – Detalle de Políticas de Seguridad de la Información*

* + Política 9-1. Reporte de incidentes de seguridad de la información
	+ Política 9-2. Reporte de debilidades de la seguridad de la información
	+ Política 9-3. Recopilación de evidencias
	+ Política 9-4. Valoración de impacto en incidentes de Seguridad de la información

# APROBACIÓN DEL DOCUMENTO

La presente política se aprueba a los 20 días del mes de marzo de 2014 por el Comité de Seguridad de la Información cuyos miembros firman a continuación.

En calidad de integrantes permanentes del comité firman:

Presidente Corporativo Presidente Regional Costa Rica

Vicepresidente Comercial Vicepresidente de Operaciones

Jefe de Seguridad Informática Vicepresidente de Tecnología

Vicepresidente de Riesgo Vicepresidente Financiero

Vicepresidente Jurídico Vicepresidente de Gestión Humana

En calidad de observadores del comité firman:

Oficial de Seguridad de la Información

 Auditor General Auditor de Sistemas

# ANEXO 1. TÉRMINOS Y DEFINICIONES

| **TERMINO** | **DEFINICIÓN** |
| --- | --- |
| **Acceso remoto** | Acceso realizado por medio de redes de telecomunicaciones que puedan llegar a ser susceptibles a interceptación de información. Algunos ejemplos de este tipo de redes son: Internet, enlaces de datos dedicados no cifrados, redes inalámbricas, redes celulares de datos. |
| **Colaboradores** | Personas que prestan sus servicios a Tu Hogar con Estilo S.A. mediante vinculación laboral directa, temporal, o mediante la modalidad de Outsourcing de personal. |
| **Incidente de Seguridad** | Evento no deseado que compromete la Confidencialidad, Integridad o Disponibilidad de la información. |
| **Información** | Conjunto de datos que tiene un significado, propósito y utilidad. |
| **Perfil** | Conjunto de privilegios de acceso a la información definidos para cumplir con ciertas funciones o responsabilidades en la empresa.  |
| **Recursos informáticos** | Concepto utilizado para enmarcar los siguientes recursos tecnológicos: servidores, equipos de cómputo, dispositivos móviles, dispositivos de infraestructura, aplicaciones y sistemas de información. |

1. Las políticas de segundo nivel se mencionan a manera de índice en este documento y se desarrollan en documentos adicionales. [↑](#footnote-ref-1)