1. INTRODUCCIÓN

En el contexto de la transformación digital y los riesgos de ciberseguridad asociados el Directorio de CASA TRES define como un objetivo primario la seguridad de la información que gestiona para preservar su confidencialidad, integridad y disponibilidad.

CASA TRES reconoce la importancia de identificar y proteger los activos de información como parte esencial en la conducción y consecución de sus objetivos estratégicos y la prestación de sus servicios.

Para ello, evitará la destrucción, divulgación, modificación y utilización no autorizada de toda información, comprometiéndose a desarrollar, implantar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información.

El Directorio de CASA TRES declara su compromiso con el cumplimiento de la normativa la norma ISO/IEC 27001:2022 y las recomendaciones del estándar ISO 27002:2022 en relación con los aspectos de seguridad de la información.

Se tendrá en cuenta la legislación vigente y demás regulaciones aplicables (Ley 18.331 de Datos Personales).

La Seguridad de la Información es la preservación de su:

- confidencialidad, asegurando que sólo quienes estén autorizados puedan acceder a la información.
- integridad, asegurando que la información y sus métodos de proceso sean exactos y completos.
- disponibilidad, asegurando que los usuarios autorizados tengan acceso a la información cuando lo requieran.

2. POLÍTICA GENERAL DE CASA TRES (5.1, 5.4)

Es política de CASA TRES

1. Definir, desarrollar, implementar y mantener un Sistema de gestión de seguridad de la información como la herramienta para minimizar los riesgos de exposición de la información, comprometiéndose a **brindar los recursos** para mantener vigente el mismo a través de mejora continua.
2. Establecer como prioritario la protección de la información de sus clientes.
3. **Manual de políticas de Seguridad de la Información**: Adicionalmente, se establecerán políticas específicas de seguridad de la información las cuales se fundamentan en los controles y objetivos de control del Anexo A de la norma internacional ISO 27001.
4. La seguridad de la información (ciberseguridad en cuanto a medios digitales), se consigue implantando un conjunto adecuado de controles, los que se justifican a través de un análisis de los riesgos a los que se ve expuesta. (Ver “SOA CASA TRES”)

5. Dar cumplimiento a los controles incluidos en el **SOA** (Enunciado de aplicabilidad) basado en el Apéndice A norma UNIT ISO/IEC 27001:2022. Establecer una cultura positiva de seguridad de la información y garantizar el cumplimiento de los requerimientos legales, contractuales, regulatorios y de negocio vigentes.
6. La Política de Seguridad de la Información, se integrará a la normativa básica de la Empresa, incluyendo su difusión previa, y la instrumentación de las medidas sancionatorias correspondientes por incumplimiento de esta referidas en el **código de conducta de la empresa.**
7. CASA TRES se compromete a divulgar la presente Política de Seguridad de la Información, a fin de su debido conocimiento por parte del personal y a los efectos de que sea cumplida por todo el personal de la Empresa, independientemente del cargo que se desempeñe y de la naturaleza jurídica del vínculo funcional.
8. **Brindar concientización y formación** en materia de seguridad de la información a todo el personal.

3. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (5.2)

1. Designar un Responsable de la Seguridad de la Información (RSI), quien se encargará del mantenimiento, implementación y el desarrollo del Sistema de Gestión de Seguridad de la Información.

2. Designar un Comité de Seguridad de la Información (CSI), de integración multidisciplinaria que, a través de sus representantes, personal vinculado a temas de seguridad de la información. Ver ANEXO II: Reglamento de funcionamiento del Comité de Seguridad de la Información.

3. El Comité –que reportará directamente Directorio a través del Responsable de SI como coordinador- tendrá como cometido el desarrollo y mantenimiento de las políticas aprobadas, así como las propuestas de modificación y actualización de estas. También tendrá como objetivo el establecimiento la aprobación de un Plan de Acción anual en material de Seguridad de la Información.

4. SEGREGACIÓN DE FUNCIONES (5.3)

Deben separarse las funciones incompatibles y las áreas de responsabilidad incompatibles en la medida de lo razonablemente practicable, incorporando controles compensatorios si fuera necesario.

5. TRATAMIENTO DE LOS RIESGOS Y OTROS

1. Desarrollar un proceso de identificación, evaluación y tratamiento de riesgos de seguridad, y de acuerdo con su resultado implementar las acciones de control y mitigación correspondiente, así como elaborar y actualizar el plan de acción.
2. Establecer objetivos anuales con relación a la Seguridad de la Información.

3. Clasificar y proteger la información de acuerdo con la normativa vigente y con los criterios de valoración en relación con la importancia que posee para la Empresa.
4. Cumplir con los requisitos del servicio, legales o reglamentarios y las obligaciones contractuales de seguridad,
5. Adoptar una política de gestión de incidentes de seguridad para un adecuado tratamiento de estos.
6. Establecer que todo el personal es responsable de registrar y reportar los incidentes a la seguridad, confirmados o sospechas de acuerdo con los procedimientos correspondientes.
7. Brindar los medios necesarios para garantizar la continuidad de las operaciones de la Empresa.
8. La presente Política de Seguridad de la Información debe ser cumplida por todo el personal de CASA TRES, independiente del cargo que desempeñe y de su situación contractual.

6. CONTACTOS CON AUTORIDADES Y GRUPOS DE INTERÉS DE SEGURIDAD (5.5, 5.6)

El Responsable de SI debe mantener contactos con autoridades relevantes vinculadas directa o indirectamente con la seguridad de la información y con grupos de interés especial o foros especializados en seguridad, con el propósito de establecer inteligencia contra las amenazas para lo cual debe:

1. Incrementar el conocimiento sobre las mejores prácticas y mantenerse al día con la información relevante sobre seguridad;
2. Garantizar que la comprensión de la realidad en materia de seguridad de la información es actual y completa;
3. Recibir advertencias adecuadas de alertas, avisos y actualizaciones de seguridad referidos a ataques o vulnerabilidades;
4. Compartir e intercambiar información sobre nuevas tecnologías, productos, amenazas o vulnerabilidades;
5. Proveer puntos adecuados de enlace para el manejo de incidentes de seguridad de la información.

7. SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS (5.8)

Se debe Integrar la seguridad de la información en el método de gestión de proyectos de la empresa para garantizar que los riesgos de seguridad de la información sean identificados y tratados como parte del proyecto, independientemente del tipo de proyecto, así como la consideración de los requisitos de seguridad de la información en forma temprana.

8. INTELIGENCIA DE AMENAZAS (5.7)

La investigación en inteligencia de amenazas ayuda a una organización a comprender los riesgos cibernéticos y los pasos necesarios para mitigar tales riesgos. Es responsabilidad del Encargado de Seguridad mantenerse informado y actualizado en cuanto a las nuevas amenazas y estrategias de ataques, vectores de ataques, para una adecuada gestión de la Ciberseguridad.

9. INCUMPLIMIENTO A LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

El incumplimiento de esta política podrá dar lugar a acciones disciplinarias por parte de la Dirección que puede variar de acuerdo con lo establecido en el Código de Conducta pudiendo incluso tener como consecuencia la desvinculación de la empresa.

Las violaciones a la seguridad de los sistemas de información pueden originar responsabilidad penal y/o civil. CASA TRES investigará todos los hechos relacionados con dichas violaciones y cooperará con la aplicación de la ley si se sospecha que ha ocurrido una violación de las leyes penales.

ANEXO I: GLOSARIO

Aceptación del riesgo: decisión informada de aceptar un riesgo particular. [ISO 73:2009].

Activos de información: Son aquellos datos o información que tienen valor para una organización. [Decreto N° 451/009 de 28 de Setiembre 2009 – Art.3 Definiciones]

Amenaza: causa potencial de un incidente no deseado, que puede dar lugar a daños en un sistema o una organización. [UNIT- ISO/IEC 27000:2014].

Confidencialidad: propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados. [UNIT- ISO/IEC 27000:2014].

Custodio de la Información: rol que recae sobre la persona o grupo de personas que proveen un alto nivel de confianza y a los cuales se les deja en posesión y responsabilidad, delegada por su propietario, de velar por la seguridad de la información que no les pertenece.

Disponibilidad: propiedad de ser accesible y utilizable por solicitud de una entidad autorizada [UNIT-ISO/IEC 27000:2014].

Evaluación de riesgos: proceso para comprender la naturaleza de un riesgo y determinar su nivel de riesgo. [UNIT- ISO/IEC 27000:2014].

Evento de seguridad de la información: ocurrencia identificada de un estado de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de controles, o una situación previamente desconocida que pueda ser relevante para la seguridad. [UNIT- ISO/IEC 27000:2014].

Gestión de incidentes de Seguridad de la información: procesos para la detección, notificación, evaluación, respuesta, tratamiento, y aprendizaje de incidentes de seguridad de la información. [UNIT- ISO/IEC 27000:2014].

Incidente de Seguridad de la Información: evento o serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información. [UNIT- ISO/IEC 27000:2014].

Incidente de seguridad informática: violación o amenaza inminente de violación a una política de seguridad de la información implícita o explícita, así como un hecho que compromete la seguridad de un sistema (confidencialidad, integridad o disponibilidad). [Decreto N° 451/009 de 28 de Setiembre 2009- Art.3 Definiciones]

Integridad: propiedad de exactitud y completitud. [UNIT- ISO/IEC 27000:2014].

Propietario de los activos de información: persona o entidad que rinde cuentas y tiene autoridad sobre los activos de información.

Proyecto SGSI: actividades estructuradas conducidas por una organización para implementar un SGSI. [UNIT- ISO/IEC 27000:2014].

Riesgo: efecto de incertidumbre sobre los objetivos [UNIT- ISO/IEC 27000:2014].

Seguridad de la Información: preservación de la confidencialidad, integridad y disponibilidad de la información. [UNIT- ISO/IEC 27000:2014].

SGSI: Sistema de Gestión de Seguridad de la Información.

Sistema de información: aplicaciones, servicios, activos de tecnología de la información o cualquier otro componente que maneje información. [UNIT- ISO/IEC 27000:2014].

Valoración de riesgos: proceso de comparación de resultados de un análisis de riesgos con los criterios de riesgo para determinar si el riesgo o su magnitud es aceptable o tolerable. [UNIT- ISO/IEC 27000:2014].

Vulnerabilidad: debilidad de un activo o control que puede ser explotada por una o más amenazas. [UNIT- ISO/IEC 27000:2014].

ANEXO II: REGLAMENTO DE FUNCIONAMIENTO DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

- El Comité sesionará al menos una vez al año o cada vez que sea necesario para tratar asuntos vinculados a la Seguridad de la Información, incidentes, nuevos requisitos legales, etc.
- Integración del Comité de Seguridad de la Información (CSI)
    - Un representante de la Dirección o en quien la misma delegue
    - Contador de la empresa
    - Encargado de Seguridad de la Información
    - Encargado de Sistemas
    - Encargado de Gestión Humana
- Cualquiera de sus integrantes podrá convocar a una sesión extraordinaria del CSI para tratar asuntos relevantes vinculados a la Seguridad de la Información
- El Comité será liderado por el Responsable de Seguridad de la Información.
- Se elaborará un acta dejando constancia de los asuntos resueltos, siendo el Responsable de Seguridad quien deberá hacer un seguimiento de los mismos.

10. HISTORIAL DE REVISIONES

Fecha	Responsable	Descripción	Aprobación	Versión
30/Oct/2022	Jesús González Andrea Parada	Revisión anual Ajuste a versión ISO/IEC 27002:2022	Comité de Seguridad de la información	1.0
30/Nov/2023	Andrea Parada	Revisión anual y cambio de denominación “Política Empresarial…” por “Política Organizacional…”	Comité de Seguridad de la información	2.0