CASA TRES

CONTACT CENTER

POLÍTICA ORGANIZACIONAL DE SEGURIDAD DE LA INFORMACIÓN

Dirección: Av. Rondeau 1715 (Montevideo - Uruguay) | Teléfono: 2924 3333 | www.casatres.com.uy

1. Introducción

En el marco de la transformación digital y los desafíos que esta implica, el Directorio de CASA TRES establece como objetivo prioritario la protección de la información que gestiona, preservando su confidencialidad, integridad y disponibilidad.

CASA TRES reconoce que la identificación, valoración y resguardo de los activos de información son elementos fundamentales para el cumplimiento de sus objetivos estratégicos y la prestación eficaz de sus servicios, independientemente del formato o medio en que dicha información se encuentre.

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 y las recomendaciones del estándar ISO 27002 en relación con los aspectos de seguridad de la información.

Se tendrá en cuenta la legislación vigente y demás regulaciones aplicables en materia de seguridad de la información, protección de datos personales y continuidad del negocio. Entre ellas, la Ley N.º 18.331 de Protección de Datos Personales y normas asociadas, así como cualquier otra normativa aplicable a las actividades de la organización. Los requisitos legales y reglamentarios aplicables al SGSI se encuentran documentados en el “Listado de requisitos legales y reglamentarios aplicables al SGSI”.

La Seguridad de la Información se entiende como el conjunto de medidas y prácticas orientadas a preservar:

- **La confidencialidad**, limitando el acceso a la información únicamente a personas autorizadas.
- **La integridad**, manteniendo la exactitud y completitud de la información y sus métodos de procesamiento.
- **La disponibilidad**, procurando que los usuarios autorizados puedan acceder a la información cuando lo necesiten.

Este enfoque permite gestionar los riesgos que afectan a los activos de información, contribuyendo al cumplimiento de los objetivos estratégicos de la organización y al fortalecimiento de la confianza de las partes interesadas.

2. Política general de casa tres (5.1, 5.4)

Es política de CASA TRES

1. Definir, desarrollar, implementar y mantener un SGSI 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. 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 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 ISO/IEC 27001. Establecer una cultura positiva de seguridad de la información y velar por el cumplimiento de los requerimientos legales, contractuales, regulatorios y de negocio vigentes.
6. La Política Organizacional 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 Organizacional 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 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 RSI 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 promover 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 RSI debe mantener vínculos activos con autoridades relevantes, grupos de interés y foros especializados en seguridad de la información, con el propósito de fortalecer la inteligencia frente a amenazas. Para ello, deberá:

1. Mantenerse actualizado sobre buenas prácticas, tendencias y novedades relevantes en materia de seguridad de la información.
2. Promover una comprensión clara y actualizada del entorno de amenazas y vulnerabilidades que puedan afectar a la organización.
3. Recibir y gestionar alertas, avisos y actualizaciones sobre incidentes, vulnerabilidades o riesgos emergentes.
4. Intercambiar información técnica y estratégica sobre tecnologías, productos, amenazas y vulnerabilidades con actores relevantes.
5. Actuar como punto de contacto para la coordinación y gestión 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 promover 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 a la seguridad de la información y los pasos necesarios para mitigarlos. Es responsabilidad del RSI mantenerse informado y actualizado sobre nuevas amenazas,
estrategias y vectores de ataque, para una adecuada gestión de la seguridad de la información.

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.

10. Referencias

- SOA CASA TRES
- LIST-001 Listado de requisitos legales y reglamentarios aplicables al SGSI

11. Anexos

- ANEXO I: Glosario
- ANEXO II: Reglamento de funcionamiento del comité de seguridad de la información

Historial de revisiones

Fecha	Responsable	Descripción	Aprobación	Versión
30/10/2022	Jesús González Andrea Parada	Revisión anual Ajuste a versión ISO/IEC 27002	Comité de Seguridad de la información	1.0
30/11/2023	Andrea Parada	Revisión anual y cambio de denominación “Política Empresarial…” por “Política Organizacional…”	Comité de Seguridad de la información	2.0
20/09/2024	Jesús González	Revisión	Comité de Seguridad de la información	2.1
20/05/2025	Jesús González	Se incluye referencia a Listado de requisitos legales aplicables al SGSI	Comité de Seguridad de la información	2.2
18/11/2025	Jesús González	Actualización de Glosario	Comité de Seguridad de la información	2.3

Aceptación del riesgo: Decisión informada de asumir un riesgo, tomada en base a criterios establecidos. [ISO 31073].

Activos de información: "Todos los elementos físicos, virtuales, tangibles o intangibles que tienen valor para la organización y para el propósito de garantizar la seguridad de la información". [ISO/IEC 27001].

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

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

CSI: Comité de Seguridad de la Información

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 [ISO/IEC 27000].

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

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. [ISO/IEC 27000].

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. [ISO/IEC 27000].

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. [ISO/IEC 27000].

Incidente de seguridad informática: incidente de seguridad de la información evento o eventos de seguridad de la información relacionados e identificados que pueden dañar los activos de una organización o comprometer sus operaciones. [ISO/IEC 27035-1].

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

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. [ISO/IEC 27000].

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

RSI: Responsable de Seguridad de la Información

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

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. [ISO/IEC 27000].

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. [ISO/IEC 27000].

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

- El CSI 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 CSI
    - Un representante de la Dirección o en quien la misma delegue
    - Contador de la empresa
    - RSI
    - 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 CSI será liderado por el RSI.
- Se elaborará un acta dejando constancia de los asuntos resueltos, siendo el RSI quien deberá hacer un seguimiento de los mismos.