CASA TRES
CONTACT CENTER

POLÍTICA EMPRESARIAL DE SEGURIDAD DE LA INFORMACIÓN

Fecha	Responsable	Descripción	Aprobación	Acta
Marzo 2015	Adrian Hitateguy	Creación	Gcia. Gral.	
Marzo 2016	Adrian Hitateguy	Revisión Anual	Gcia. Gral.	
18 Marzo 2017	Cristina Ledesma	Revisión anual, creación de roles	Comité de Seguridad	
Diciembre 2019	Roberto Auliso Andrea Parada	Revisión anual	Comité de Seguridad	
Diciembre 2020	Jesús González Andrea Parada	Revisión anual	Comité de Seguridad	
Abril 2022	Andrea Parada Jesús Gonzalez	Revisión anual	Comité de Seguridad	
Marzo 2023	Andrea Parada Jesús Gonzalez	Revisión anual	Comité de Seguridad	

Contenido

1. Introducción

En el contexto de la transformación digital 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 CONTACT CENTER 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 27001:2013 y las recomendaciones del estándar ISO 27002:2013 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.

CASA TRES CONTACT CENTER establece como prioritario la protección de la información de sus clientes, así como el cumplimiento de los requisitos de seguridad establecidos por los mismos, a través de un monitoreo constante y la toma de medidas preventivas y de contención ante un incidente de ciberseguridad.

Consciente de las necesidades actuales, CASA TRES implementa un modelo de gestión de seguridad de la información como la herramienta que permite identificar y minimizar los riesgos a los cuales se expone la información, ayudando a la reducción de costos operativos y financieros, establece una cultura de seguridad de la información y garantizando el cumplimiento de los requerimientos legales, contractuales, regulatorios y de negocio vigentes.

Para asegurar el objetivo de seguridad de la información de la Empresa, es propósito de CASA TRES la implantación de un Sistema de gestión de seguridad de la información, identificando los eventos que puedan impactar en este objetivo, adecuado los controles en dicha materia, tales como políticas, procedimientos, estructuras organizativas si fuera necesario, software e infraestructura.

CASA TRES ha designado un Comité de Seguridad de la Información, de integración multidisciplinaria que, a través de sus representantes, involucra a todas las áreas de la empresa. Dicho Comité –que reportará directamente Directorio a través de su coordinador- tendrá como cometido el desarrollo y mantenimiento de las políticas aprobadas, así como las propuestas de modificación y actualización de estas.

Del mismo modo, ha designado un Responsable de la Seguridad de la Información, quien se encargará de la guía, implementación y el mantenimiento del Sistema de Gestión de Seguridad de la Información.

CASA TRES se compromete a divulgar la presente Política de Seguridad de la Información, a fin de su debido conocimiento 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, así como también a las partes interesadas.

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.

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 UNIT ISO/IEC 27001. 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.

2. Política General de Seguridad de la Información:

Es política de CASA TRES en materia de Seguridad de la Información:

1. Establecer objetivos anuales con relación a la Seguridad de la Información.

2. 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.

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. Brindar concientización y formación en materia de seguridad de la información a todo el personal.

6. Adoptar una política de gestión de incidentes de seguridad para un adecuado tratamiento de estos.

7. Establecer que los empleados, personal externo, proveedores y todos aquellos que tengan responsabilidades sobre las fuentes, repositorios y recursos de procesamiento de la información de CASA TRES, deben cumplir con la normativa en la materia garantizando la confidencialidad de la misma

8. CASA TRES designa un Responsable de la Seguridad de la Información, quien se encarga del desarrollo, la implementación y el mantenimiento del Sistema de Gestión de Seguridad de la Información.

9. Se establece la conformación de un Comité de Seguridad de la Información que deberá de realizar una revisión de las políticas de Seguridad de la Información anualmente o cuando se considere pertinente.

10. 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.

11. Establecer que todo el personal es responsable de registrar y reportar las violaciones a la seguridad, confirmadas o sospechadas de acuerdo con los procedimientos correspondientes.

12. Brindar los medios necesarios para garantizar la continuidad de las operaciones de la Empresa.

3. Compromiso de la Dirección

La Dirección de CASA TRES demuestran su compromiso a través de:

- La revisión y aprobación de las Políticas de Seguridad de la Información contenidas en varios documentos.
- La promoción activa de una cultura de ciberseguridad.
- El aseguramiento de los recursos adecuados para implementar y mantener el Sistema de Gestión de Gestión de Seguridad de la Información (SGSI)
- La verificación del cumplimiento de las políticas definidas y los requerimientos regulatorios que apliquen.

4. Sanciones a las violaciones a la Políticas de Seguridad de la Información

Las Políticas de Seguridad de la Información pretenden instituir y afianzar la cultura de seguridad de la información entre los funcionarios, personal externo y proveedores de CASA TRES. Por tal razón, es necesario que las violaciones a las Políticas Seguridad de la Información sean clasificadas, con el objetivo de aplicar medidas correctivas conforme con los niveles de clasificación definidos y mitigar posibles afectaciones contra la seguridad de la información. Las medidas correctivas pueden considerar desde acciones administrativas, hasta acciones de orden disciplinario o penal, de acuerdo con las circunstancias, si así lo ameritan y de acuerdo con el marco legal vigente. Por mayor información ver documento con código de conducta de CASATRES.

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].