Versión: 2

Fecha de aprobación: 12/06/14

Proceso responsable: Tecnología

Aprobado por: Comité Directivo

Política de Seguridad de la información

- **Política de Seguridad de la información**

Política de Seguridad de la información

Establecer todas aquellas medidas organizacionales, técnicas, físicas y legales necesarias para proteger los activos de información contra acceso no autorizado, divulgación, duplicación, interrupción de sistemas, modificación, destrucción, pérdida, robo, o mal uso, que se pueda producir en forma intencional o accidental.

A través de esta política se difunden los objetivos de Seguridad de la información de CELSIA, que se consiguen con la aplicación de sus respectivos controles para gestionar un nivel de riesgo aceptable.

Tecnología es responsable de realizar las acciones de sensibilización, comunicación, entrenamiento y socialización de la política de Seguridad de la información.

El cumplimiento de la Política de Seguridad de la Información es obligatorio. Si los colaboradores, consultores, contratistas, terceras partes violan estas políticas, la organización se reserva el derecho de tomar las medidas correspondientes.

Los principios de la política son parte de la cultura de CELSIA, por lo que se asegura un compromiso por parte del Comité Directivo de CELSIA para la difusión, consolidación y cumplimiento de la presente política.

Lineamientos de la Política de la Política de Seguridad

Esta Política es aplicable a todos los colaboradores, consultores, contratistas, terceras partes, que usen activos de información que sean propiedad de CELSIA.

Esta política debe ser revisada como mínimo una vez al año o cuando sea necesario.

Organización para la Seguridad

Tecnología a través del Líder de Ciberseguridad es responsable de definir, coordinar y controlar la gestión necesaria para mitigar los riesgos asociados a la seguridad de la información en CELSIA y reportará al Comité de Riesgos de Tecnología, dicho comité debe contar con la presencia de personal clave y claramente definido, con el objeto de cumplir y soportar las actividades de Seguridad de la Información.

Clasificación y control de activos de información

La información debe estar inventariada y tener identificados los riesgos y exposiciones de seguridad; con el objetivo de evitar pérdidas financieras, operativas y/o de imagen para la organización, la información deberá estar clasificada como secreta, restringida o general.

La información secreta y restringida debe estar soportada por un acuerdo de confidencialidad o de no-divulgación cuando sea compartida con terceros.

Uso aceptable de los activos y recursos de información

Todos los colaboradores, consultores, contratistas, terceras partes, que usen activos de información que sean propiedad de Celsia, son responsables de cumplir y acoger con integridad los lineamientos de Uso Aceptable para dar un uso racional y eficiente los recursos asignados.

Tratamiento y Gestión del Riesgo en Seguridad de la Información

Tecnología a través del líder de Ciberseguridad, es responsable de analizar los riesgos en seguridad de la información, con base en los objetivos de negocio y de acuerdo con la Política de Gestión de Riesgos y con aprobación del Comité de Riesgos de Tecnología.

Los líderes de cada proceso son responsables de priorizar y realizar el tratamiento de los riesgos en seguridad de la información de acuerdo con el apetito de riesgo de la organización.

En los proyectos o nuevas adquisiciones se debe realizar la identificación de los activos de información, los riesgos, amenazas, vulnerabilidades y el nivel de gestión para establecer un plan de seguridad de la información.

Seguridad de la información en Gestión Humana

Gestión Humana debe asegurar que los colaboradores comprenden sus responsabilidades y son idóneos en los roles para los que se consideran, tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.

Gestión Humana debe proteger los intereses de la organización como parte del proceso de cambio o terminación del contrato.

Seguridad Física y del Entorno

El centro de procesamiento de datos y cuarto de equipos de TIC, deben de estar en áreas protegidas físicamente contra el acceso no autorizado, daño o interferencia y deben cumplir con los lineamientos de seguridad física.

Control de acceso a la información

Tecnología, conforme la clasificación de activos de información debe implementar las medidas de seguridad aplicables según el caso, con el fin de evitar la adulteración, pérdida, fuga, consulta, uso o acceso no autorizado o fraudulento.

El control de acceso de datos e información sensible se debe basar en el principio del menor privilegio, lo que implica que no se otorgará acceso a menos que sea explícitamente permitido.

Gestión de incidentes de seguridad de la información

Todos los colaboradores, consultores, contratistas, terceras partes, deben anotar y comunicar cualquier punto débil que hayan observado o que sospechen que exista en los sistemas o servicios a través de la Mesa de Ayuda y Servicios.

Gestión de continuidad de los servicios TIC

Tecnología deberá implementar los procedimientos de recuperación de desastres para asegurar la continuidad de las operaciones y la disponibilidad de los servicios críticos TIC.

Gestión de Telecomunicaciones e Infraestructura de TIC

Tecnología debe proveer el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y medios de comunicación, a través de una Gestión de Telecomunicaciones e Infraestructura de TIC efectiva y eficiente.

Adquisición, Desarrollo y Mantenimiento de sistemas

Tecnología debe proveer medidas de seguridad en sistemas de información desde la fase de requerimientos, y deben ser incorporados en las etapas de diseño, desarrollo, implementación y mantenimiento.

Los sistemas de información adquiridos o desarrollados por CELSIA deben cumplir unos requerimientos mínimos de seguridad, conforme a las buenas prácticas en seguridad de la información y a esta política de seguridad. El diseño y operación de los sistemas debe obedecer a estándares de seguridad comúnmente aceptados y la normatividad vigente.

Cumplimiento y normatividad legal

Toda solución de servicios o infraestructura tecnológica debe garantizar que su selección está de acuerdo con las condiciones contractuales, de legislación y regulación externa e interna, para el debido cumplimiento de los regímenes legales a los cuales está sometida la organización.

Excepciones

Las excepciones a cualquier cumplimiento de la Política de Seguridad de la Información deben ser aprobadas por Tecnología o el Líder de Gestión Humana Administrativa y Tecnología o el Líder de CELSIA. Todas las excepciones a la política deben ser formalmente documentadas, registradas y revisadas.

Incumplimiento a la política de Seguridad de la información

Las violaciones a la política de Seguridad de la información o sus lineamientos por parte de los colaboradores, desencadenarán en medidas de tratamiento a los incidentes de Seguridad generados y podrían ser objeto de acciones disciplinarias por parte de Gestión Humana.

DEFINICIONES

Para los propósitos de este documento, se definen los siguientes conceptos:

- **Activo:** cualquier cosa que tenga valor para la empresa.
- **Amenaza**: causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema o a la empresa.
- **Confidencialidad:** propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
- **Comité de Riesgos de Tecnología:** el Comité de Riesgos de Tecnología debe establecer los criterios de dirección y control, que permitan implantar los mecanismos más apropiados de protección de la información de CELSIA, aplicando los principios de confidencialidad, integridad y disponibilidad de la misma y de los recursos informáticos o de otra índole que la soportan, acorde con la planeación estratégica de la empresa.

- **Desastre:** interrupción de la capacidad de acceso a información y procesamiento de la misma a través de computadoras u otros medios necesarios para la operación normal de un negocio.

- **Disponibilidad:** propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

- **Lineamientos de seguridad:** son productos, procedimientos y métricas aprobadas, que definen en detalle como las políticas de seguridad serán implementadas para un ambiente en particular, teniendo en cuenta las fortalezas y debilidades de las características de seguridad disponibles. Deben estar reflejadas en un documento que describe la implantación de una guía para un componente específico de *hardware, software* o infraestructura.

- **Evaluación del riesgo:** proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.

- **Integridad:** propiedad de salvaguardar la exactitud y el estado completo de los activos.

- **Organización de seguridad:** es una función que busca definir y establecer un balance entre las responsabilidades y los requerimientos de los roles asociados con la administración de seguridad de la información.

- **Políticas:** toda intención y directriz expresada formalmente por la dirección**.**

- **Procesos:** se define un proceso de negocio como cada conjunto de actividades que reciben una o más entradas para crear un producto de valor para el cliente o para la propia empresa (concepto de cliente interno de calidad). Típicamente una actividad empresarial cuenta con múltiples procesos de negocio que sirven para el desarrollo de la actividad en sí misma.

- **Procedimientos:** los procedimientos son los pasos operacionales que los funcionarios deben realizar para alcanzar ciertos objetivos.

- **Riesgo:** combinación de la probabilidad de un evento y sus consecuencias.

- **Seguridad de la información:** preservación de la confidencialidad, integridad y disponibilidad de la información, además puede involucrar otras propiedades tales como: autenticidad, trazabilidad (*accountability*), no repudio y fiabilidad.

- **TIC:** se refiere a tecnologías de la información y comunicaciones

- **Vulnerabilidad:** debilidad de un activo o grupo de activos, que puede ser aprovechada por una o más amenazas.

ANEXOS Y REFERENCIAS

- *Normas ISO 27000.*
- *Lineamientos de Seguridad de la información y Anexos.*

CONTROL DE CAMBIOS

VERSION	FECHA	JUSTIFICACIÓN DE LA VERSIÓN
1	12/06/2014	Creación del documento
2	30/10/2017	Cambio de formato del documento
3	18/06/2019	Simplificación de la política excluyendo los lineamientos documentándolos como un anexo. Inclusión de las palabras de la cultura Celsia tales como: equipo, líder, entre otras.