Declaración de Seguridad de la Información / Ciberseguridad

En Cencosud trabajamos diariamente con **pasión, respeto, transparencia y confianza,** para mejorar la calidad de vida de nuestros clientes a través de una **experiencia única, sostenible y con estándares inigualables de calidad** en sus productos y servicios. Nuestra Estrategia de Sostenibilidad y Modelo de Negocio, basada en los principios de Abastecimiento, Producción y Consumo Sostenible, busca conducir a las diferentes Unidades de Negocios hacia la transformación de la organización en un negocio sostenible.

Conscientes de esto, es que surge la "Declaración de Seguridad de la información", que tiene por objetivo brindar un resumen de los controles y procesos de seguridad dentro del grupo Cencosud. Este documento es para uso con terceros (clientes, inversionistas, proveedores, entre otros) que estén relacionados o comprometidos con Cencosud, y que deseen conocer sobre los arreglos de seguridad dentro del grupo. Esta declaración será revisada y actualizada anualmente.

Marco Normativo

La Compañía cuenta con un Marco Normativo, basado en las mejores prácticas y marcos de referencia internacionales, tales como NIST y Sans CIS, que establece los lineamientos y medidas de seguridad a contemplar por las diferentes áreas y por todos los Colaboradores de Cencosud, a fin de asegurar la protección de la información en todas sus formas y medios, contra su modificación accidental o deliberada y utilización y/o divulgación no autorizada.

Compromiso con la Seguridad

Cencosud está comprometido con mantener y mejorar continuamente la seguridad para cumplir con nuestras responsabilidades, con nuestros clientes y organismos reguladores, para reducir exposición a riesgos, sanciones legales, pérdidas operativas o daños a la reputación.

Como grupo, nos comprometemos con:

- La confidencialidad de la información corporativa, de socios, proveedores y de clientes
- La integridad de la información
- La disponibilidad de nuestra información
- El cumplimiento de requisitos legales, regulatorios y reglamentarios
- Brindar capacitación en seguridad de la información y conciencia de riesgos a todo el personal
- Informar e investigar violaciones de la seguridad de la información, reales o sospechas.

Organización de Riesgos de Información y Ciberseguridad

La administración de Cencosud en su conjunto es responsable de identificar, evaluar y administrar el espectro de riesgos a los que está expuesto el grupo.

Cencosud aplica un modelo de protección que garantiza que los riesgos y controles sean gestionados adecuadamente dentro de sus negocios, funciones y equipos de tecnología, de manera continua.

Estructura de Gobernanza de Seguridad de la información / Ciberseguridad

- Nombre: Marcelo Dalceggio
- Cargo: Chief Information Security Officer

Personal Cencosud

En Cencosud, la revisión de antecedentes es una defensa clave a nivel grupo contra el uso de información privilegiada y otros riesgos y se han definido requisitos mínimos de antecedentes. Todos los colaboradores del grupo Cencosud, incluyendo contratistas, proveedores de servicios y trabajadores de contingencia son sujetos a revisión de antecedentes, previo a entrar a un cargo o ejercer una función. El proceso de revisión de antecedentes también busca proveer un nivel de seguridad que indique que los antecedentes no levantan preocupaciones razonables sobre si dicha incorporación pudiera exponer al grupo a niveles inaceptables de riesgo. Como pre-filtro para todos los postulantes, se realiza un test DISC.

Las revisiones de antecedentes, según lo permitido por la ley local, incluye cuando es posible:

- Certificado de estudios
- Currículum Vitae
- Referencias laborales a ex empleadores (Administración central)
- Curso OS10 (Cargos de seguridad)

Consciencia de Seguridad

Cencosud cuenta con un programa de concientización continua de seguridad, el cual emplea diversos canales para realizar la bajada de información con el fin de involucrar al personal.

Este programa cuenta principalmente con:

- Capacitaciones presenciales y/o virtuales;
- Publicación en intranet/carteles;
- Campañas de Awareness;
- Cursos de inducción para nuevos colaboradores.

Política Cencosud

Cencosud ha desarrollado, para todo el grupo, una política de Seguridad de la Información, en la que se establecen lineamientos para Cencosud, sus colaboradores y terceros involucrados.

La política provee un marco de trabajo para todos los procesos y mecanismo de seguridad. Define los objetivos de seguridad, clasificación, responsabilidades y principios fundamentales para asegurarla de acuerdo con los objetivos del negocio.

Las políticas de Cencosud incluyen, pero no se limitan a:

- Responsabilidades definidas de seguridad de la información para colaboradores, contratistas y terceros
- Testeos para identificar controles faltantes o deficientes
- Política y lineamientos para todos los usuarios, acerca de uso aceptable de correo e internet
- Criterios definidos para el control de acceso, incluyendo la necesidad de conocer, principio de privilegio, usuario / ID único, complejidad de contraseñas, aprobaciones de acceso, transferencia de recertificación y procesos de abandono (desvinculación), acceso privilegiado y controles de acceso remoto
- Ciclos de vida de desarrollo de software para aplicaciones que incluyen revisión de código, separación de tareas, revisiones de seguridad para servicios web, entre otros.
- Control de cambios y respaldo de información para la continuidad del negocio.
- Procesos definidos para clasificación de información
- Instrucciones detalladas para encriptación, transferencia segura y destrucción de datos
- Políticas del entorno del usuario final, que abarcan la extracción de datos, el procesamiento de datos no gestionados por TI (informática del usuario final), clasificación de datos, etiquetado, destrucción segura del almacenamiento y trabajo remoto.
- Configuración técnica y configuración de control para infraestructura de TI, redes y plataformas.
- Seguridad física

La política define requerimientos mínimos para:

- La gestión y gerenciamiento de la información
- El control de accesos
- La seguridad física
- Las comunicaciones, operaciones y desarrollo de sistemas.

Gestión de Riesgos

Cencosud utiliza la gestión de riesgos en todas sus líneas clave de defensa para identificar, informar y gestionar los riesgos en toda la organización. Los marcos de seguridad de la información dentro de Cencosud siguen estándares de mejores prácticas a nivel internacional.

Las evaluaciones de riesgo se realizan periódicamente para abordar cambios en requisitos de seguridad de la información del grupo o el apetito de riesgo y cuando ocurren cambios significativos. Cencosud realiza evaluaciones de riesgo en la variedad de activos estratégicos/críticos dentro de la organización. Estos pueden ser activos físicos, personas, software e información. Por ejemplo, se realizan evaluaciones periódicas del riesgo de seguridad de la información sobre las tecnologías de aplicaciones e infraestructura para:

- Identificar, cuantificar y gestionar los riesgos de seguridad de la información para alcanzar los objetivos comerciales.
- Proporcionar medios para identificar actividades y factores que representan el mayor riesgo de seguridad para Cencosud.
- Asegurar que los problemas de seguridad de la información se gestionen de acuerdo con su calificación de riesgo y que los controles sean proporcionales al nivel de riesgo descubierto.
- Proporcionar una visión empresarial de los riesgos de seguridad de la información y los planes de corrección respectivos para desarrollar la estrategia de seguridad de la información.
- Planificar el despliegue de recursos en áreas que brinden la mayor reducción de riesgos para la información del cliente / corporativa.
- Evaluar todos los aspectos de los riesgos, amenazas y vulnerabilidades de seguridad de la información de nuestros activos.

Gestión de Accesos

Una unidad de gestión de identidad y acceso posee y opera el control de gestión de acceso dentro de Cencosud, esto garantiza una gestión de acceso alineada con el regulador y orientada por políticas en todo el ciclo de vida de los controles de soporte.

Los servicios/responsabilidades del equipo de gestión de identidad y acceso incluyen:

- Controles de nuevos colaboradores, colaboradores que abandonan la empresa o se mueven internamente, incorporando segregación de funciones para garantizar que se gestionen y/o mantengan los derechos autorizados de nivel correspondiente de privilegios para todas las actividades de los usuarios
- Controles de gestión de acceso privilegiado con la debida justificación y autorización, incorporando la validación de actividades a través de un proceso de registro y monitoreo.
- Acceso a controles de recertificación para garantizar que las cuentas y derechos asociados sean revisados, mantenidos o revocados, periódicamente, por el revisor apropiado.

Seguridad de Aplicaciones

Los equipos de seguridad de aplicaciones técnicas identifican amenazas, controles y realizan pruebas que incluyen:

- Consultoría de seguridad de aplicaciones y evaluaciones de riesgos: para garantizar que los riesgos dentro de las aplicaciones y sistemas de Cencosud se gestionen a un nivel aceptable;
- Asesoramiento técnico y de seguridad de la información a empresas, proyectos o iniciativas de funciones.
- Definición y prueba de los controles del sistema de aplicaciones relacionados con la seguridad de la información.
- Aportación a los estándares y procedimientos de construcción del sistema.
- Instalación y monitoreo de controles de nivel de aplicación.
- Desarrollo de estándares mínimos de seguridad de referencia.
- Pruebas de seguridad/penetración de aplicaciones (que incluyen vulnerabilidades cubiertas por el marco de seguridad cibernética) y revisiones de código.

Seguridad de Redes

Para permitir una gestión eficaz, Cencosud utiliza diversas tecnologías implementadas estratégicamente en toda su red, las cuales se describen a continuación:

- Gestión de redes inalámbricas
- Protección de denegación de Servicio
- Filtro de acceso a internet
- Testeo de Infraestructura de Seguridad
- Auditoría Externa de Cumplimiento y seguridad de la Información

Cifrado de Datos

Cencosud, como Compañía de primer nivel, es consciente de la importancia del cuidado de los datos personales, sensibles y críticos, tratándolos de manera acorde a las reglamentaciones vigentes de privacidad en la región.

Un ejemplo de ello es el cifrado de datos para todos los datos sensitivos para medios de pago utilizando tecnología EMV, para transacciones presenciales y pasarelas de pago certificadas para compras no presenciales, como así también, las comunicaciones con bancos son cifradas y seguras.

Seguridad del host

Estaciones de trabajo (notebook) y dispositivos móviles

Las estaciones de trabajo y las computadoras portátiles de Cencosud tienen un software antivirus incorporado en las compilaciones operativas predeterminadas, configuradas para verificar automáticamente los archivos como parte de su análisis regular "a tiempo completo" y obtener actualizaciones a medida que estén disponibles.

- Las computadoras de escritorio / portátiles tienen una compilación personalizada preinstalada que limita el acceso administrativo de los usuarios.
- El acceso a la red interna de Cencosud desde fuera de la oficina está restringido a dispositivos autorizados controlados por conectividad remota estándar de la industria y controles de autenticación de múltiples factores.
- El acceso a Internet y la conectividad de red de las computadoras portátiles Cencosud se enruta a través de la red Cencosud. El software VPN garantiza que los usuarios de computadoras portátiles Cencosud no puedan conectarse directamente a Internet público.

Plataforma del servidor

La seguridad del sistema está integrada en nuestras plataformas de servidor. Se incorporan medidas y controles de endurecimiento en las compilaciones del servidor; estos incluyen, pero no se limitan a:

- Servicios innecesarios y redundantes, dispositivos, procesos, protocolos, utilidades de sistemas y redes, programas y cuentas, se deshabilitan / eliminan.
- Las operaciones / servicios se ejecutan con los privilegios mínimos requeridos; Se aplica la seguridad adecuada del sistema de archivos.
- Se implementan fuertes controles de contraseñas y cuentas de usuario para todos los usuarios que imponen la longitud, complejidad, historial y bloqueos. Control automatizado de contraseñas con registro y auditoría aplicados a cuentas privilegiadas.
- Los ajustes de configuración se definen según el principio del "mínimo privilegio".
- Monitoreo y reporte de cualquier incumplimiento.

Gestión y manejo de parches

Los equipos de primera línea reciben notificaciones de vulnerabilidades del proveedor de productos y las respuestas de parches recomendadas. La priorización para la implementación en el patrimonio de Cencosud está determinada por la clasificación de prioridad de parche, asignada como parte del proceso de evaluación que utiliza el Sistema de puntuación de vulnerabilidad común del marco estándar de la industria.

Los parches antes de la implementación en los sistemas de producción se prueban en entornos que no son de producción a nivel mundial

Todas las implementaciones de parches se administran siguiendo los Procesos de gestión de cambio global y gestión de incidentes de Cencosud.

La gobernanza y supervisión apropiadas se ejercen a través del compromiso y la comunicación regulares con las empresas y funciones globales de acuerdo con el marco establecido.

Trabajo Remoto

El acceso que realiza el personal de Cencosud a los recursos de la Compañía por fuera de la red interna se efectúa a través del mecanismo de Acceso Remoto autorizado por Seguridad Informática.

Los controles y la orientación adicionales para el personal que trabaja de forma remota incluyen, entre otros:

- Capacitación y educación sobre el riesgo de trabajo remoto que debe completarse antes de proporcionar acceso remoto.
- Ingreso a la red de la Compañía a través del uso de VPN, de manera única, personal e intransferible.
- Disponibilización de herramientas de correo electrónico, mensajería instantánea, audio/video y de colaboración para enviar o recibir información y el trabajo colaborativo.

Operaciones de Seguridad

Cencosud cuenta con procesos, actividades y servicios para evitar interrupciones de sistemas de TI y ataques cibernéticos, como así también, para reaccionar adecuadamente ante la ocurrencia de los mismos. A continuación se detallan algunos ejemplos:

- Monitoreo proactivo 24/7 todo el año
- Soporte de análisis técnico y respuesta a amenazas
- Soluciones automatizadas
- Análisis forense de medios digitales y artefactos electrónicos.
- Detección y mitigación de malware
- Detección y monitoreo de intrusiones de red y host
- Evaluación de amenazas tecnológicas emergentes
- Gestión regional/global de incidentes de ciberseguridad

Manejo de incidentes

Ante incidentes, se activa el procedimiento interno de gestión de incidencias.

Procesos de gestión y respuesta a incidentes de operaciones de ciberseguridad:

Coordinar los incidentes de seguridad cibernética para garantizar que se completen todas las tareas requeridas y que se eviten esfuerzos duplicados o contradictorios.

- Asegurar que los incidentes de ciberseguridad se investiguen de manera oportuna
- Asegurar que el riesgo asociado con un incidente se identifique, mida y controle adecuadamente
- Asegurar que se completen las notificaciones internas y los informes externos requeridos
- Asegurar que todos los incidentes de ciberseguridad se rastreen de manera centralizada para el análisis de tendencias y la generación de informes consolidados a la gerencia

Acuerdos de no divulgación y confidencialidad

Cencosud solo divulga información a terceros, si se han considerado e implementado los controles apropiados (según corresponda) para administrar el acceso, uso y almacenamiento de la información de Cencosud por parte de terceros. Estos controles pueden incluir:

- Acordar obligaciones de confidencialidad y seguridad de la información con el tercero;
- Hacer evaluaciones apropiadas de la información en sí, cómo y por qué se divulgará; y
- La transferencia de información se asegura utilizando controles técnicos o de proceso apropiados según lo requiera Cencosud para cumplir con nuestras responsabilidades legales, obligaciones del cliente y requisitos reglamentarios.

Gestión de seguridad de proveedores

Cencosud tiene una política de gestión de riesgos de terceros para identificar y controlar los riesgos (incluidos los riesgos de seguridad de la información) asociados con las relaciones y contratos con los proveedores.

Cencosud requiere que terceros cumplan al menos el mismo nivel de seguridad según las políticas y estándares del Grupo Cencosud, cubriendo los requisitos legales y reglamentarios que se aplican a la información o sistemas de Cencosud a los que se accede en la prestación del servicio a Cencosud.

Además, los terceros con acceso a la red o información de Cencosud están sujetos a revisiones de diligencia debida de seguridad de la información en función de su riesgo potencial para la organización. Se incluyen cláusulas específicas de seguridad de la información en los términos y condiciones de los contratos con terceros. Estos pueden incluir el derecho a realizar auditorías de las instalaciones de terceros, controles de seguridad físicos y lógicos.

Los colaboradores de terceros con acceso a nuestros sistemas están sujetos a una recertificación de acceso periódico.