PRÁCTICAS DE SEGURIDAD DE LA INFORMACIÓN

TABLA DE CONTENIDO

1 GENERALIDADES

1.1 OBJETIVO

Este documento describe las prácticas adheridas por Compass Group Asset Management Holding S.L. y sus filiales (en adelante "Compass"), para sus operaciones internas y servicios. Compass reconoce la importancia crítica en la protección de la información, por este motivo se ha adoptado controles de seguridad y prácticas que se enfocan en la confidencialidad, integridad y disponibilidad.

1.2 ALCANCE

Estas prácticas aplican a Compass.

2 MARCO NORMATIVO DE SEGURIDAD DE LA INFORMACIÓN

Las políticas de Compass cubren la gestión de seguridad tanto para las operaciones internas como para los servicios otorgados a nuestros clientes. Las políticas aplican a todos los colaboradores y proveedores que tengan acceso a la información de Compass. El marco normativo de Seguridad de la Información fue elaborado siguiendo como referencia al standard ISO/IEC 27001, estos documentos son de uso interno, y no son visibles a clientes o terceras partes, sin embargo, se comparten resúmenes de las políticas y normas principales en el presente documento.

Las políticas aprobadas por Directorio son:

- **Política General de Seguridad de la Información y Ciberseguridad.** Esta política establece los lineamientos generales en cuanto a la seguridad de la información, donde se destaca el compromiso del Directorio y la Gerencia en establecer políticas para proteger apropiadamente los activos de información de los riesgos que pueden afectarlos.
- **Política de Gobierno Seguridad de la Información y Ciberseguridad.** En esta política se establece principalmente la organización interna que gestionará, evaluará y resolverá sobre materias relacionadas a la seguridad de la información.

2.1 CUMPLIMIENTO

El marco normativo aplica a todos los colaboradores de Compass, y en caso de presenciar un incumplimiento a las políticas, normas, brecha de seguridad, incidente u otro evento, los usuarios tienen el deber de reportar internamente y de forma inmediata para su tratamiento.

2.2 ADHESIÓN

Los colaboradores que no se adhieran al marco normativo de Compass, procedimientos y prácticas establecidas en general en la compañía estarán sujetos a sanciones, las que incluso pueden o cese del contrato.

3 ORGANIZACIÓN DE LA SEGURIDAD

3.1 ESTRUCTURA DE SEGURIDAD

A continuación, se presentan los grupos/personas involucradas en la Seguridad de la Información:

- Oficial de Seguridad de la Información: Responsable de la implementación de los programas de seguridad, incluyendo las políticas, normas, entre otros. Además de la gestión de riesgos, soporte, cumplimiento y asistencia en la mitigación de riesgos de Seguridad de la Información.

- Comité de Seguridad de la Información: Grupo en donde se discuten los tópicos relevantes de Seguridad de la Información, iniciativas y/o decisiones en relación a su gestión. Se aprueban además normas y/o estándares o procedimientos.

- Junta Directiva: Responsables de las decisiones en ámbitos estratégicos, financieros y organizacionales. Discuten cambios, apoyan a la alta dirección entre otras acciones. Además, se encargan de la formulación y aprobación de marcos normativos, políticas, de la compañía.

- Gerencia de Servicios Tecnológicos: Encargados de implementar y mantener la infraestructura tecnológica, el soporte a usuarios, y fortalecimiento de la ciberseguridad.

- Gerencia de Proyecto y Sistemas: Responsables de que se implementen los controles de seguridad en los proyectos, desarrollos y adquisiciones de sistemas en estrecha coordinación con la Gerencia de Servicios Tecnológicos.

3.2 Acuerdos de confidencialidad

Todos los colaboradores y contratistas que tengan acceso a la información de Compass estarán sujetos a acuerdos de confidencialidad. Los proveedores, previo a la prestación de servicios, deberán firmar un acuerdo de confidencialidad, y se deberá definir el servicio entregado por el proveedor.

4 Seguridad de los recursos humanos

Compass ha tomado medidas de seguridad con los colaboradores, las medidas se enfocan en minimizar los riesgos de fraude y el mal uso de los recursos, lo que incluye verificación de antecedentes, acuerdos de confidencialidad, acciones disciplinarias, entre otros.

4.1 Revisión de antecedentes

La organización solicitará los antecedentes, tales como certificados de estudios, u otros que avalen su conocimiento. En caso de utilizar los servicios de una empresa externa para reclutamiento, se recibirá un informe con el análisis del perfil del candidato.

4.2 Conductas en el negocio

Compass establece en el Código de ética y Conducta los estándares de ética moral y conducta en el negocio para todos los niveles de la organización y en cada ubicación en donde Compass se encuentra ofreciendo sus servicios. El estándar aplica a todos los colaboradores de Compass, independiente de si son proveedores o colaboradores temporales. Este estándar cubre áreas legales, cumplimiento regulatorio, conductas de negocio y relaciones.

4.3 Confidencialidad

Los colaboradores deben resguardar la información de Compass, por lo que en los contratos se incluye una cláusula sobre la confidencialidad. Además, los colaboradores reciben un manual de compliance y políticas de recursos humanos que incluye Código de ética y conducta, manual de prevención y detección de lavado de dinero, reglamento interno de orden, higiene y salud y políticas de recursos humanos.

4.4 Entrenamiento y concientización

Los usuarios recibirán de forma periódica ciclos de capacitación y concientización con el fin de mantener a los usuarios alertas y seguir las medidas de seguridad adoptadas por la compañía. En caso de existir un evento, incidente o violación a las políticas los usuarios tienen el deber de comunicarlo a las áreas de Riesgo Operacional y Servicios Tecnológicos para tomar acciones.

4.5 Términos

Los términos de contratos de los colaboradores son coordinados con la Gerencia de Desarrollo del Talento y la Gerencia de Servicios Tecnológicos con el fin de dar de baja los accesos de los usuarios oportunamente y recibir los dispositivos que hayan sido provistos por la compañía.

4.6 Proceso disciplinario

Todo empleado que incumpla con las políticas y normas establecidas será sujeto a un proceso de investigación y sanción de acuerdo a lo establecido por la Gerencia de Desarrollo del Talento.

5 Seguridad física y ambiental

5.1 Controles físicos en sala de servidores

Sólo personal autorizado puede ingresar a la sala de servidores, por medio de un código, tarjeta de acceso o acceso biométrico. Existe un solo punto de ingreso a la sala y se cuenta con cámaras de seguridad.

5.1.1 Controles de ingreso a sala de servidores

Proveedores, subcontratistas y visitantes podrán ingresar a la sala de servidores siendo escoltados por el personal autorizado y se mantiene un registro de visitas en una bitácora de acceso físico.

5.2 Controles ambientales

Se mantienen las condiciones ambientales para proteger a los equipos. Esto incluye temperatura, humedad y consumo de energía.

6 Gestión de infraestructura TI y comunicaciones

6.1 Protección de códigos maliciosos

Todos los equipos y laptops de Compass conectados a la red poseen una solución antimalware, el cuál es actualizado regularmente. Además, se cuenta con un producto antispam que escanea los mails. Para evitar la ejecución de programas no autorizados se tiene una herramienta para el control de los privilegios. En la navegación en internet se tiene un filtro de contenido que evita el acceso a categorías maliciosas.

6.2 Respaldos y recuperación

Para proteger la información se realizan respaldos de forma diaria y mensual, y se define la programación, además del manejo de cintas de respaldo, rotación y etiquetado. Las cintas son transportadas y almacenadas por un proveedor, quien retira las cajas de forma mensual para su posterior almacenamiento. Asimismo, se realizan pruebas de recuperación para validar que la información es accesible y puede ser utilizada en caso de pérdida de información o una contingencia. Actualmente, el proceso de gestión y almacenamiento se encuentra centralizado en la oficina de Chile.

6.2 GESTIÓN DE SEGURIDAD DE LA RED

Compass cuenta con tecnología de respuesta autónoma con inteligencia artificial que "aprende" del comportamiento de los usuarios en la red, interrumpiendo ataques de manera rápida y precisa, incluso si la amenaza es sofisticada y desconocida.

6.2.1 MECANISMOS DE PROTECCIÓN

Compass cuenta con Web Aplication Firewall, Firewall, IPS, IDS y filtros de spam, phishing, y malware. Además, se cuenta con servicio SOC que analiza y gestiona eventos permanentemente, el resumen de los reportes mensuales es informado por el proveedor a Servicios Tecnológicos y Seguridad de la Información de Compass.

6.2.2 MANEJO DE MEDIOS Y ELIMINACIÓN

La información sensible impresa es eliminada de forma segura en trituradoras cuando ya no tiene vigencia legal ni para el negocio.

Los medios electrónicos y electromagnéticos de almacenamiento de información que son reutilizados en Compass son borrados de manera segura; mientras que los dispositivos que no son requeridos son destruidos.

7 CONTROL DE ACCESOS

7.1 REGISTRO DE USUARIOS

Los accesos de usuarios son canalizados por el Área de Soporte, quienes mantienen un registro de las solicitudes, autorizaciones y tipos de accesos.

7.2 CONTRASEÑA DE USUARIOS

Las contraseñas de usuarios deben ser robustas y cumplir con las siguientes características para acceder a la red:

- Al menos 12 caracteres alfanuméricos y caracteres especiales.
- Expirar cada 60 días.
- No reutilizar las últimas 5 contraseñas.
- Bloqueo de cuenta al tercer intento fallido.

7.3 RESPONSABILIDAD DE LOS USUARIOS

Los usuarios deben conocer las políticas de Compass, siguiendo los lineamientos para uso de contraseñas, resguardar la información y cuidados de su entorno dentro y fuera de la oficina al manejar dispositivos corporativos.

8 CONTROLES DE ACCESO A LA RED

Los accesos remotos de los usuarios deberán ser por medio de VPN, con el fin de asegurar las conexiones y transmisión de información.

Las redes se encuentran segregadas y se cuentan con controles de acceso.

Además, se utiliza Firewalls que controlan el acceso y permite sólo tráfico autorizado.

9 ADQUISICIÓN, DESARROLLO Y MANTENCIÓN DE SISTEMAS DE INFORMACIÓN

La adquisición, desarrollo y mantención de sistemas de información considera la seguridad de la información para resguardar los activos de información.

Los cambios en los sistemas de información son gestionados y documentados de acuerdo al proceso de gestión de cambios.

Además, Compass realiza análisis de vulnerabilidades con el fin de tomar las medidas de seguridad y proteger los activos de información.

10 GESTIÓN DE INCIDENTES

Compass evalúa y responde ante los eventos y/o incidentes que se puedan presentar con el fin de tomar los resguardos necesarios y proteger la información. Esta es una actividad realizada con herramientas especializadas gestionadas por Compass y en conjunto con los proveedores de servicios de ciberseguridad.

11 Continuidad del negocio

Compass tiene un plan de continuidad de negocio que se enfoca en reestablecer la operación en el menor tiempo posible, el cual contempla los procesos críticos de la compañía los cuales pueden ser afectados por eventos como indisponibilidad de plataformas tecnológicas, proveedores, personal, instalaciones, entre otros.

El plan establece una estructura que determina los roles y responsabilidades, además de los escenarios posibles de eventos, análisis de riesgos, impacto al negocio y el plan de recuperación ante desastres.

Se realizan pruebas de forma anual, con el fin de medir la efectividad del plan considerando los escenarios.

12 Cumplimiento legal

12.1 Cumplimiento regulatorio

Compass cumplirá con las regulaciones en relación a sus negocios.

12.2 Reportes de auditorías externas

Compass es auditado de forma anual por una empresa externa que evalúa y prueba el control interno asociado a los estados financieros de la compañía. El informe final es revisado por la Junta Directiva quienes evalúan las decisiones estratégicas en base a lo reportado.