.Company

Política general de seguridad de la información.

2020

Control de cambios

Fecha	Autor	Control de cambios - descripción de la modificación

1. Objetivos

El propósito de la “Política General de Seguridad de la Información”, es declarar la posición de UpCompany con respecto al buen uso y protección de los activos de información. Esto se traduce en:

- **1.1.** Definir lineamientos o principios generales que sirven como medio para alcanzar los objetivos de un Sistema de Seguridad de la Información.
- **1.2.** Establecer responsabilidades aplicables a los distintos niveles jerárquicos y a todo el personal vinculado con UpCompany.
- **1.3.** Fijar directrices sobre las cuales se sustentan normativas e instructivos de seguridad que desarrollen con mayor grado de detalle aspectos relativos a la seguridad de un tema particular o sistema en específico.
- **1.4.** Definir medios de difusión al interior y exterior del servicio para alineamiento con la Dirección.
- **1.5.** Definir plazos y periodicidad para su revisión y evaluación de cumplimiento.

2. Alcance

La presente política establece un marco regulatorio aplicable a todo el personal relacionado con UpCompany, ya sea colaboradores sujetos al Código del Trabajo, como a personal externo que preste servicios permanentes o temporales.

También es aplicable a todo activo de información que la organización posea en la actualidad o en el futuro, asociados a los procesos de negocio de UpCompany, de manera que la no inclusión explícita en el presente documento, no constituye argumento para no proteger estos activos de información.

La política cubre toda la información, entre otras, la impresa o la escrita en papel, la almacenada electrónicamente, la transmitida por correo o usando medios

electrónicos, mostrada en video o hablada en una conversación, entre otras formas de información.

3. Definiciones

3.1. Activo de Información

Aquello que tenga valor y es importante para el UpCompany, sean documentos, sistemas o personas y todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la organización. Se distinguen tres niveles:

3.1.1. La Información propiamente tal, en sus múltiples formatos (papel, digital, texto, imagen, audio, video, etc.)

3.1.2. Los equipos, sistemas e infraestructura que soportan o contienen esta información.

3.1.3. Las personas que utilizan la información, y que tienen el conocimiento de los procesos de la organización.

3.2. Colaborador

Toda persona que tenga un vínculo contractual de trabajo con el UpCompany, sea éste indefinido, a plazo fijo o a honorarios.

3.3. Política

Directriz u orientación general expresada formalmente por la administración de UpCompany.

3.4. Norma

Disposición de carácter general que se desprende de las políticas, estableciendo obligaciones, restricciones, prohibiciones u otras conductas esperadas.

3.5. Procedimiento

Sucesión cronológica de acciones concatenadas entre sí, para la realización de una actividad o tarea específica dentro del ámbito de los controles, en este caso, de Seguridad de la Información.

3.6. Riesgo

Es la posibilidad que ocurra un evento que afecte adversamente el logro de los objetivos de UpCompany. Se mide combinando las consecuencias del evento (impacto) y su probabilidad de ocurrencia.

3.7. Amenaza

Causa potencial de un incidente no deseado, que puede dar lugar a daños a un sistema o proceso.

3.8. Vulnerabilidad

Debilidad de un activo o grupo de activos que puede ser materializada por una o más amenazas.

3.9. Evento de Seguridad de la Información

Actividad o serie de actividades sospechosas que amerita ser analizada desde la perspectiva de la Seguridad de la Información.

3.10. Incidente de Seguridad de la Información

Evento o serie de eventos de Seguridad de la Información, no deseados o inesperados, que compromete la Seguridad de la Información y amenaza la operación del negocio.

3.11. Confidencialidad

Propiedad de la información que determina que sólo podrá ser accedida por personas, entidades o procesos debidamente autorizados.

3.12. Integridad

Propiedad de la información según la cual sólo puede ser modificada, agregada o eliminada por las personas o sistemas autorizados para cada proceso, de tal forma de salvaguardar la exactitud y completitud de los activos de información.

3.13. Disponibilidad

Propiedad de la información según la cual es accesible y utilizable oportunamente por las personas o sistemas o procesos autorizados, en el formato requerido para su procesamiento.

4. Políticas

4.1. De la información interna

4.1.1. La información es un activo vital, por lo que su utilización, es decir, accesos, procesamiento y mantenimiento deberán ser consistentes con lo instruido en las políticas, normas, y procedimientos emitidos por Upcomapny en cada ámbito en particular.

4.1.2. La información debe ser protegida de una manera consistente con su importancia, valor y criticidad, siguiendo las reglas establecidas en las políticas específicas de seguridad de la información, sus procedimientos asociados y en las recomendaciones dadas por el responsable designado de dicha información.

4.1.3. Toda información creada o procesada por la organización debe ser considerada como “reservada”, a menos que se determine expresamente lo contrario. Upcomany proveerá los mecanismos para que la información sea accedida y utilizada por el personal que de acuerdo con sus funciones así lo requiera. Sin embargo, se reserva el derecho de revocar al personal, el privilegio de acceso a la información y tecnologías que la soportan, si la situación y las condiciones lo ameritan.

4.2. De la información de los clientes o terceros.

4.2.1. Si la organización procesa y mantiene información de clientes que sean datos personales y/o sensibles de acuerdo con la normativa vigente, ésta se compromete a asegurar que dicha información no será divulgada sin previa autorización y estará protegida de igual manera que la información interna, de conformidad a lo establecido en la Ley N° 19.628, sobre

protección a la vida privada, sin perjuicio de lo señalado en la ley N° 20.285.

4.2.2. En el caso de información externa, proveniente de fuentes públicas, que se procese, mantenga y que no tenga las características anteriormente mencionadas, ésta podrá ser divulgada sin previa autorización.

4.2.3. Si se requiere compartir información de los clientes de UpCompany con organizaciones externas, será requisito la suscripción de un contrato, cláusula y/o convenio de confidencialidad y no divulgación previo a la entrega de la información.

4.3. De las auditorías.

4.3.1. Con el fin de velar por el correcto uso de los activos de información, UpCompany se reserva el derecho de auditar en cualquier momento el cumplimiento de las políticas y documentos vigentes que digan relación con el acceso y uso que los usuarios hacen de los activos de información.

4.3.2. Las auditorías podrán ser realizadas internamente o por auditorías a cargo de organizaciones externas, cuando sea pertinente y requerido por el Encargado u Oficial de Seguridad, en coordinación con el Comité de Seguridad de la Información.

4.4. De la gestión de la seguridad de la información.

4.4.1. La gestión de la seguridad de la información se realizará mediante un proceso sistemático, documentado y conocido por la organización. Este proceso deberá ser aplicado a los procesos críticos del negocio.

4.4.2. El cumplimiento de los objetivos del sistema de gestión de seguridad de la información de Upcomapny se basará en la identificación de los activos de información involucrados en los procesos de negocio críticos, lo que implica al Encargado

de Seguridad de la Información, junto a los responsables de los diferentes procesos y subprocesos de negocio de UpCompany, realizar las siguientes actividades fundamentales:

4.4.2.1. Identificar y clasificar los activos de información involucrados.

4.4.2.2. Para cada activo de información, identificar un responsable.

4.4.2.3. Analizar el riesgo al cual están expuestos.

4.4.2.4. Difundir en forma planificada entre todo el personal el objetivo corporativo de la preservación de la información, sus características y las responsabilidades individuales para lograrlo, inserto esto, en planes de capacitación anuales así como en el proceso de inducción del nuevo personal.

4.5. Deberes del personal y de terceros.

Los deberes del personal y de terceros son:

4.5.1. La información y las tecnologías de información deben ser usadas sólo para propósitos relacionados con el cumplimiento de las funciones asignadas y autorizados por la jefatura directa, debiéndose aplicar criterios de buen uso.

4.5.2. Las claves de acceso a la información y a las tecnologías de información serán de carácter individual, intransferibles y de responsabilidad única de su propietario.

4.5.3. El personal está en la obligación de alertar, de manera oportuna y adecuada, cualquier incidente que atente contra lo establecido en esta política según procedimientos que se establezcan en el manejo de incidentes.

4.5.4. Se prohíbe la divulgación de información que esté considerada o clasificada como “reservada”.

4.6. Revisión de la Política.

4.6.1. Una de las tareas a realizar por el Comité de Seguridad de la Información de UpCompany, es la reevaluación de la Política General de la Seguridad de la Información. Esto deberá realizarse por lo menos una vez al año o ante cualquier cambio significativo de tecnología, personal o evento que amerite su reevaluación para asegurar continuidad, idoneidad, eficiencia y efectividad.

4.7. Difusión de la Política.

4.7.1. La Dirección de UpCompany considera fundamental integrar en la cultura organizacional, la existencia de un plan formal de difusión, capacitación y sensibilización en torno a la seguridad de la información.

4.8. Documentación de referencia.

Se considerará como documentación de referencia para la presente política, toda la normativa vigente en Chile a esta fecha, a decir:

4.8.1. Ley N° 17.336, sobre Propiedad Intelectual.
4.8.2. Ley N° 19.223 que tipifica figuras penales relativas a la informática.
4.8.3. Ley N° 19.628, sobre protección a la vida privada.
4.8.4. Ley N° 20.285, sobre acceso a la información pública.
4.8.5. Ley N° 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma.
4.8.6. Norma NCh- ISO 27001:2013.
4.8.7. Norma NCh- ISO 27002:2013.
4.8.8. Norma NCh- ISO 27032:2012.

5. Controles aplicables de Norma NCh/ISO 27001:2013

5.1.1. A.5.5.1. Políticas para la seguridad de información.

6. Aprobación

La política general de seguridad de la información ha sido aprobada por la alta dirección de la organización:

AGUAYO MORA, CRISTIÁN ANDRÉS
18.084.547-k
CEO

BARRERA FARFAN, ORLANDO ANDRÉ
18.085.335-9
CTO