Secuoya
content group

Política de Seguridad de la Información

Código	PO.00
Título	Política de Seguridad de la Información

Índice

1. INTRODUCCIÓN 4

2. OBJETO 5

3. MISIÓN 6

4. ALCANCE 8

5. MARCO NORMATIVO 9

6. CONTENIDO 10

6.1 Gobierno Normativo 10

6.1.1 Nivel Estratégico o Nivel Superior 10
6.1.2 Nivel Táctico o Nivel Intermedio 10
6.1.3 Nivel Operativo o Nivel Inferior 10
6.1.4 Nivel Funcional o Nivel Técnico 11

6.2 Estructura Normativa 11

6.3 Políticas 11

6.4 Prevención 11

6.5 Detección 12

6.6 Respuesta 12

6.7 Recuperación 12

7. ORGANIZACIÓN DE LA SEGURIDAD 13

7.1 Comité de Seguridad 13

7.1.1 Misión 13

7.2 Roles y Responsabilidades 13

7.2.1 Gobierno y Organización 15

7.3 Comité de Crisis 15

7.3.1 Objetivos y Funciones 15
7.3.2 Gobierno y Organización 16

8. DATOS DE CARÁCTER PERSONAL 17

9. GESTIÓN DE RIESGOS 18

10. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN 19

10.1 Sistema de Gestión de Seguridad de la Información 19

10.2 Política de Uso de los Sistemas de Información 19

10.3 Seguridad de la Gestión de Recursos Humanos 20

10.4 Seguridad Física y del Entorno 20
10.4.1 Áreas Seguras 20
10.4.2 Seguridad de los Equipos 20
10.5 Gestión de Comunicaciones y Operaciones 21
10.5.1 Procedimientos Operativos y Responsabilidades 21
10.5.2 Protección frente a Código Malicioso y Código Móvil 21
10.5.3 Copias de Seguridad 21
10.5.4 Gestión de la Seguridad de la Red 22
10.6 Gestión de Soportes 22
10.6.1 Intercambio de Información 22
10.6.2 Seguimiento 22
10.7 Control de accesos 22
10.7.1 Requisitos del Servicio para el Control de Accesos 22
10.7.2 Gestión de Accesos de los Usuarios 22
10.7.3 Responsabilidades del Usuario 22
10.7.4 Control de Acceso a la Red 23
10.7.5 Informática Móvil y Teletrabajo 23
10.8 Gestión de Incidencias 23
10.9 Continuidad del Servicio 23
11. OBLIGACIONES DEL PERSONAL 25
12. TERCERAS PARTES 26

1. INTRODUCCIÓN

La información es un activo estratégico para para las empresas que conforman Grupo Secuoya (en adelante, Secuoya), como empresas cuyas actividades principales se enmarcan en la prestación de servicios audiovisuales. Secuoya depende de los sistemas TI (Tecnologías de Información) para alcanzar sus objetivos estratégicos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad, confidencialidad, autenticidad, o trazabilidad de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a las incidencias.

Los sistemas TI deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios.

Esto implica que se deben aplicar las medidas de seguridad exigidas por el Sistema de Gestión de la Seguridad de la Información Corporativo (SGSI), Secuoya realiza un seguimiento continuo de los criterios y requisitos establecidos en la legislación aplicable, como el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS), la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) y el Reglamento de la Unión Europea 2016/679 relativo a la protección del tratamiento de datos personales (RGPD). Asimismo, se realiza un seguimiento continuo de los niveles de prestación de servicios, se analizan las vulnerabilidades reportadas, y se prepara una respuesta efectiva a las incidencias para garantizar la continuidad de los servicios prestados.

Por tanto, podemos identificar la existencia de tres figuras diferenciadas que forman parte, siendo:

- Responsable de la información: determinará los requisitos de la información tratada.
- Responsable del servicio: determinará los requisitos de los servicios prestados.
- Responsable de seguridad: determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

Secuoya debe asegurar que la seguridad de la información es una parte integral de cada etapa del ciclo de vida de los sistemas TI, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en propuestas de externalización de proyectos de TI.

2. OBJETO

Secuoya define la presente Política de Seguridad de la Información con el objetivo fundamental de garantizar la seguridad de la información y la prestación continuada de los servicios que proporciona, actuando preventivamente, supervisando la actividad y reaccionando con presteza frente a las incidencias que puedan ocurrir.

Esta Política debe sentar las bases para que el acceso, uso, custodia y salvaguarda de los activos de información, de los que se sirve Secuoya para desarrollar sus funciones, se realicen, bajo garantías de seguridad, en sus distintas dimensiones:

- **Disponibilidad**: propiedad o característica de los activos que garantiza que las entidades o procesos autorizados tengan acceso a los mismos cuando lo requieran.
- **Integridad**: propiedad o característica consistente en que el activo de información no sea alterado de manera no autorizada.
- **Confidencialidad**: propiedad o característica consistente en que la información no se ponga a disposición ni se revele a individuos, entidades o procesos no autorizados.
- **Autenticidad**: propiedad o característica consistente en que una entidad sea quien dice ser o bien que garantice la fuente de la que proceden los datos.
- **Trazabilidad**: propiedad o característica consistente en que las actuaciones de una entidad puedan ser imputadas exclusivamente a dicha entidad.

Bajo estas premisas los objetivos específicos de la Seguridad de la información en Secuoya serán:

- Velar por la seguridad de la información, en las distintas dimensiones antes descritas.
- Gestionar formalmente la seguridad, sobre la base de procesos de análisis de riesgos.
- Elaborar, mantener y probar los planes de disponibilidad y continuidad de la actividad que se definan para los distintos servicios ofrecidos por la organización.
- Realizar una adecuada gestión de incidencias que afecten a la seguridad de la información.
- Mantener informado a todo el personal acerca de los requerimientos de seguridad, y difundir buenas prácticas para el manejo seguro de la información.
- Proporcionar los niveles de seguridad acordados con terceras partes cuando se compartan o cedan activos de información.
- Cumplir con la reglamentación y normativa vigente.

La Política de Seguridad:

- Será aprobada formalmente por el Comité de Seguridad y presentada ante el Consejo de Administración.
- Se revisará regularmente, de manera que se adapte a las nuevas circunstancias, técnicas u organizativas, y evite la obsolescencia.
- Será comunicada a todos los empleados y empresas externas que trabajen con Secuoya.

3. MISIÓN

El propósito de esta Política de Seguridad de la Información es proteger la información y los servicios de Secuoya.

- Secuoya reconoce expresamente la importancia de la información, así como la necesidad de su protección, por constituir un activo estratégico y vital, hasta el punto de poder llegar a poner en peligro la continuidad de la organización, o al menos suponer daños muy importantes, si se produjera una pérdida total e irreversible de determinados datos.
- Secuoya implementa, mantiene y realiza un seguimiento de los controles contenidos en su declaración de aplicabilidad y los procesos del SGSI, conforme a las normas ENS, RGPD, LOPDGDD, ISO 27001 e ISO 20000-1 principalmente, y cumple con todos los requisitos legales aplicables.
- La información y los servicios están protegidos contra pérdidas de disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad.
- Se cumplen los requisitos del servicio respecto a la seguridad de la información y los sistemas de información.
- Los controles serán proporcionales a la criticidad de los activos a proteger y a su clasificación.
- La responsabilidad de la seguridad de la información involucrada en la prestación de los servicios incluidos en el alcance es del Comité de Seguridad, que pondrá los medios adecuados, sin perjuicio de que los empleados o usuarios asuman su parte de responsabilidad respecto a los medios que utiliza, según lo indicado en las políticas, normativas y en los procedimientos complementarios.
- Se ha identificado a los responsables de la información, que deberán promover el establecimiento de los controles y medidas destinadas a proteger los datos que la integran, especialmente los de carácter personal o críticos.
- Se han establecido y puesto a disposición, los medios necesarios y adecuados para la protección de personas, datos, programas, equipos, instalaciones, documentación y otros soportes que contengan información, y, en general, de cualquier activo de Secuoya.
- Los aspectos específicos más relacionados con la información sobre datos personales están regulados por el conjunto de normas recogidas en este documento de seguridad y en la normativa interna o de otra índole a la que pueda remitir o que se cite.
- Quienes no cumplan lo determinado en estas normas y en los procedimientos complementarios podrán ser sancionados de acuerdo con la legislación laboral y el convenio colectivo de referencia, o bien con sanciones personalizadas si están vinculados a Secuoya bajo contratos no laborales, de acuerdo con las cláusulas que figuren en dichos contratos y la legislación aplicable en este último caso.
- Se realizan periódicamente evaluaciones de riesgos y, en función de las debilidades, se determina si es necesario elaborar planes de implantación o reforzamiento de controles.
- Se fomenta la difusión de información y formación en seguridad a empleados y colaboradores, previniendo la comisión de errores, omisiones, fraudes o delitos, y tratando de detectar su posible existencia lo antes posible, y en caso de que existieren, procurándose una difusión muy restringida de las indagaciones.
- El personal de Secuoya deberá conocer las normas, reglas, estándares y procedimientos relacionados con su puesto de trabajo, así como sus funciones y obligaciones, además de la separación de funciones y la revisión independiente de

los registros, cuando sea necesario, para saber quién ha hecho qué, cuándo y desde dónde.

- Las incidencias de seguridad se comunican y tratan apropiadamente.

4. ALCANCE

La presente Política de Seguridad se aplica a todas las empresas que componen el grupo Secuoya, así como a sus sistemas y activos de información, incluyendo:

- Todos los departamentos, tanto directivos como empleados.
- Contratistas, clientes, y cualquier otra tercera parte con acceso a la información o los sistemas de la organización.
- Bases de datos, archivos electrónicos y en formato papel, actividades de procesamiento, equipos, soportes, programas y sistemas.
- Información generada, procesada y almacenada, independientemente del soporte o formato, empleada en tareas operativas o administrativas.
- Información cedida en un marco legal establecido, la cual será considerada como propia exclusivamente a efectos de protección.
- Todos los sistemas empleados para la gestión y administración de información, tanto propios como alquilados o licenciados por la organización.

Esta Política de Seguridad de la Información está diseñada para soportar los sistemas de información que respaldan los procesos de gestión y servicios audiovisuales, incluyendo:

A. Producción y postproducción de contenido e información audiovisual para televisión.
B. Producción y servicios audiovisuales: experiencias avanzadas (realidad aumentada y virtual) y contenidos innovadores para marcas.

Esta política se aplica conforme a la declaración de aplicabilidad vigente y a los centros de actividad y emplazamientos permanentes de las siguientes entidades:

- CBM SERVICIOS AUDIOVISUALES, S.L. (B18911651)
- CBM MEDIA SERVICIOS DE PRODUCCIÓN, S.L. (B18893164)
- CBM SERVICIOS DE TELEVISION, S.L. (B73881716)
- SECUOYA NEXUS, S.L. (B18950642)

5. MARCO NORMATIVO

El control de la normativa y legislación de aplicación de esta política de seguridad que se incluye dentro del Sistema de Gestión de la Seguridad de la Información hace referencia, entre otras, a las siguientes normativas y leyes:

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD).
- Ley Orgánica 03/2018 de Protección de Datos y garantías de los derechos digitales (LOPDGDD).
- Ley 31/1995 de 8 de noviembre de Prevención de Riesgos Laborales y Real Decreto 39/1997 de 17 de enero, por el que se aprueba el Reglamento de los Servicios de Prevención.
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI-CE).
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica (ENS).
- Código Penal (Ley Orgánica 10/1995, de 23 de noviembre), que incluye disposiciones sobre delitos relacionados con la protección de datos y la privacidad.
- La Ley de Enjuiciamiento Criminal, relevante por su contenido en el Libro II, Título VIII, Capítulo III, que incluye disposiciones comunes a la interceptación de las comunicaciones telefónicas y telemáticas, la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, la utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen, el registro de dispositivos de almacenamiento masivo de información y los registros remotos sobre equipos informáticos.

6. CONTENIDO

6.1 Gobierno Normativo

Secuoya establece un cuerpo normativo alrededor de la Seguridad de la Información para permitir el despliegue todos aquellos recursos normativos que permitan las capacidades y protección jurídica para dar respuesta a la misión que establece el Comité de Seguridad.

Para obtener esta eficiencia se establece un sistema que se gestiona en tres niveles principales funcionales: el estratégico, el táctico y el operacional. Además, se añade un nivel técnico para adaptar la norma a las evoluciones tecnológicas de los Sistemas de la Información.

Los siguientes son los tres niveles presentes en un sistema de planificación, más el nivel técnico adaptado a los recursos de los Sistemas de la Información:

6.1.1 Nivel Estratégico o Nivel Superior

Corresponde a la planeación que se orienta a lograr los objetivos de la organización y su fin es establecer los planes de acción para el funcionamiento de la compañía. Se basa en decidir los objetivos de la empresa, definir los recursos que se usarán y las políticas para obtener y administrar dichos recursos.

Este nivel establece el marco de referencia general, pero no detallado, para el funcionamiento de Secuoya.

El nivel estratégico es conducido por el Comité de Seguridad que lo representa y aprueba.

6.1.2 Nivel Táctico o Nivel Intermedio

Desarrolla detalladamente la planeación del funcionamiento de cada una de las áreas de Secuoya a partir del marco de referencia elaborado en el nivel estratégico.

Este nivel es redactado, aprobado y validado por el Comité de Seguridad.

La diferencia básica con el nivel estratégico es que el primero se refiere a una política que afecta a toda la empresa y se extiende en el tiempo, mientras que la segunda se refiere a una norma específica en el uso de un producto, servicio, funcionamientos generales, métrica de calidad u otras que ofrece la organización con tiempos y plazos determinados.

6.1.3 Nivel Operativo o Nivel Inferior

Corresponde a normas internas que permiten ejecutar tareas de forma coordinada con otros departamentos de Secuoya que componen la compañía. Se desarrolla a partir de los lineamientos proporcionados por los niveles de planeación estratégico y táctico.

Este nivel es creado y aprobado por el Comité de Seguridad.

Los encargados de redactar esta documentación deben seguir las normas superiores y acatar reglas definidas con precisión por parte de los otros dos niveles. La norma interna de este nivel cubre periodos de tiempo específicos de acuerdo con cada proceso.

6.1.4 Nivel Funcional o Nivel Técnico

Corresponde a documentación técnica que permite a un trabajador poder utilizar una herramienta de los Sistemas de Información de Secuoya que se esté implementando para dar servicio al trabajador

La creación depende de un responsable y su publicación solo deberá constar en los sistemas internos de la organización.

6.2 Estructura Normativa

Para ello se establece el siguiente cuerpo normativo, de mayor rango a menor:

- Nivel Superior o Estratégico
  - Política Corporativa
- Nivel Medio o Táctico
  - Normativa Corporativa
- Nivel Inferior u Operativo:
  - Procedimientos Corporativos
- Nivel Técnico:
  - Guías Técnicas
  - Manuales internos
  - Manuales de fabricantes

6.3 Políticas

Secuoya debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidencias, de acuerdo con las políticas establecidas y los acuerdos de niveles de servicios comprometidos con sus clientes y usuarios.

Además, en el presente documento, trataremos cómo encaramos las políticas de la Seguridad de la Información, cómo organizamos la seguridad en la corporación, cómo garantizamos y protegemos los datos de carácter personal, la gestión del riesgo y el desarrollo de la política de la seguridad de la información.

6.4 Prevención

Secuoya se compromete a poner todos los medios a su alcance para evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidencias de seguridad. Para ello se implementarán las medidas necesarias de seguridad determinadas por la legislación que le es de aplicación, los controles estimados como necesarios establecidos en el ENS, la ISO 27001 y la ISO 20000-1, así como cualquier control adicional identificado a través de su evaluación de amenazas y riesgos.

Para garantizar el cumplimiento de la presente política, Secuoya pondrá los medios organizativos y técnicos necesarios para:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Garantizar que los riesgos a los que puede verse afectado Secuoya están identificados y se encuentran bajo niveles aceptables.
- Asegurar que los servicios que presta Secuoya a sus clientes y las actividades que desarrolla para su prestación, poseen un creciente nivel de seguridad y han pasado por las pruebas necesarias para garantizar un nivel de riesgo aceptable.
- Desarrollar e implantar todas aquellas políticas, controles y normas necesarias en materia de seguridad de la información para garantizar el cumplimiento de los requisitos del negocio, los acuerdos de niveles de servicio comprometidos y las expectativas de las personas interesadas.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

6.5 Detección

Dado que los servicios se pueden degradar rápidamente debido a incidencias, que van desde una simple desaceleración hasta su detención, es preciso monitorizar la operación de manera continua, para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia.

La monitorización es especialmente relevante cuando se establecen líneas de defensa. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables, tanto regularmente, como cuando se produzca una desviación significativa de los parámetros que se haya prestablecido como normales.

6.6 Respuesta

- Se establecen mecanismos para responder eficazmente a las incidencias de seguridad gestionados por el Comité de Seguridad.
- Pone a disposición de sus clientes y usuarios un punto de contacto para las comunicaciones de incidencias detectadas en sus operaciones (incidencias@secuoyacontentgroup.com) y también está a disposición una herramienta interna de HelpDesk (https://helpdesk.secuoyacontentgroup.com)

6.7 Recuperación

Para garantizar la disponibilidad de los servicios críticos, se han desarrollado planes de continuidad de los sistemas TIC como parte de un plan general de continuidad del servicio y actividades de recuperación.

7. ORGANIZACIÓN DE LA SEGURIDAD

Secuoya establece una definición de los siguientes comités y roles generales relacionados con su participación en la gestión y supervisión de la seguridad de la información.

- Comité de Seguridad
- Comité de Crisis

7.1 Comité de Seguridad

El Comité de Seguridad se constituye como órgano colegiado para liderar y coordinar la seguridad de la información en Secuoya, velar por el gobierno y la gestión de los riesgos de ciberseguridad, y emprender acciones para la salvaguarda y mitigación de estos.

7.1.1 Misión

Apoyar los objetivos y metas de todas y cada una de las empresas que componen el grupo, proporcionando liderazgo para garantizar la legalidad, confidencialidad, integridad, disponibilidad y trazabilidad de sus recursos de información, así como velar por el no compromiso de activos de terceros (clientes) accesibles por la actividad propia que desarrolla Secuoya con sus sistemas de información (de manera presencial o remota).

Entendemos por información:

- La propia información, como datos gestionados en los sistemas que la soportan, transmitidos a través de procesos digitales (redes, aplicaciones o cualquier tipo de mecanismo utilizado para la interoperabilidad con los sistemas objeto) o que se almacenen en dispositivos de almacenamiento, ya sean propiedad de Secuoya o de terceros.
- Los procesos, aplicaciones y sistemas de información que los soportan y que son objeto de actividad propia que desarrolla Secuoya.

En definitiva, la concienciación de todo el personal de Secuoya acerca de los riesgos en materia de ciberseguridad, la protección de los recursos de información de Secuoya, la investigación del posible mal uso de los sistemas, la supervisión del cumplimiento de todas las políticas establecidas, los procedimientos y las normas relativas al uso aceptable y adecuado de los recursos, así como el gobierno de los mecanismos de seguridad que se deriven para la protección y defensa de los sistemas objeto ante las amenazas tecnológicas que pudieran materializarse y comprometer el negocio propio o de terceros.

El Comité de Seguridad pertenece a los órganos de gestión y servicios transversales que Secuoya presta a todas las empresas y divisiones pertenecientes al grupo. Además de ser el responsable de la formalización de las políticas y de los objetivos en materia de ciberseguridad, alineados con los objetivos estratégicos de la compañía.

7.2 Roles y Responsabilidades

Un Comité de Seguridad dentro de la Política Corporativa de Seguridad de un grupo empresarial tiene roles y responsabilidades clave para asegurar la protección de los activos físicos, digitales

y humanos de la organización. Sus funciones pueden variar según la empresa, pero en general incluyen:

i. Desarrollo de la Política de Seguridad:
   - Elaboración y actualización de las políticas de seguridad, asegurándose de que estas cumplan con las normativas legales y estándares de la industria.
   - Revisión periódica de dichas políticas para adaptarlas a nuevas amenazas o cambios en el entorno empresarial.

ii. Evaluación de Riesgos:
   - Identificación y evaluación de riesgos potenciales que puedan afectar la seguridad de la empresa, tanto físicos como digitales.
   - Monitoreo continuo de amenazas emergentes y análisis de vulnerabilidades para priorizar acciones preventivas.

iii. Planificación y Estrategia:
   - Diseño de estrategias de seguridad para proteger la infraestructura, datos y personal.
   - Desarrollo de planes de respuesta a incidentes y procedimientos de emergencia.

iv. Supervisión y Coordinación:
   - Supervisión de la implementación de medidas de seguridad en todas las áreas de la empresa.
   - Coordinación con otros departamentos (TI, recursos humanos, legal) para asegurar una cobertura integral en la protección de datos y activos.

v. Capacitación y Concienciación:
   - Organización de programas de capacitación y concienciación para los empleados sobre prácticas óptimas de seguridad.
   - Promoción de una cultura de seguridad en toda la organización para fomentar comportamientos seguros.

vi. Manejo de Incidentes:
   - Gestión de incidentes de seguridad, desde la identificación hasta la resolución y documentación de lecciones aprendidas.
   - Evaluación posterior al incidente para mejorar y ajustar las estrategias de seguridad existentes.

vii. Auditorías y Cumplimiento:
   - Realización de auditorías internas de seguridad y verificación del cumplimiento de políticas.
   - Aseguramiento de la conformidad con regulaciones externas y estándares de la industria, como ISO 27001, GDPR, etc.

viii. Reportes y Comunicación:
   - Presentación de informes regulares al nivel directivo sobre el estado de la seguridad y cualquier incidente relevante.
   - Mantenimiento de canales de comunicación efectivos para alertas de seguridad y notificaciones de actualización de políticas.

ix. Mejora Continua:
   - Evaluación continua de procesos de seguridad para identificar áreas de mejora.
   - Incorporación de nuevas tecnologías y métodos de protección conforme a los avances y mejores prácticas.

En resumen, el Comité de Seguridad actúa como el principal órgano de control y toma de decisiones en cuestiones de seguridad, siendo esencial para proteger la integridad, confidencialidad y disponibilidad de los activos de la organización.

7.2.1 Gobierno y Organización

El Comité de Seguridad se constituye como un órgano colegiado, conforme a la siguiente estructura:

- Dirección de Compras y Auditoría Interna
- Director de Sistemas de Información
- Delegada de Protección de Datos

Y según la materia:

- Director de operaciones de negocio
- Responsable del servicio afectado/comprometido
- Otros perfiles específicos

Actividades propias:

- Establecimiento de la política y los objetivos de seguridad y que estos sean compatibles con las políticas y objetivos estratégicos de la organización.
- Integración de los requisitos del sistema de gestión de seguridad en los procesos de la empresa.
- Disponibilidad de los recursos necesarios.
- Establecimiento de políticas de comunicación eficientes en relación con las prácticas de ciberseguridad dentro de la organización.
- Trasladar a los proyectos los requerimientos necesarios sobre ciberseguridad.
- Dar traslado de los planes que se están elaborando, documentando y manteniendo sobre el plan de gestión de riesgos de ciberseguridad.

7.3 Comité de Crisis

Es una figura necesaria para la toma de decisiones clave para la gestión de cualquier situación de crisis que proceda de un incidente de seguridad muy grave.

En este comité se decide qué se hace y cuáles son los pasos que se tienen que dar para la resolución del problema y la gestión de la comunicación con todos los implicados.

7.3.1 Objetivos y Funciones

Entre los objetivos tenemos:

- Gestión unificada de una situación de crisis.
- Definir los principales escenarios para tener en cuenta y cómo actuar.
- Acelerar el proceso de toma de decisión para solventar incidencias y/o crisis, estableciendo prioridades, estrategias y tácticas a seguir.

Funciones:

- Decidir si se trata de una situación de crisis y de qué tipo de nivel o grado es en función del sistema de alertas y de los niveles de gravedad previamente definidos.
- Decidir si se actúa o no ante ese problema. En caso afirmativo, decidir qué se hace.
- Establecimiento de las medidas para solucionar el problema y su ejecución.

- Repartir responsabilidades dentro de las áreas de gestión del problema para facilitar su resolución y la coordinación entre todas las partes que la integran.
- Proteger la imagen pública y reputación del impacto negativo que pueda tener la situación.
- Establecer toda la política informativa durante la situación de crisis.
- Ir evaluando en cada momento la estrategia que se lleva a cabo, sus acciones y resultados.
- Detectar y prever acontecimientos y pasos a seguir en función del desarrollo de los hechos.
- Centralizar la información tanto en el plano interno como externo.
- Dotar de coherencia y unidad a todas las acciones llevadas a cabo en los diferentes niveles de intervención que sean necesarios.
- Asignación de los portavoces internos y externos.

7.3.2 Gobierno y Organización

El comité puede ser convocado a petición de la dirección o bien por un responsable de la organización. Deberá estar integrado por distintos responsables de Secuoya:

- Dirección General
- Dirección de Sistemas IT
- Dirección de Legal
- Dirección de RRHH
- Dirección de Comunicación/Marketing
- Delegada de Protección de Datos

Dependiendo de la crisis, se podrá crear el comité con las personas concretas que se requieran sin hacer participar a todos sus integrantes.

8. DATOS DE CARÁCTER PERSONAL

La LOPDGDD y el RGPD, tratan de garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor, intimidad y privacidad personal y familiar. Estas normativas resultan de aplicación a los datos de carácter personal registrados tanto informáticamente como en soporte papel.

La política de privacidad de Secuoya que regula la normativa de protección de datos se encuentra publicada en https://secuoyacontentgroup.com/politica-de-privacidad

Todos los sistemas de información de Secuoya se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos para su tratamiento.

Para garantizar dicha protección, se han adoptado las medidas de seguridad correspondientes con las exigencias previstas en la legislación de aplicación.

Todo usuario interno o externo que, en virtud de su actividad profesional, pudiera tener acceso a datos de carácter personal, está obligado a guardar secreto sobre los mismos, deber que se mantendrá de manera indefinida, incluso más allá de la relación laboral o profesional con Secuoya.

9. GESTIÓN DE RIESGOS

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se revisará:

- Regularmente, al menos una vez al año.
- Cuando cambie la información manejada.
- Cuando cambien los servicios prestados.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.

Para la armonización de los análisis de riesgos, el Comité de Seguridad establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. Desde el Comité, se dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

10. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

10.1 Sistema de Gestión de Seguridad de la Información

Para una correcta gestión del Sistema de Gestión de Seguridad de la Información (SGSI) nos basamos en las normas ISO 27001 y el Esquema Nacional de Seguridad, con la intención de adecuar de la manera más correcta posible controles de revisión periódicos, niveles de madurez, planes de implantación y mejora, etc.

Niveles de Madurez establecidos:

- Nivel 0 Inexistente: la organización no tiene una implantación efectiva del control ni de los procesos asociados.
- Nivel 1 Inicial: la organización implementa y alcanza los objetivos de los procesos.
- Nivel 2 Repetible pero intuitivo: la organización gestiona los controles y los procesos y los resultados de las actividades se establecen, controlan y mantienen.
- Nivel 3 Proceso definido y en implantación: la organización utiliza controles y procesos adaptados basados en estándares. Los procesos se describen según estándares, procedimientos, herramientas y métodos mediante guías de adaptación.
- Nivel 4 Gestionado y medible: la organización gestiona cuantitativamente los controles y procesos asociados.
- Nivel 5 Optimizado: la organización mejora continuamente los procesos, basándose en una comprensión cuantitativa de las causas comunes de variación, para cumplir los objetivos de la seguridad de la información y del negocio.

10.2 Política de Uso de los Sistemas de Información

La política interna de uso de los Sistemas de Información se comunica desde el departamento de RRHH cuando el nuevo empleado se da de alta en la organización, y puede solicitarse en cualquier momento. Esta información tiene por objeto regular la utilización de los sistemas de información propiedad de Secuoya puestos a disposición de sus trabajadores y usuarios, así como garantizar la seguridad, legalidad, rendimiento, integridad y privacidad de la información, preservar la privacidad y seguridad del personal y en general, garantizar el cumplimiento efectivo de las actividades y demás tareas que emanan del ámbito estrictamente laboral.

No se considera aceptable:

- La creación, uso o transmisión de material infringiendo las leyes de protección de datos o de propiedad intelectual.
- Instalar, modificar o cambiar la configuración de los sistemas de software (sólo los administradores de los equipos están autorizados a ello).
- El uso de Internet para fines personales (incluido el correo electrónico personal basado en Web) se limitará a los tiempos de descanso autorizados. Cualquier transacción electrónica personal que se realice será bajo la responsabilidad del usuario.
- Facilitar el acceso a las instalaciones o los servicios a personas no autorizadas deliberadamente.
- Malgastar los recursos de la red de manera premeditada.
- Corromper o destruir datos de otros usuarios o violar su privacidad intencionadamente.

- Introducir virus u otras formas de software malicioso intencionadamente. Antes de utilizar cualquier medio de almacenamiento de información, se deberá comprobar que esté libre de virus o similares.
- Revelar las contraseñas y los medios de acceso voluntariamente.
- Utilizar los equipos para lucro personal.
- La creación, utilización o transmisión de material ofensivo, obsceno o que pueda causar molestia u ofender.
- Enviar mensajes de correo muy grandes o a un grupo muy numeroso de personas (que pueda llegar a saturar las comunicaciones).
- No verificar que los correos están libres de virus.

10.3 Seguridad de la Gestión de Recursos Humanos

La seguridad ligada al personal es fundamental para reducir los riesgos de errores humanos, robos, fraudes o mal uso de las instalaciones y servicios.

Se requerirá la firma de un documento de confidencialidad, como parte de la firma del contrato, para todos los empleados para evitar la divulgación de información confidencial.

Todas las políticas y procedimientos en materia de seguridad deberán ser comunicadas regularmente a todos los trabajadores y usuarios externos, si procede. Cuando se termine la relación laboral o contractual con empleados o personal externo, se les retirarán los permisos de acceso a las instalaciones y la información y se les pedirá que devuelvan cualquier tipo de información o equipos que se les haya entregado para la realización de los trabajos.

10.4 Seguridad Física y del Entorno

Para que una seguridad lógica sea efectiva, es primordial que las instalaciones mantengan una correcta seguridad física para evitar los accesos no autorizados, así como cualquier otro tipo de daño o interferencia externa.

10.4.1 Áreas Seguras

Secuoya tomará las precauciones necesarias para que sólo las personas autorizadas tengan acceso a las instalaciones.

La totalidad de las instalaciones de Secuoya cuentan con las barreras físicas necesarias para asegurar los recursos que estas alberguen y el acompañamiento del personal durante la estancia en las instalaciones.

10.4.2 Seguridad de los Equipos

Los equipos informáticos son un activo importante del que depende la continuidad de las actividades, por lo que serán protegidos de manera adecuada y eficaz.

Los equipos informáticos de Secuoya están protegidos contra posibles fallos de energía (ordenador portátil con batería, SAIs, etc.).

Los equipos deberán mantenerse de forma adecuada para garantizar su correcto funcionamiento y su perfecto estado para que mantengan la confidencialidad, integridad y sobre todo la disponibilidad de la información. Para ello deben someterse a las revisiones

recomendadas por el proveedor. Sólo el personal debidamente autorizado podrá acceder al equipo para proceder a su reparación. También será necesario adoptar las medidas de precaución necesarias en caso de que los equipos deban abandonar las instalaciones para su mantenimiento.

10.5 Gestión de Comunicaciones y Operaciones

10.5.1 Procedimientos Operativos y Responsabilidades

Secuoya controlará el acceso a los servicios en redes internas y externas y se asegurará de que los usuarios no ponen en riesgo dichos servicios. Para ello deberá establecer las interfaces adecuadas entre la red de Secuoya y otras redes, los mecanismos adecuados de autenticación para usuarios y equipos, y los accesos para cada usuario del sistema de información.

Para evitar un uso malicioso de la red existirán mecanismos para limitar los servicios en red a los que se puede acceder, así como los procedimientos de autorización para establecer quién puede acceder a que recursos de red y los controles de gestión para proteger los accesos a la red.

Todos los empleados autorizados para el manejo de información automatizada deberán estar registrados como usuarios del dominio. Cada vez que accedan al sistema de información deberán validarse con su nombre de usuario, que será único e intransferible, y su contraseña personal. Esta contraseña caducará periódicamente.

Para asegurar la operación correcta y segura de los sistemas de información, los procedimientos de operación estarán debidamente documentados y se implementarán de acuerdo con estos procedimientos. Estos procedimientos serán revisados y convenientemente modificados cuando haya cambios significativos en los equipos o el software que así lo requieran.

En algunos casos será necesario que distintas áreas estén lógicamente separadas del resto para evitar accesos no autorizados.

10.5.2 Protección frente a Código Malicioso y Código Móvil

Queda totalmente prohibida la instalación de otro software que no sea el permitido y necesario para el desarrollo del trabajo por parte del personal de Secuoya.

Todo software adquirido por la organización sea por compra, donación o cesión es propiedad de la institución y mantendrá los derechos que la ley de propiedad intelectual le confiera, vigilando los diferentes tipos de licencias.

Cualquier software que requiera ser instalado para trabajar sobre la red deberá ser evaluado por el Comité de Seguridad.

El Administrador del Sistema instalará las herramientas informáticas adecuadas para la protección de los sistemas contra virus, gusanos, troyanos, etc. y los usuarios deberán seguir las directrices que se les indiquen para proteger los equipos, aplicaciones e información con los que trabajan.

10.5.3 Copias de Seguridad

Los datos deben ser guardados según las normas establecidas en la política de uso de los sistemas de información, para asegurar su disponibilidad.

10.5.4 Gestión de la Seguridad de la Red

Los elementos de red (switch, router...) permanecerán fuera del acceso del personal no autorizado para evitar usos malintencionados que puedan poner en peligro la seguridad del sistema.

10.6 Gestión de Soportes

Los usuarios aplicarán las mismas medidas de seguridad a los soportes que contengan información sensible que a los ficheros de donde han sido extraídos.

10.6.1 Intercambio de Información

Se establecerán procedimientos para proteger la información que se intercambie a través de cualquier medio de comunicación (electrónico, verbal, fax...).

10.6.2 Seguimiento

Según se considere necesario, se establecerán los mecanismos necesarios que permitan detectar actividades de proceso de información no autorizadas. Esto implicará realizar tareas para llevar a cabo controles e inspecciones de los registros del sistema y actividades para probar la eficiencia de la seguridad de datos y procedimientos de integridad de datos, para asegurar el cumplimiento con la política establecida y los procedimientos operativos, así como para recomendar cualquier cambio que se estime necesario.

10.7 Control de accesos

10.7.1 Requisitos del Servicio para el Control de Accesos

La información debe estar protegida contra accesos no autorizados. El responsable del servicio definirá las necesidades de acceso a la información a dos niveles, para el conjunto de áreas y para cada usuario dentro del conjunto. Sólo se facilitará el acceso a la información necesaria para el trabajo a desarrollar.

10.7.2 Gestión de Accesos de los Usuarios

El administrador del sistema es responsable de proporcionar a los usuarios el acceso a los recursos informáticos, así como el acceso lógico especializado a los recursos (servidores, enrutadores, bases de datos, etc.) conectados a la red.

Cada usuario deberá estar asociado a un perfil, de acuerdo con las tareas que desempeña en la organización, definido por su responsable directo. Cada uno de estos perfiles dispondrá de unos determinados permisos y verá restringido su acceso a información y sistemas que no le son necesarios para las competencias de su trabajo.

10.7.3 Responsabilidades del Usuario

Los puestos de trabajo del personal deben estar despejados de papeles y otros medios de almacenamiento de la información para reducir los riesgos de acceso no autorizado, así como otros posibles daños. Estos deberían guardarse en espacios cerrados adecuados, especialmente fuera del horario laboral.

10.7.4 Control de Acceso a la Red

No se permitirá el acceso a la red, a los sistemas, aplicaciones o información a ningún usuario que no esté formalmente autorizado para ello.

En el caso de proveedores de servicios o entidades externas, que necesiten acceder a ellos por un motivo justificado, se requiere que firmen acuerdos de confidencialidad con Secuoya y se les trasladen las políticas, normas y procedimientos de seguridad que deban adoptar para mantener el mismo nivel de seguridad que si fueran empleados de la propia organización.
No se recomienda el uso de servicios de VPN gratuitos o terceros para acceder a los sistemas de información de la compañía.

Se restringirá, siempre que sea posible, el acceso a los sistemas de información desde redes de anonimización (TOR, I2P, etc.) y otros servicios comúnmente utilizados para realizar acciones ilegales y cuya finalidad es la de ocultar el origen real de las conexiones.

10.7.5 Informática Móvil y Teletrabajo

Cuando los equipos o la información propiedad de Secuoya están fuera de las instalaciones, es el empleado que los está utilizando el que debe tomar las medidas pertinentes para evitar robos o daños durante su manipulación, transporte y almacenamiento.

10.8 Gestión de Incidencias

Las incidencias de ciberseguridad que cualquier empleado observe o sospeche deben ser trasladadas a el Comité de Seguridad mediante los medios que se faciliten para su comunicación, principalmente correo electrónico.

Para otras incidencias de seguridad, bien sea física (fuego, agua, etc.) o de servicios de soporte (comunicaciones, electricidad, etc.) se deben comunicar inmediatamente también a l Comité de Seguridad para que tome las medidas oportunas y registre la incidencia. En función de la gravedad, la prioridad será el uso del teléfono frente al email.

Se establecerán responsabilidades y procedimientos de gestión de incidencias para asegurar una respuesta rápida, eficaz y ordenada a los eventos en materia de seguridad.

El registro de incidencias servirá de base para identificar riesgos nuevos y para comprobar la eficacia de los controles implantados.

10.9 Continuidad del Servicio

Es imprescindible para Secuoya establecer las pautas de actuación a seguir en caso de que se produzca una interrupción de las actividades por fallos graves en la seguridad o desastres de cualquier tipo.

Para garantizar la continuidad de la actividad en estos casos, Secuoya establecerá planes de contingencia que permitan la recuperación de las actividades al menos a un nivel mínimo en un plazo razonable de tiempo. La gestión de la continuidad del servicio incluirá, por tanto, diversos controles para la identificación y reducción de riesgos y un procedimiento que limite las consecuencias dañinas de los mismos y asegure la reanudación de las actividades esenciales en el menor tiempo posible.

La estrategia de continuidad del servicio se documentará, partiendo de los riesgos detectados y de los controles definidos en consecuencia que deberán probarse y actualizarse regularmente para comprobar su idoneidad.

La gestión de la continuidad del servicio se incorporará a los procesos de Secuoya y será responsabilidad de una o varias personas dentro de la entidad.

11. OBLIGACIONES DEL PERSONAL

Todos los miembros de Secuoya tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información, siendo responsabilidad de la Oficina de Seguridad proveer los medios necesarios para que la información llegue a los afectados.

Todos los miembros de Secuoya recibirán formación y concienciación en materia de seguridad al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de Secuoya, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación como si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

12. TERCERAS PARTES

Cuando Secuoya preste servicios a otras entidades u organismos o maneje información de estas, se les hará partícipe de esta Política de Seguridad de la Información, se establecerán canales para el reporte y la coordinación de los respectivos Comités Corporativos de Seguridad y se establecerán procedimientos de actuación para la reacción ante incidencias de seguridad.

Cuando Secuoya utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dichas terceras partes quedarán sujetas a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.