uPlanner

Política de Seguridad de la Información

/uplanner

/company/u-planner

/u-planner

/uplannerEducation

1 Objetivo

Establecer las políticas, prácticas y lineamientos internos de Seguridad de la Información para uPlanner con el fin de asegurar la protección de los activos de información en todas sus formas y medios contra su modificación accidental o deliberada, utilización no autorizada, divulgación o interrupción, de modo de garantizar su confidencialidad, integridad y disponibilidad.

uPlanner establece que ante cualquier presentación legal que se requiera y esté relacionado con los sistemas informáticos o los usuarios internos, se observarán las leyes vigentes mediante el asesoramiento legal respectivo, para asegurar los requisitos regulatorios que apliquen.

2 Alcance

El presente documento es aplicable en todas las fases del ciclo de vida de la información, el cual incluye desde la creación o generación, distribución, almacenamiento, procesamiento, transporte y consulta, hasta su destrucción, así como también alcanza a todos los sistemas involucrados, áreas y personal, tanto interno como externo que trabaja o manipula de algún modo activos e información de la empresa.

3 Lineamientos

3.1 Gestión con instituciones de seguridad de la información (Controles A.6.1.3, A.6.1.4)

La gestión con instituciones de seguridad de la información tiene como objetivo establecer una conexión con organizaciones especializadas que puedan proporcionar apoyo para la implementación y mantenimiento del SGSI.

Ante la ocurrencia de un incidente de seguridad de la información, será el Senior Cloud System Administrator quien realice los contactos con autoridades internas o externas, según la naturaleza del incidente, que permitan mitigar o eliminar la amenaza que afecte la seguridad de la información.

Una vez informado un incidente que afecte la confidencialidad, integridad o disponibilidad de los activos de información, éste deberá evaluar y/o verificar que corresponde a un incidente de estas características, el cual se comunicará con la autoridad que corresponda:

Organizaciones	Contacto
Brigada Investigadora del Ciber Crimen de Policía de Investigaciones (Chile)	**Teléfono:** 2 2708 0658 **Correo electrónico:** cibercrimen@investigaciones.cl
Brigada Investigadora Delitos Contra la Propiedad Intelectual (Chile)	**Teléfono**: 2 2708 2366
Carabineros de Chile	**Teléfono**: 133
PDI (Chile)	**Teléfono**: 134

Organizaciones	Contacto
Policía Cibernética (México)	**Teléfono:** 55 5242 5100 **Correo electrónico:** ucontacto@ssc.cdmx.gob.mx
Policía Nacional de Colombia	**Teléfono:** 57 6015159111 / 9112 **Teléfono:** 123
Policía Cibernética Perú	**Teléfono:** 942 440 729 **Correo electrónico:** divindat.servicioguardia@policia.gob.pe
FBI Miami	**Teléfono:** (754) 703-2000

Para asegurar la concientización y el conocimiento de los colaboradores, la empresa también mantiene contacto con grupos de interés especial que les permite capacitarse y estar actualizados sobre las mejores prácticas, nuevas amenazas, alertas y/o vulnerabilidades de seguridad.

Empresa | Institución	Medio de contacto
Hackmetrix	Blog, Hacknews (notificaciones sobre vulnerabilidades), Hackmeets (foros sobre temas de seguridad de la información).
Microsoft Tech News	Boletín mensual enviado por correo electrónico por parte de Microsoft, con información reciente relacionado a avances tecnológicos, noticias de productos y eventos.

Empresa | Institución	Medio de contacto
uPlanner Seguridad de la Información	Equipo de Microsoft Teams para el envío de notificaciones sobre vulnerabilidades, cursos y temas de seguridad de la información a todos los usuarios uPlanner.

3.2 Gestión de protección de datos personales (Control A.18.1.4)

uPlanner comprende la importancia de la protección de datos personales y el cumplimiento de las normativas de seguridad aplicables al SGSI.

La seguridad implementada para la protección de datos de identificación personal es de manera general y consistente para toda la información de la empresa, sin distinción de la que contiene o no datos personales.

Con lo anterior garantiza que se permee la integridad, confidencialidad y disponibilidad en los datos personales que gestiona.

3.3 Gestión de los dispositivos móviles y el teletrabajo (Controles A.6.2.1, A.6.2.2)

La gestión de los dispositivos móviles y el teletrabajo tiene como objetivo asegurar el buen uso por parte de los colaboradores o partes externas, de los activos y la información de la compañía que procesan.

Por lo que uPlanner establece las siguientes medidas de seguridad en relación a los dispositivos:

- ➔ Contar con inicios de sesión seguros utilizando un usuario y contraseña robusta.
- ➔ Eliminar el software innecesario.

- Actualizar el sistema operativo y aplicaciones de forma regular.
- Mantener el antivirus y firewall encendido en todo momento.
- Colocar todos los documentos y archivos en repositorios oficiales de la empresa para que estén respaldados y disponibles.
    - En la medida de lo posible, no se descargan archivos de manera local en los dispositivos. Y de hacerlo, éstos se eliminan una vez que ya no se necesiten.
- Mantener en medida de lo posible el cifrado de disco encendido para sistemas operativos compatibles.
- Mantener un área de trabajo segura y sin información confidencial a la vista.
- Generar copias de seguridad de manera periódica siguiendo los lineamientos establecidos en la Política de Tecnología y Operaciones de TI y en el Procedimiento de Gestión de Backups definidos por la empresa.
- Limitar la conexión con redes públicas para realizar actividades de trabajo.
    - Cuando el uso de estas redes sea muy necesario, se debe utilizar una VPN.
- Transmitir información sólo por medio de redes seguras y páginas web con protocolos HTTPS, y aplicar los lineamientos establecidos en la Política de Tratamiento de la Información definida por la empresa.
- Habilitar el rastreo y borrado remoto para los posibles casos de robo o extravío.
    - Al ocurrir un robo o extravío, el colaborador debe informar de inmediato a su jefe directo y a las autoridades pertinentes.
- En casos de urgencia donde surja la necesidad de utilizar equipos de terceros, se utiliza una sesión o ventana en modalidad “incógnito” para asegurar que no se puedan rastrear las direcciones web y que no se registre una trazabilidad de las claves o contraseñas utilizadas.
- Para los dispositivos propios de los colaboradores se deben implementar los lineamientos establecidos en la Política uso correcto de dispositivos definida por la empresa.

3.3.1 Consistencia con la clasificación de la información

Al trabajar de forma remota o en movimiento, los colaboradores y partes externas se aseguran que la información es manejada de manera coherente respecto a su clasificación asignada, y de acuerdo con lo establecido en esta política.

3.3.2 Lineamientos de seguridad sobre el entorno

uPlanner establece las siguientes medidas de seguridad para proteger sus activos de información en cualquier tipo de entorno:

- Garantizar un nivel de privacidad adecuado y asegurar que personas externas no puedan ver documentos, archivos o pantallas en los que se pueda visualizar información confidencial.
- Implementar los lineamientos establecidos en la Política de Escritorios Limpios definida por la empresa.

3.4 Gestión de los recursos humanos (Controles A.7.1.1, A.7.2.3, A.8.1.4)

La gestión de los recursos humanos tiene como objetivo seleccionar a las personas más adecuadas, mantener e incluso reforzar sus competencias, conocimientos, habilidades y comportamientos éticos y garantizar la seguridad de la información de la empresa.

Para esto, uPlanner realiza las siguientes actividades:

- Diseña e implementa un Procedimiento de Preselección y Selección de Personal que:
  - Valora el talento de las personas.
  - Respeta la igualdad de oportunidades y no promueven la discriminación de ningún tipo.

- Asegura que la selección de personal se realiza con base en los criterios profesionales del candidato y alineados a las necesidades reales de la organización.
- Cumple con la legislación laboral vigente.
- Garantiza la confidencialidad y protección de los datos personales.

➔ Realiza la investigación de los candidatos de acuerdo a las regulaciones aplicables para validar la información proporcionada en la solicitud de empleo, como la identificación de la persona.

Una vez seleccionados los candidatos adecuados, se diseña e implementa un Proceso de Contratación y Desvinculación de Personal que:

➔ Asegura el establecimiento de los términos y condiciones de la relación laboral en el contrato acordado con el colaborador, incluyendo aquellos relacionados con las sanciones administrativas, la desvinculación y la devolución de todos los activos provistos por la compañía.

- Puede ocurrir el caso en que personal interno o externo incurra en alguna desviación o incumplimiento de los lineamientos de seguridad establecidos por la empresa, lo cual será motivo de sanciones administrativas e incluso legales, las cuales quedan por escrito en los contratos celebrados. Esto involucra un proceso disciplinario que considera:
  - La identificación de la actividad o comportamiento inapropiado, o la violación de las políticas internas de la organización.
  - La investigación adecuada para determinar la causa y el impacto de lo ocurrido.
  - La definición de las acciones disciplinarias apropiadas a implementar, las cuales pueden incluir una advertencia verbal, por escrito, una suspensión temporal, una terminación del contrato, una acción legal o una combinación de estas medidas.
  - El registro y documentación de las acciones disciplinarias tomadas.

- Formaliza un compromiso de confidencialidad y lealtad con el colaborador para proteger la información de la empresa.
- Brinda la inducción y concientización pertinente a los colaboradores sobre sus responsabilidades de seguridad de la información y los riesgos asociados a sus funciones, así como también de la misión y visión de la empresa.
    - Para esto además implementa un programa anual de capacitación y concientización sobre seguridad de la información para todos los colaboradores.
- Proporciona las políticas y procedimientos pertinentes que deben ser de conocimiento del colaborador para su lectura y comprensión.
- Otorga los accesos y permisos pertinentes de acuerdo al puesto asignado, siguiendo los lineamientos establecidos en esta política y el Procedimiento de Gestión de Accesos definido por la empresa.

3.5 Gestión y clasificación de los activos de información (Controles A.8.1.3, A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.2)

Los activos de información de la empresa y los recursos que le dan soporte son identificados, inventariados y clasificados en función de los requerimientos del negocio y del programa de seguridad de la empresa.

uPlanner establece una adecuada gestión de sus activos y su clasificación, por medio de las siguientes acciones:

- La identificación y mantenimiento de un inventario de activos de información que abarca todos los dispositivos.
- La asignación de propietarios de los activos de información.
- La clasificación de la información en función a sus niveles de confidencialidad, integridad y disponibilidad.
- El acceso, manejo y tratamiento adecuado de los activos de información acorde a su clasificación asignada.

uPlanner establece las siguientes categorías de clasificación:

- **Información confidencial o sensible:** Es aquella con el mayor nivel de importancia y/o custodia dentro de la organización. Su afectación puede traer consecuencias graves al negocio.
- **Información organizacional:** Es aquella con un nivel de importancia y/o custodia moderada dentro de la organización.
- **Información Organizacional Restringida**: Es aquella con un nivel de importancia y/o custodia moderada solo de algunas áreas o cargos de la organización.
- **Información pública:** Es aquella con un nivel de importancia y/o custodia mínimo e incluso nulo dentro de la organización.

La empresa realiza la clasificación de su información dentro de los registros de su Inventario de Activos.

3.5.1 Etiquetado de los activos de información

uPlanner etiqueta sus activos de información con base en su clasificación asignada para identificarlos fácil y rápidamente.

Los métodos para el etiquetado de la información que pueden ser utilizados por la empresa son:

- **Versionado**, es decir indicando la clasificación de la información dentro del control de versiones que se encuentra en la documentación.
- **Marca de agua**, incluyendo en la documentación un sello o leyenda que indique su clasificación.
- **Encabezado o pie de página**, incluyendo en la parte superior o inferior dentro de la documentación la clasificación de la información correspondiente en todas las hojas que contenga.
- **Carpeta lógica**, etiquetando una carpeta creada dentro de un equipo de cómputo o dispositivo con la clasificación de la información que tendrán todos los archivos depositados en ella.

- **Diapositiva**, indicando la clasificación de la información en la primera diapositiva o portada del documento correspondiente.

Nota importante: Toda la información que no cuente con un etiquetado explícito será considerada como información pública.

3.5.2 Intercambio de información con partes externas

uPlanner implementa políticas, procedimientos y controles formales para proteger el intercambio de información a través de los distintos medios de comunicación y acorde con la clasificación de la información a intercambiar.

La empresa define los lineamientos del intercambio de información en su Política de Tratamiento de la Información.

3.5.3 Saneamiento y destrucción de activos de información

uPlanner define los siguientes métodos de saneamiento y destrucción para garantizar que la reutilización o eliminación de activos y la información contenida en ellos sea segura:

Tipo de activo de información	Saneamiento (o borrado seguro)	Destrucción
Laptop institucional	Desconfiguración de cuenta de correo y otros sistemas organizacionales. Restaurar los valores predeterminados del proveedor.	No aplica; el equipo es reutilizado o comprado por el usuario.

3.6 Gestión de los riesgos de seguridad (Cláusula 6)

La gestión de los riesgos de seguridad dentro de la organización tiene como objetivo facilitar la identificación y evaluación de los eventos potenciales que podrían provocar la pérdida, ya sea operativa o tecnológica, que afecten la confidencialidad, integridad y/o disponibilidad de la información.

Otro de sus objetivos es establecer y priorizar planes de tratamiento adecuados que minimicen el impacto de los riesgos dentro de las operaciones de la compañía.

uPlanner establece un proceso formal dentro de su Metodología de Gestión de Riesgos que contempla lo siguiente:

- El alcance del proceso de gestión de riesgos y su necesidad de adaptación al contexto más actual de la empresa.
- La implementación de métodos para la identificación y evaluación de los riesgos de seguridad de la información.
- El análisis y decisión de los planes de tratamiento de riesgo.
- La definición del umbral de tolerancia y los criterios de aceptación de los riesgos.
- La evaluación y aceptación del nivel de riesgo residual.
- La planificación y evaluación periódica de los riesgos, la cual se realiza por lo menos una vez al año o cuando ocurran cambios significativos dentro de la empresa.

3.7 Gestión de los accesos (Controles A.9.1.1, A.9.4.1, A.9.4.2)

La gestión de los accesos tiene como objetivo asignar y controlar los roles y permisos de los usuarios del personal o partes externas, utilizados para acceder a la información, sistemas o aplicaciones de la empresa.

Para esto, uPlanner establece los siguientes lineamientos:

- Los colaboradores cuentan con un usuario único.
- Las altas, bajas y modificaciones de usuarios y/o permisos se realizan siguiendo el Procedimiento de Gestión Accesos definido por la empresa.
    - Al dar de alta a un nuevo usuario se otorgan los accesos y permisos estrictamente necesarios para llevar a cabo sus tareas de trabajo y garantizar una adecuada segregación de funciones.
    - Ante un cambio de funciones se eliminan los accesos relacionados con la función anterior y se asignan los accesos necesarios para las nuevas responsabilidades.
    - Al dar de baja a un usuario se eliminan o deshabilitan todos los accesos asociados a la persona.
- Los privilegios de administrador de los sistemas de la empresa son restringidos solo a personal capacitado y previamente autorizado.
- Los accesos son revisados periódicamente por lo menos una vez al año.
- El registro de los roles y permisos otorgados dentro de la empresa se realiza dentro de la Matriz de Accesos, la cual se actualiza conforme a los cambios que van ocurriendo.

3.8 Gestión de contraseñas e información de autenticación (Controles A.9.2.4, A.9.3.1, A.9.4.3)

La gestión de contraseñas e información de autenticación tiene como objetivo asegurar la protección de la información sensible de la empresa por medio de contraseñas robustas y siguiendo las mejores prácticas de la industria.

Para esto, uPlanner establece los siguientes lineamientos:

- Está prohibido compartir información de autenticación o contraseñas, así como también el compartir credenciales en texto plano por medios no seguros.

- Las contraseñas por defecto que proporciona el proveedor se cambian desde el primer uso.
- Las contraseñas son personales e intransferibles, y es responsabilidad del usuario hacer un buen uso de ellas.
- Las contraseñas deberán ser cambiadas de manera regular una vez al año y/o cuando sea detecta actividad sospechosa.
- No se utiliza la misma contraseña para más de un sistema o aplicación.
- Las contraseñas tienen una longitud mínima de 8 caracteres y contienen minúsculas, mayúsculas, números y símbolos.
- Se recomienda a todos los colaboradores utilizar un gestor de contraseñas.
- Se configura el segundo factor de autenticación (2FA) para todos los sistemas y aplicaciones en medida de lo posible.
- No se escriben ni resguardan PINs o contraseñas al lado de computadores, teléfonos, en libretas, notas, etcétera.

3.9 Gestión de la criptografía (Control A.10.1.1)

La gestión de la criptografía tiene como objetivo proporcionar un nivel más alto de seguridad de la información para que ésta no pueda ser leída por personas no autorizadas.

Y para esto, uPlanner utiliza métodos criptográficos que protegen la confidencialidad e integridad de su información, no solo durante su almacenamiento, sino también durante su transferencia y recepción.

Estos métodos son aplicados en los siguientes elementos:

- Credenciales de accesos.
- Información y repositorios de backups.
- Información interna restringida para la mayoría de los empleados.

- Bases de datos.
- Registros de usuarios.

Además, para ejecutar un protocolo de seguridad de criptografía eficiente, uPlanner considera lo siguiente:

- El establecimiento y gestión de las claves públicas y privadas, lo cual se realiza siguiendo el Procedimiento de Gestión de Claves Públicas y Privadas definido por la empresa.
- La autenticación de los usuarios.
- La aplicación de cifrado de mensajes y métodos de no repudio.

La organización establece que los métodos criptográficos a implementar son:

Activo de información	Método criptográfico	Especificaciones
Firma de documentos digitales	Firma electrónica	DocuSign
Almacenamiento de información en la nube	Cifrado simétrico	AES
Accesos a plataformas en trabajo remoto.	VPN	OpenVPN

3.10 Gestión de la tecnología y las operaciones (Dominio A.12)

La gestión de la tecnología y las operaciones considera todos los procesos operativos con el objetivo de garantizar la implementación de la seguridad de la información en las operaciones y servicios del negocio.

uPlanner establece los lineamientos para estos procesos dentro de la Política de Tecnología y Operaciones de TI.

3.11 Gestión de la seguridad en los sistemas y aplicaciones (Control A.12.2.1)

La gestión de la seguridad en los sistemas, aplicaciones, plataformas o cualquier otra herramienta usada por la empresa tiene como objetivo implementar y controlar la seguridad en todos los entornos que soportan los servicios y operaciones del negocio.

Y para esto, uPlanner utiliza los siguientes sistemas:

- Servicio de seguridad en correos electrónicos: (Políticas de seguridad de Office 365).
- Antimalware: (Políticas de seguridad de Office 365).
- Antivirus: (Microsoft Defender).
- WAF (Web Application Firewall): (Azure WAF).

La configuración de los sistemas mencionados anteriormente abarcan a:

- Redes y dispositivos de red.
- Dispositivos móviles.
- Sistemas de almacenamiento.
- Sistemas de virtualización.
- Bases de datos.
- Correo electrónico e internet.
- Aplicaciones en general.
- Aplicaciones web.
- Soluciones de seguridad.

Los lineamientos que se aplican a nivel de sistema operativo y de aplicaciones se encuentran definidos en la Política de Seguridad por Capas de la empresa.

3.12 Gestión de los registros de eventos (logs) (Controles A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4)

La gestión de los registros de eventos también llamados logs, tiene como objetivo registrar y monitorear las actividades realizadas en los sistemas de información de la empresa para la detección de acciones inusuales o accesos no autorizados a tiempo que permitan la prevención de incidentes de seguridad.

uPlanner establece los lineamientos para esto en la Política de Gestión de Logs y aplica las acciones definidas en el Procedimiento de Gestión de Logs.

3.13 Gestión de las vulnerabilidades técnicas (Control A.12.6.1)

La gestión de vulnerabilidades técnicas tiene como objetivo revisar constantemente los sistemas de información para identificar vulnerabilidades y posibles brechas de seguridad que puedan ser explotadas para perjudicar a la organización, y de esta manera dar solución a ellas en el modo y momento adecuado.

Dado esto, uPlanner establece lo siguiente:

- Se realiza Ethical Hacking por lo menos **una vez al año**.
- El Procedimiento de Gestión de Vulnerabilidades establecido por la empresa contempla:
  - La verificación periódica de la publicación de vulnerabilidades por parte de los fabricantes de tecnología.
  - La realización periódica de escaneos de vulnerabilidades.

- La priorización de atención para las vulnerabilidades con respecto a su criticidad e impacto.
- La generación de un plan de remediación con plazos establecidos y su seguimiento.
- La validación de la remediación por medio de retest de vulnerabilidades.

→ Para mitigar la explotación de posibles vulnerabilidades se deben mantener los sistemas actualizados en sus últimas versiones, incluyendo la instalación de los parches pertinentes.

→ La instalación de software en dispositivos propiedad de la empresa debe limitarse a actualizaciones y parches de seguridad. No se permite la instalación de nuevo software para uso personal y cuya procedencia es desconocida o sin licencia.

3.14 Gestión de la seguridad en las redes (Controles A.9.1.2, A.13.2.3, A1.4.1.3)

La gestión de la seguridad en las redes tiene como objetivo proteger la información y el tráfico de datos transmitidos por redes internas o externas, y para ello uPlanner implementa las siguientes medidas:

→ El usuario no deberá usar conexiones con redes que no sean confiables.

→ Se segregan en distintas redes los servicios, usuarios y sistemas de información de la empresa.

→ El acceso público directo entre internet y los sistemas de la organización deberá ser realizado solo por medio de una VPN.

→ Se aplican medidas de seguridad para la protección de la información transferida por medio de la mensajería electrónica contra acceso no autorizado, asegurando el correcto direccionamiento, usando canales de comunicación seguros y garantizando la disponibilidad e integridad de la información.

- Se documenta, comunica e implementa una Política de Seguridad por Capas donde se establecen las medidas aplicadas a nivel de red.
- Las páginas web de la organización utiliza protocolos de seguridad como el uso de certificados (HTTPS), autenticación de usuarios.

3.15 Gestión del ciclo de vida del desarrollo (Control A.12.1.4)

La gestión del ciclo de vida del desarrollo tiene como objetivo mantener un control adecuado de los cambios y adecuaciones, así como del mantenimiento e implementación de medidas de seguridad durante todas las fases que contempla el desarrollo de software.

Para esto, uPlanner aplica las siguientes acciones:

- Se cuenta con una segregación de ambientes para el desarrollo, pruebas y producción con el fin de minimizar los riesgos latentes en los procesos de gestión de cambios. Además, se definen los requisitos para el paso entre cada uno de los ambientes y los derechos de usuario responsables de ello.
    - Para la ejecución de las pruebas, no se utilizan datos productivos de clientes.
- Se documenta, comunica e implementa una Política de Desarrollo Seguro donde se establecen los lineamientos de seguridad pertinentes.
- Se documenta, comunica e implementa una Metodología de Ciclo de Vida de Desarrollo donde se establecen todas las actividades y controles de seguridad realizados por la empresa durante el desarrollo.
- Se documenta, comunica e implementa un Procedimiento de Gestión de Cambios Productivos donde se establece el proceso formal para el control de los cambios aplicados en los pasos a producción.
    - Los lineamientos establecidos para la gestión de cambios productivos se encuentran dentro de la Política de Tecnología y Operaciones de TI.

3.16 Gestión de las relaciones con los proveedores (Controles A.15.1.1, A.15.1.2, A.15.2.2)

La gestión de las relaciones con los proveedores tiene como objetivo asegurar un nivel apropiado de los servicios obtenidos por partes externas, así como garantizar la seguridad de los activos e información de la empresa a los que tienen acceso.

Para esto, uPlanner implementa las siguientes medidas:

- Se mantiene una lista de los proveedores de la empresa y se realiza una evaluación anual de sus servicios, la cual se documenta en la Matriz de Evaluación de Proveedores.
- Se cuenta con un contrato por escrito con cada proveedor, el cual incluye sus responsabilidades asociadas a la seguridad de la información y acuerdos de confidencialidad.
- En el documento Procedimiento de revisión y contratación de Proveedores se definen los requerimientos mínimos de seguridad para proteger la información según su clasificación asignada, y el tipo de acceso y permisos a otorgar con base en las necesidades del proveedor y del negocio.
- Se deberán comunicar las políticas y procedimientos operativos aplicables al proveedor para cumplir con todos los requisitos de seguridad establecidos por la empresa.
- Se gestiona adecuadamente la comunicación y el impacto de los posibles cambios que puedan presentarse en los contratos con proveedores, en sus servicios o cualquier aspecto dentro de la organización que afecte directa o indirectamente la relación con ellos.

3.17 Gestión de incidentes de seguridad (Control A.16.1.1)

La gestión de incidentes de seguridad tiene como objetivo llevar un adecuado análisis, registro y tratamiento de los incidentes de seguridad que puedan afectar las operaciones o servicios de la compañía.

Para esto, uPlanner define los siguientes lineamientos:

- Todos los colaboradores, clientes y proveedores deben reportar a la organización la identificación de posibles incidentes de seguridad y la ocurrencia de ellos.
- Se deben analizar, definir y registrar soluciones para todo incidente de seguridad reportado o detectado, siguiendo el Procedimiento de Gestión de Incidentes de Seguridad establecido por la empresa.
- Se deben asignar a los responsables más adecuados para atender y resolver los incidentes de seguridad y otras posibles vulnerabilidades detectadas.
- Se debe registrar toda la información relevante sobre los incidentes de seguridad, incluyendo su impacto, frecuencia y forma de resolución aplicada.
    - Esto tiene como objetivo recolectar datos sobre su comportamiento y crear una base de conocimiento a la que se pueda consultar ante la ocurrencia de eventos similares en el futuro.

3.18 Gestión de la continuidad del negocio (Control A.17.1.1)

La gestión de la continuidad del negocio tiene como objetivo asegurar que las operaciones de la empresa se mantengan funcionando adecuadamente aún durante eventos de crisis o de desastre.

Para esto, uPlanner define los siguientes lineamientos:

- La documentación, comunicación e implementación de planes de continuidad y recuperación ante desastres que garanticen la restauración de los servicios o elementos interrumpidos por eventos inesperados, y su correcto funcionamiento una vez levantados.

- La asignación de los responsables adecuados, con el conocimiento y capacitación pertinentes para la ejecución adecuada de los planes definidos por la empresa.
- El aseguramiento de los recursos necesarios para la ejecución adecuada de los planes ante un evento inesperado.
- El mantenimiento de los planes, considerando la aplicación de pruebas y la mejora continua, siguiendo los lineamientos establecidos en el Plan de Recuperación ante Desastres y el Plan de Continuidad definidos por la empresa.

3.19 Gestión del cumplimiento (Control A.18.1.1)

La gestión del cumplimiento tiene como objetivo mantener a la empresa alineada a las diferentes regulaciones y normativas a las que está sujeta.

Para esto, uPlanner realiza lo siguiente:

- Identifica y documenta los requisitos, regulaciones y normativas aplicables al giro de negocio y a la empresa en general dentro de la Matriz de Evaluación de Requisitos Legales y Contractuales.
- Verifica que los acuerdos con los colaboradores, clientes y proveedores cumplan con las pautas de las regulaciones aplicables, así como también que se identifiquen los riesgos de seguridad de la información derivados del servicio prestado o asociados a la relación con cada una de estas partes.
- Establece las políticas y procedimientos necesarios para adherirse a los requisitos regulatorios y normativos.
- Realiza revisiones de cumplimiento y auditorías internas del SGSI de manera anual.

4 Versionado

Confeccionado por:	José Garagorry (SCSA)
Código de documento:	DOC-ISO-05
Versión:	V4
Fecha última de actualización:	16/11/2023
Revisado por:	Mayra Abarca (CSA) Daniela Hellman (BI Engineer)
Aprobado por:	Comité de Seguridad de la Información.
Comunicado a:	Todos los colaboradores de uPlanner.
Fecha aprobación	30/11/2023
Clasificación de esta información:	Información Pública.

5 Control de versiones

Versión	Fecha de la Revisión	Descripción de la Revisión
V4	16/11/2023	Es agregado el recuadro de control de versiones. Es cambiado el formato del documento, pues es aplicado el último formato compartido por Hackmetrix. Es definida la periodicidad del cambio de contraseñas en el punto 3.8 Se agrega lineamiento de comunicación en apartado 3.16 para aplicar en nuevas contrataciones de proveedores a partir de la nueva versión.