POLÍTICAS INTERNAS

Este documento describe las políticas internas de Live Now Technology SLU. Estas políticas están diseñadas para garantizar un entorno de trabajo seguro y de alta calidad, cumpliendo con los requisitos legales y reglamentarios.

Código de conducta

Live Now Technology SLU se compromete a mantener los más altos estándares de **ética, profesionalismo y responsabilidad corporativa**. Este Código de Conducta se aplica a todos los empleados, contratistas y socios comerciales, garantizando un lugar de trabajo justo, inclusivo y que cumpla con la ley.

1. Prácticas comerciales éticas

En **Live Now Technology SLU** creemos que la ética y la transparencia son la base del éxito empresarial sostenible. Todas nuestras decisiones y acciones deben guiarse por... **principios de honestidad, responsabilidad y equidad**, asegurando que nuestras operaciones sean **justo, legal y alineado con los más altos estándares éticos**.

Todos los empleados, ejecutivos y socios comerciales deben adherirse a las siguientes pautas de conducta empresarial ética:

1.1 Cumplimiento de leyes y regulaciones

Live Now Technology SLU opera dentro de un marco internacional, haciendo del cumplimiento legal y regulatorio una máxima prioridad.

- Todos los empleados deben **Comprender y cumplir con las leyes locales, nacionales e internacionales** relevantes para su trabajo.
- Regulaciones de entidades internacionales como la **Unión Europea (UE), la Agencia Española de Protección de Datos (AEPD) y la Organización para la Cooperación y el Desarrollo Económicos (OCDE)** deben seguirse.
- La empresa proporcionará **capacitación periódica sobre ética y cumplimiento** para garantizar que todos los empleados se mantengan actualizados con los requisitos legales aplicables.

1.2 Política anticorrupción y antisoborno

La corrupción y el soborno representan serias amenazas a la integridad empresarial. En Live Now Technology SLU, aplicamos... **política de tolerancia cero** contra cualquier forma de corrupción.

- **Es estrictamente prohibido ofrecer, prometer, solicitar o aceptar sobornos.** en cualquier transacción comercial.
- Los empleados deben **no realizar pagos indebidos** a funcionarios gubernamentales, clientes, proveedores u otras partes interesadas.
- Si se sospecha corrupción, los empleados deben denunciarlo inmediatamente a través de **mecanismo interno de denuncia anónima.**
- La empresa realizará evaluaciones periódicas **auditorías financieras** para identificar riesgos relacionados con la corrupción.
- **Pagos de facilitación** (No se permiten pequeños pagos para agilizar procesos administrativos).

Ejemplo de mala conducta: Un empleado ofrece una "comisión especial" a un funcionario del gobierno para agilizar la aprobación de una licencia de operación. Esto es un acto ilegal que resultará en... **consecuencias disciplinarias y legales.**

1.3 Conflicto de intereses

Los empleados y ejecutivos de Live Now Technology SLU deben **tomar decisiones basadas en los mejores intereses de la empresa**, evitando situaciones en las que **el beneficio personal o los beneficios de terceros interfieren con sus responsabilidades profesionales.**

- **Incompatibilidad** surge cuando los intereses personales de un empleado **podría influir en su juicio.**
- Los empleados deben **revelar cualquier relación personal o financiera** con proveedores, clientes o competidores que puedan afectar su objetividad.
- Los empleados tienen prohibido: **mantener empleo simultáneo con competidores** o **aceptando regalos valiosos** de clientes o proveedores.
- La empresa proporciona un mecanismo para **informar y gestionar de forma transparente los posibles conflictos de intereses.**

Ejemplo de conflicto de intereses: Un empleado responsable de seleccionar un proveedor de software recomienda la empresa de su hermano para el contrato. Antes de continuar, debe... **revelar esta relación** a Recursos Humanos para evitar la toma de decisiones sesgada.

1.4 Prácticas de competencia justas y transparentes

Live Now Technology SLU promueve **competencia de mercado libre y justa**, evitando cualquier **prácticas desleales o monopolísticas.**

- Cualquiera **acuerdos de colusión o fijación de precios** con los competidores son **estrictamente prohibido**.
- Los empleados no deben compartir **información confidencial sobre precios, clientes o estrategias** con competidores de la industria.
- Se deben respetar los derechos de propiedad intelectual y **la información de la competencia no debe obtenerse ilegalmente**.
- Las relaciones comerciales con clientes y proveedores deben ser **transparentes e incluyen términos y condiciones claros**.

Ejemplo de conducta prohibida: Dos empresas tecnológicas competidoras llegan a un acuerdo **no competir en mercados específicos** para mantener precios altos. Esta práctica es ilegal y una violación de **leyes de competencia leal**.

1.5 Relaciones éticas con clientes y proveedores

Las relaciones comerciales deben basarse en **transparencia, equidad y respeto mutuo**.

- Los contratos deben ser **claro, justo y libre de cláusulas engañosas o abusivas**.
- Las condiciones de pago acordadas con proveedores y clientes deben ser **estrictamente seguidas**.
- Los empleados deben **no presionar a los proveedores para que ofrezcan precios no competitivos**.
- La selección de proveedores debe seguir **criterios objetivos y documentados**, evitando favoritismos o sesgos personales.

Ejemplo de conducta empresarial ética: Antes de firmar un contrato con un proveedor de software, un director de la empresa **revisa múltiples opciones** en el mercado y elige el más adecuado en función de **calidad, precio y servicio**.

1.6 Uso responsable de la información y protección de datos

La información de la empresa debe manejarse con **confidencialidad y responsabilidad**.

- Los empleados deben **salvaguardar la información confidencial de la empresa y de los clientes**.
- La empresa cumple con las **Reglamento General de Protección de Datos (RGPD)** para el tratamiento de datos personales.
- La información confidencial no debe compartirse con terceros **sin autorización explícita**.
- Los empleados deben evitar transmitir datos confidenciales **a través de canales no seguros**.

- Los empleados deben utilizar **Contraseñas seguras y autenticación multifactor (MFA)** en los dispositivos de la empresa.

Ejemplo de violación de protección de datos: Un empleado descargó **datos confidenciales de clientes** a su computadora personal sin autorización. Esto es un grave **Violación del RGPD** y un **riesgo de seguridad**.

1.7 Auditorías y monitoreo del cumplimiento ético

Live Now Technology SLU lleva a cabo **auditorías internas** para garantizar el cumplimiento de las prácticas comerciales éticas.

- Se realizan inspecciones y controles periódicos para **Identificar riesgos y posibles violaciones**.
- Los empleados deben **cooperar plenamente** con auditorías y proporcionar información precisa.
- Cualquier irregularidad encontrada será revisada por el **Comité de Ética**, que implementará las acciones correctivas necesarias.

Ejemplo de auditoría interna: El equipo de cumplimiento **revisa contratos recientes** con los proveedores para garantizar que **Los procedimientos se han seguido correctamente** y que hay **sin conflictos de intereses**.

Conclusión

En **Live Now Technology SLU** todos somos responsables de garantizar que **Las prácticas comerciales son éticas, transparentes y legalmente compatibles**. Nuestro compromiso con la integridad es esencial para **Construir una empresa sólida, confiable y respetada en el sector tecnológico**.

2. Conducta en el lugar de trabajo y respeto a los demás

En **Live Now Technology SLU** Nos comprometemos a fomentar un entorno de trabajo profesional, inclusivo y respetuoso donde todos los empleados se sientan seguros, valorados y capacitados para contribuir a nuestro éxito colectivo. **Creemos que una cultura laboral positiva y ética es esencial para el bienestar de los empleados, la productividad y el crecimiento general de la organización.**

Esta sección establece las pautas y expectativas de conducta en el lugar de trabajo, enfatizando el respeto mutuo, la equidad y la adhesión al comportamiento ético en todas las interacciones profesionales.

2.1 Compromiso con un entorno de trabajo profesional e inclusivo

Live Now Technology SLU se dedica a crear un **Lugar de trabajo libre de discriminación, acoso e intimidación**. Esperamos que cada empleado, contratista y socio comercial actúe con **respeto, integridad y profesionalismo** en todo momento.

- **Respeto por la diversidad y la inclusión:** Celebramos la diversidad y creemos que un lugar de trabajo inclusivo fomenta la creatividad, la innovación y la excelencia. **Discriminación. basado en raza, género, edad, discapacidad, orientación sexual, religión, nacionalidad o cualquier otra característica** Está estrictamente prohibido.
- **Igualdad de oportunidades de empleo:** Todas las decisiones de empleo, como contrataciones, ascensos, aumentos salariales y capacitación, deben basarse **puramente en base al mérito, desempeño y calificaciones** Sin sesgo.
- **Conciencia cultural:** Los empleados que trabajan en un entorno global o multicultural deben ser conscientes de **diferencias culturales** y practicar el respeto en todas las interacciones profesionales.

Ejemplo de conducta positiva en el lugar de trabajo: Un gerente de contratación se asegura de que todos los candidatos al puesto sean evaluados **basado en habilidades y experiencia**, en lugar de características personales como el género o la nacionalidad.

× Ejemplo de comportamiento inapropiado: Un empleado de alto nivel constantemente **ignora** la aportación de un colega más joven basada en prejuicios relacionados con la edad. Esto es inaceptable y debe denunciarse.

2.2 Política contra el acoso y la intimidación

El acoso, la intimidación y cualquier forma de hostilidad en el lugar de trabajo son **estrictamente prohibido**. En Live Now Technology SLU, definimos el acoso como **cualquier comportamiento no deseado que cree un ambiente de trabajo intimidante, hostil u ofensivo**.

- **Acoso sexual:** Insinuaciones no deseadas, bromas inapropiadas, comentarios sugerentes o cualquier comportamiento de naturaleza sexual que **hace que un empleado se sienta incómodo**. No será tolerado.
- **Acoso verbal y físico:** El lenguaje insultante, los gestos ofensivos, el comportamiento agresivo o las amenazas no son aceptables bajo ninguna circunstancia.
- **Ciberbullying y acoso digital:** Los empleados no deben participar en **acoso en línea**, incluidos correos electrónicos ofensivos, humillación pública o mensajes inapropiados en plataformas de comunicación (Slack, Teams, etc.).
- **Procedimientos de escalada:** Si un empleado siente que ha sido acosado o intimidado, debe denunciar el problema a través de **Canal de comunicación interna de empleados (mecanismo de denuncia anónima)** para investigación inmediata.

Ejemplo de acoso laboral: Un gerente **hace comentarios repetidos** sobre la apariencia física de un empleado de una manera que lo incomode. Esto debe reportarse a Recursos Humanos de inmediato.

2.3 Relaciones laborales y profesionalismo

- **Mantener los límites profesionales:** Si bien se fomentan las relaciones amistosas, los empleados deben **mantener una conducta profesional en todo momento** y evitar **familiaridad excesiva o favoritismo** en el lugar de trabajo.
- **Cómo evitar conflictos de intereses en las relaciones laborales:** Empleados que participan en **relaciones románticas o personales** con colegas o gerentes **debe revelar la relación** si crea un conflicto de intereses.
- **Comunicación profesional:** Todas las comunicaciones internas y externas deben realizarse de manera **manera cortés, respetuosa y constructiva**—ya sea en correos electrónicos, reuniones o herramientas de colaboración en línea.
- **Código de vestimenta y apariencia profesional:** Los empleados deben presentarse de una manera que refleje **profesionalismo y respeto por el ambiente laboral**. Si bien permitimos flexibilidad, los empleados deben seguir **directrices de la empresa** respecto a los estándares de vestimenta apropiados.

Ejemplo de comportamiento profesional: Durante un desacuerdo en una reunión, dos empleados **Discutir sus diferentes opiniones con respeto y profesionalismo.**, en lugar de alzar la voz o realizar ataques personales.

✗ Ejemplo de conducta no profesional: Un empleado frecuentemente **interrumpe y despid**e colegas en discusiones de equipo, creando un **ambiente de trabajo hostil**.

2.4 Seguridad y salud en el trabajo

La salud y la seguridad de los empleados son de **importancia extrema** a Live Now Technology SLU. Nos comprometemos a brindar un **entorno de trabajo seguro y libre de riesgos** y promover **bienestar físico y mental**.

- **Cumplimiento de las normas de seguridad:** Los empleados deben **adherirse a los protocolos de seguridad** e informar inmediatamente sobre cualquier condición peligrosa o riesgo de seguridad.
- **Preparación para emergencias:** Los empleados deben familiarizarse con **procedimientos de emergencia, salidas de incendio y recursos de primeros auxilios** disponible en el lugar de trabajo.
- **Salud mental y bienestar:** La empresa promueve el equilibrio entre la vida laboral y personal y anima a los empleados **buscar apoyo** para cualquier problema de salud mental. **Medidas de prevención del burnout** se apoyan activamente las iniciativas de bienestar y la distribución razonable de la carga de trabajo.
- **Política sobre abuso de alcohol y sustancias:** El consumo de alcohol o sustancias ilegales **durante el horario laboral o en las instalaciones de la empresa** está estrictamente prohibido, excepto durante eventos oficiales de la empresa en los que se puede permitir el consumo de alcohol. **manera responsable**.

Ejemplo de una violación de seguridad en el trabajo: Un empleado **No informa de un cable eléctrico suelto**, lo que supone un riesgo para la seguridad que podría haberse evitado.

2.5 Confidencialidad en el lugar de trabajo y protección de datos

Los empleados deben **Manejar la información de la empresa de manera responsable** y proteger los datos confidenciales del acceso no autorizado.

- **Acuerdo de confidencialidad:** Los empleados no deben revelar **secretos comerciales de la empresa, datos financieros, información del cliente o detalles del proyecto** sin la debida autorización.
- **Uso adecuado de los sistemas informáticos:** Los empleados deben utilizar **dispositivos corporativos, correos electrónicos y plataformas de software** de forma responsable y evitar exponer los sistemas de la empresa a riesgos de seguridad.

- **Seguridad en el trabajo remoto:** Los empleados que trabajan de forma remota deben **asegurar su entorno de trabajo**, usar **VPN, comunicación cifrada**, y evitar **Wi-Fi público** para el manejo de datos de la empresa.
- **Notificación de violaciones de datos:** Si un empleado sospecha que **violación de datos o vulnerabilidad de seguridad**, deberán informarlo inmediatamente a la **Equipo de seguridad informática**.

Ejemplo de violación de protección de datos: Un empleado descarga archivos de la empresa **en una unidad USB personal** y luego lo pierde, exponiendo información comercial confidencial. Esto es un **grave riesgo de seguridad**.

2.6 Resolución de conflictos y disputas en el lugar de trabajo

Los desacuerdos en el lugar de trabajo son inevitables, pero deben resolverse de manera **manera profesional y constructiva**.

- **Fomentar el diálogo abierto:** Se anima a los empleados a comunicarse abiertamente y **abordarse refiere directamente** antes de que se intensifiquen las disputas.
- **Uso de los servicios de mediación:** Si los conflictos persisten, RRHH puede facilitar un **proceso de mediación neutral** para encontrar una resolución apropiada.
- **Tolerancia cero a las represalias:** Los empleados deben **Nunca enfrentes represalias** para informar sobre un problema o disputa en el lugar de trabajo.

Ejemplo de resolución adecuada de conflictos: Dos miembros del equipo tienen un desacuerdo sobre la dirección de un proyecto, pero **programar una reunión** para discutir soluciones con calma y colaboración.

✗ Ejemplo de comportamiento indebido: Un empleado **difunde rumores negativos** sobre un colega después de un desacuerdo en el lugar de trabajo, en lugar de resolver el problema profesionalmente.

Conclusión

En **Live Now Technology SLU** nuestra cultura laboral se basa en **respeto mutuo, profesionalismo e inclusión**. Cada empleado tiene la responsabilidad de **contribuir a un ambiente de trabajo positivo**, garantizando que nuestro lugar de trabajo siga siendo un espacio donde prosperen el talento, la innovación y el trabajo en equipo.

3. Protección de datos y confidencialidad

En **Live Now Technology SLU** reconocemos que **Los datos son uno de nuestros activos más valiosos** y que proteger la información confidencial es fundamental para mantener la confianza, garantizar la continuidad del negocio y cumplir con los requisitos legales y regulatorios. Nos comprometemos a salvaguardar **datos personales, de clientes y de la empresa** en cumplimiento de **RGPD (Reglamento General de Protección de Datos)** y otras leyes aplicables.

Esta sección describe nuestras **políticas, responsabilidades y mejores prácticas** respecto a la recopilación, manejo, almacenamiento y compartición de información dentro de la empresa.

3.1 Cumplimiento de las leyes de protección de datos (RGPD y otras regulaciones)

Live Now Technology SLU se adhiere estrictamente a las **RGPD**, que regula la recopilación, el procesamiento, el almacenamiento y la transferencia de **datos personales y corporativos** dentro de la Unión Europea.

Principios clave de protección de datos (según el RGPD):

- 1. Legalidad, equidad y transparencia:** Los datos deben ser recopilados y procesados **de manera legal y transparente**.
- 2. Limitación de la finalidad:** La información sólo se puede utilizar para **fines comerciales legítimos**.
- 3. Minimización de datos:** Sólo el **cantidad necesaria de datos** deben recogerse y almacenarse.
- 4. Exactitud:** Los datos deben ser **mantenerse actualizado** y corregido si es inexacto.
- 5. Limitación de almacenamiento:** Los datos personales deben **no se conservará más tiempo del necesario**.
- 6. Integridad y confidencialidad:** Los datos deben ser **Protegido contra accesos no autorizados y amenazas cibernéticas**.
- 7. Responsabilidad:** La empresa debe demostrar **cumplimiento de las políticas de protección de datos** en todo momento.

△ **Ejemplo de violación de protección de datos:** Un empleado recopila información personal de los clientes y luego la comparte con un tercero **sin consentimiento**—esto es un **Incumplimiento del RGPD**.

3.2 Responsabilidades de los empleados en materia de protección de datos

Todos los empleados deben asegurarse la **confidencialidad, integridad y seguridad de los datos de la empresa y de los clientes**.

Responsabilidades obligatorias de los empleados:

- **Maneje los datos confidenciales con cuidado:** Los empleados deben evitar exponer o hacer mal uso de los datos de la empresa.
- **Utilice métodos de almacenamiento seguros:** Los registros físicos y digitales deben ser **almacenado de forma segura** (por ejemplo, archivos cifrados, armarios cerrados).
- **Informar sobre violaciones de datos:** Si un empleado sospecha **acceso no autorizado, filtraciones o infracciones**, deben reportarlo **inmediatamente** a la seguridad informática.
- **Seguir las políticas de control de acceso:** Los empleados deben **no compartir contraseñas ni credenciales de acceso** con personas no autorizadas.
- **Eliminar datos de forma segura:** Los documentos y archivos que contienen datos confidenciales deben **correctamente eliminado o triturado** cuando ya no sea necesario.

Ejemplo de mala conducta de un empleado: Un empleado **Imprime contratos confidenciales de clientes y los deja sin supervisión** en un escritorio de oficina compartido.

3.3 Tratamiento de datos personales y de clientes

Los datos personales de los clientes y empleados deben ser tratados con **máximo cuidado** y en cumplimiento con el RGPD.

Reglas para el Tratamiento de Datos Personales:

- Recopilar y procesar datos **sólo con consentimiento explícito**.
- Utilizar datos personales **únicamente para el propósito para el cual fue recopilado**.
- Implemente **cifrado y controles de acceso** al almacenar información personal.
- Limitar el acceso a los datos **sólo a personal autorizado**.
- Anonimizar o seudonimizar los datos siempre que sea posible para reducir el riesgo.

Ejemplo de comportamiento conforme: Un equipo de marketing **pide consentimiento explícito** antes de agregar el correo electrónico de un cliente a una lista de correo.

× Ejemplo de una violación del RGPD: Un empleado de recursos humanos **comparte la información salarial de un colega** con una persona no autorizada.

3.4 Comunicación segura y uso del sistema de TI

Los empleados deben **Siga las mejores prácticas para una comunicación segura** y garantizar que todos los sistemas de TI corporativos estén **Protegido contra amenazas cibernéticas**.

Pautas de seguridad informática:

- **Uso contraseñas seguras** y actualizarlos periódicamente.
- **Habilitar autenticación multifactor (MFA)** para correo electrónico, bases de datos y servicios en la nube.
- **No abrir correos electrónicos o archivos adjuntos sospechosos** que pueden contener intentos de phishing.
- Almacenar archivos de la empresa únicamente en **ubicaciones autorizadas (por ejemplo, almacenamiento en la nube cifrado, servidores de la empresa)**.
- Utilice VPN aprobadas por la empresa para **acceso remoto** a los sistemas internos.

△ **Ejemplo de riesgo de seguridad informática:** Un empleado **Descarga archivos confidenciales en una computadora portátil personal** que carece de medidas de seguridad, lo que lo hace vulnerable a ciberataques.

3.5 Obligaciones de confidencialidad y acuerdos de no divulgación (NDA)

Todos los empleados son **legalmente obligado a mantener la confidencialidad** respecto a información de la empresa y del cliente.

Reglas clave de confidencialidad:

- No discutir **asuntos confidenciales de la empresa** en lugares públicos o entornos no autorizados.
- No revele información confidencial a **amigos, familiares o competidores**.
- Empleados **debe firmar un NDA (Acuerdo de confidencialidad)** antes de acceder a datos confidenciales.
- El incumplimiento de las obligaciones de confidencialidad puede dar lugar a: **Acción disciplinaria, despido y consecuencias legales**.

Ejemplo de violación de confidencialidad: Un empleado **filtraciones de estrategias comerciales** a un competidor a cambio de una ganancia personal. Esto es motivo de **Terminación inmediata y acción legal**.

3.6 Informes de violación de datos y respuesta a incidentes

En caso de una **violación de datos**, los empleados deben actuar **de forma rápida y responsable** para minimizar el riesgo y evitar daños mayores.

Pasos inmediatos en caso de una violación de datos:

1. **Informar sobre la infracción** inmediatamente a la **Delegado de Protección de Datos (OPD)** o Seguridad TI.
2. **Proteger los datos afectados** y tratar de **contener la brecha** (por ejemplo, revocar el acceso no autorizado).
3. **Ayudar en la investigación** proporcionando detalles relevantes y cooperando con los equipos de seguridad interna.
4. **Cumplir con los requisitos de notificación del RGPD** si la violación involucra datos personales (clientes o empleados).

Ejemplo de una respuesta adecuada: Un empleado **advierte acceso no autorizado** a archivos de proyectos confidenciales y **Lo informa inmediatamente a Seguridad Informática.**, evitando una mayor exposición.

3.7 Manejo de datos de terceros y seguridad de proveedores

Al trabajar con **proveedores externos, consultores o socios** Live Now Technology SLU garantiza que los terceros cumplan con **nuestros estándares de seguridad de datos**.

Requisitos de protección de datos de terceros:

- Los vendedores deben **firmar un Acuerdo de Procesamiento de Datos (APD)** antes de manipular datos de la empresa.
- El acceso de terceros a los sistemas de la empresa debe ser **limitado y monitoreado**.
- Todos los proveedores de servicios externos deben cumplir **estándares de seguridad de la industria** y **Cumplimiento del RGPD**.

Ejemplo de buena práctica: Antes de trabajar con un proveedor de almacenamiento en la nube, la empresa **revisa sus políticas de seguridad** y garantiza que cumplan con **ISO 27001 y RGPD**.

3.8 Programas de capacitación y concientización de empleados

Live Now Technology SLU lleva a cabo **formación obligatoria en protección de datos** para garantizar que todos los empleados comprendan sus responsabilidades en el manejo seguro de datos.

Los temas de capacitación incluyen:

- Cumplimiento del RGPD y requisitos legales.
- Reconocer y prevenir amenazas a la ciberseguridad (por ejemplo, phishing, malware).
- Mejores prácticas para el almacenamiento y uso compartido seguro de datos.
- Uso adecuado del correo electrónico corporativo y herramientas de comunicación.

Ejemplo de conciencia de seguridad: Un empleado **reconoce un correo electrónico de phishing** intentar robar credenciales de inicio de sesión y lo informa a Seguridad TI antes de que se produzca algún daño.

Conclusión

En **Live Now Technology SLU**, proteger la información confidencial es **responsabilidad de todos**. Los empleados deben **seguir estas políticas estrictamente** para salvaguardar los activos de la empresa, mantener la confianza del cliente y **cumplir con las regulaciones GDPR**.

4. Uso de los recursos de la empresa

En **Live Now Technology SLU** reconocemos que **recursos de la empresa** son activos críticos que nos permiten operar eficientemente, innovar y brindar servicios de alta calidad. Cada empleado tiene la responsabilidad de **Utilizar estos recursos de manera responsable, ética y en consonancia con los objetivos de la empresa**. Esta sección proporciona pautas claras sobre cómo los empleados deben manejar **Tecnología, propiedad intelectual y esfuerzos de sostenibilidad** para garantizar la integridad y eficiencia de nuestras operaciones.

4.1 Uso responsable de los activos de la empresa

Activos de la empresa, incluidos **equipos físicos, sistemas de TI, software y propiedad intelectual**, se proporcionan para **Sólo para fines comerciales**. Los empleados deben respetar y proteger estos activos para evitar pérdidas, robos, daños o mal uso.

Reglas generales para el uso de los activos de la empresa:

- **Utilice los recursos de manera eficiente:** No desperdicie materiales, electricidad ni útiles de oficina.
- **Proteger los equipos de la empresa:** Mantenga las computadoras, dispositivos y herramientas seguros contra daños o pérdidas.
- **Reportar inmediatamente el mal uso o robo:** Notifique a la gerencia si sospecha cualquier uso no autorizado o violación de seguridad.
- **Mantener el profesionalismo:** Los recursos de la empresa deben utilizarse de manera que estén en consonancia con los valores corporativos y los estándares éticos.

Ejemplo de mala conducta: Un empleado **se lleva a casa el equipo de la empresa** (por ejemplo, una computadora portátil) para uso personal sin permiso, violando las políticas de activos de la empresa.

Ejemplo de cumplimiento: Un empleado **bloquea su estación de trabajo** al dejar su escritorio para evitar el acceso no autorizado.

4.2 Tecnología y sistemas de TI

Sistemas de TI, incluidos **computadoras, redes, software y servicios en la nube de la empresa**, debe utilizarse estrictamente para **fines comerciales legítimos**. Los empleados están obligados a seguir **mejores prácticas de ciberseguridad** para proteger los sistemas de la empresa de **acceso no autorizado, malware y violaciones de datos**.

Política de seguridad informática y uso aceptable:

- **Utilice contraseñas seguras:** Los empleados deben establecer **contraseñas únicas y complejas** para todos los sistemas de la empresa y habilitar **autenticación multifactor (MFA)** donde se aplica.
- **No instale software no autorizado:** Todo software debe ser aprobado por el departamento de TI.
- **Actividades prohibidas:** Los empleados no deben acceder, descargar ni compartir **contenido ilegal, ofensivo o inapropiado** utilizando dispositivos o redes de la empresa.
- **Informar sobre actividad sospechosa:** Si un empleado nota un **correo electrónico de phishing, infección de malware o amenaza de seguridad**, deberán reportarlo a Seguridad Informática inmediatamente.
- **Limitar el uso personal:** Si bien se puede tolerar un uso personal mínimo de los recursos de TI de la empresa, se prohíbe su uso excesivo o inapropiado.

△ **Ejemplo de una violación de seguridad:** Un empleado **descarga software no autorizado** en una computadora portátil de la empresa, exponiendo la red a amenazas de ciberseguridad.

Ejemplo de cumplimiento: Un empleado **Sigue la formación en seguridad informática**, reconocer y denunciar un intento de phishing antes de que se produzca cualquier daño.

Prácticas de TI estrictamente prohibidas:

- **Usar unidades USB personales o almacenamiento externo** Transferir datos de la empresa sin la aprobación del departamento de TI.
- **Evitando los controles de seguridad** intentar piratear áreas restringidas de los sistemas de la empresa.
- **Compartir credenciales de la empresa** con personas no autorizadas.

4.3 Propiedad intelectual (PI) e información confidencial

Los empleados deben **respetar y proteger la propiedad intelectual** pertenecientes a Live Now Technology SLU, así como organizaciones externas, socios y competidores.

Tipos de propiedad intelectual (PI) cubiertos:

- **Marcas comerciales y branding**—Los empleados no pueden alterar ni hacer mal uso de los logotipos, elementos de marca o documentos oficiales de la empresa sin autorización.
- **Materiales con derechos de autor**—Los empleados deben **No reproducir, distribuir ni utilizar materiales con derechos de autor.** (por ejemplo, software, imágenes, documentos) sin permiso.

- **Patentes y tecnología patentada**—Los empleados deben proteger las innovaciones, patentes y tecnologías patentadas de la empresa contra la divulgación no autorizada.

△**Ejemplo de una violación de propiedad intelectual:**Un empleado **comparte código de software propietario con un competidor**, lo que constituye una grave violación de los derechos de propiedad intelectual.

Ejemplo de cumplimiento:Un empleado debidamente **cita una investigación externa** al utilizar materiales de terceros en presentaciones o informes.

Actividades estrictamente prohibidas:

- Descarga y uso **software pirateado** en los dispositivos de la empresa.
- Copiar o compartir **archivos confidenciales del proyecto** con **terceros no autorizados**.
- **Uso de marcas comerciales de la empresa** para **personal o no relacionado con el negocio** proyectos sin aprobación.

Mejores prácticas para proteger la propiedad intelectual:

- Siempre verifique **acuerdos de licencia** antes de utilizar materiales de terceros.
- Tienda **archivos confidenciales en ubicaciones seguras aprobadas por la empresa** (por ejemplo, almacenamiento en la nube cifrado).
- **Etiquete adecuadamente los documentos confidenciales** para evitar compartir involuntariamente.

4.4 Sostenibilidad y responsabilidad ambiental

En **Live Now Technology SLU** estamos comprometidos con **reduciendo nuestro impacto ambiental** y **Promoviendo la sostenibilidad** en todos los aspectos de nuestras operaciones. Se anima a los empleados a **adoptar prácticas ecológicas** y ayudar a la empresa a implementar **iniciativas verdes**.

Prácticas clave de sostenibilidad:

1. Conservación de energía:

- Apagar **computadoras, luces y equipos de oficina** cuando no esté en uso.
- Utilice dispositivos energéticamente eficientes y fomente el uso de **modo de bajo consumo** ajustes.

2. Reducción de papel y recursos:

- Uso **Documentación digital en lugar de impresión** siempre que es posible.
- Imprimir **de dos caras** y utilice papel reciclado cuando sea necesario imprimir.

3. Gestión de residuos y reciclaje:

- Los empleados deben separarse **residuos reciclables** (por ejemplo, papel, plástico, residuos electrónicos) de forma adecuada.
- Reducir **plásticos de un solo uso** mediante el uso de botellas de agua y vasos reutilizables.

4. Viajes y desplazamientos sostenibles:

- Se anima a los empleados **utilizar el transporte público, compartir coche o trabajar de forma remota** Opciones para reducir la huella de carbono.
- Si viaja por trabajo, seleccione **Alojamientos ecológicos y opciones de transporte** Siempre que sea posible.

Ejemplo de una práctica sostenible: Empleados **Utilice herramientas de almacenamiento en la nube y colaboración digital** en lugar de imprimir documentos físicos para las reuniones.

Ejemplo de negligencia ambiental: Un empleado **deja varios dispositivos funcionando durante la noche innecesariamente**, desperdiciando electricidad.

Compromiso de sostenibilidad de la empresa: Live Now Technology SLU se compromete a:

- Evaluar periódicamente **huella de carbono** y reducir las emisiones siempre que sea posible.
- Implementar **políticas de TI verdes**, incluidos centros de datos energéticamente eficientes y adquisiciones sostenibles.
- Educar a los empleados sobre **iniciativas de responsabilidad social corporativa (RSC) y sostenibilidad**.

4.5 Denuncia de infracciones y búsqueda de orientación

Empleados que **Presenciar o sospechar el uso indebido de los recursos de la empresa** Debería informar el problema **confidencialmente** a:

Departamento de Seguridad Informática (por violaciones de TI)

Equipo Legal y de Cumplimiento (por cuestiones de propiedad intelectual)

Oficial de Sostenibilidad (por preocupaciones sobre el impacto ambiental)

Política de no represalias: Los empleados **no enfrentan el castigo** para informar de buena fe sobre preocupaciones relacionadas con el uso indebido de los activos de la empresa.

Conclusión

Live Now Technology SLU espera que todos los empleados **Utilizar los recursos de la empresa de manera responsable, ética y eficiente**. Para garantizar la seguridad, la innovación y la sostenibilidad. Al seguir estas directrices, los empleados contribuyen a... **Lugar de trabajo seguro, productivo y respetuoso con el medio ambiente**.

5. Denuncia de infracciones y protección de los denunciantes

En **Live Now Technology SLU** estamos comprometidos a mantener los más altos estándares de **ética, integridad y transparencia**. Para garantizar la rendición de cuentas y defender nuestra **Código de conducta**, proporcionamos a los empleados un **mecanismo de denuncia seguro y anónimo** por violaciones o comportamiento poco ético.

Los empleados deben sentirse capacitados para **Reportar preocupaciones sin temor a represalias**, sabiendo que todos los informes serán **manejados de forma confidencial e investigados a fondo**. Esta sección detalla los procedimientos de denuncia, las protecciones establecidas y cómo se llevan a cabo las investigaciones para mantener un **lugar de trabajo justo y responsable**.

5.1 Importancia de denunciar infracciones

Todo empleado tiene la responsabilidad de: **mantener estándares éticos** y denunciar cualquier comportamiento que **viola las políticas, leyes o pautas éticas de la empresa**. La notificación rápida de inquietudes ayuda **Prevenir que la mala conducta se intensifique** y protege a la empresa, a los empleados y a las partes interesadas.

Tipos de infracciones que deben denunciarse:

- ✓ **Fraude, corrupción o mala conducta financiera**–Uso no autorizado de fondos de la empresa, falsificación de registros o soborno.
- ✓ **Acoso o discriminación**–Cualquier forma de acoso, racismo, acoso sexual o trato injusto.
- ✓ **Conflictos de intereses**–Empleados que participan en actividades comerciales que entran en conflicto con los intereses de la empresa.
- ✓ **Violación de la confidencialidad**–Intercambio no autorizado de información confidencial de la empresa.
- ✓ **Amenazas a la ciberseguridad y mal uso de las TI**–Acceso no autorizado, piratería o violaciones de seguridad intencionales.
- ✓ **Violaciones de seguridad en el lugar de trabajo**–No adherirse a **normas de salud y seguridad** poniendo en peligro a sus compañeros.
- ✓ **Incumplimiento ambiental**–Violaciones a las políticas de sostenibilidad o disposición inadecuada de residuos.

Ejemplo de mala conducta: Un gerente **Presiona a un empleado para que manipule registros financieros** para beneficio personal.

Ejemplo de cumplimiento: Un empleado informa **transacciones financieras sospechosas**. Lo descubrieron en una auditoría.

5.2 Mecanismos de denuncia

Los empleados pueden **denunciar infracciones de forma segura y confidencial** a través de múltiples canales:

Canal de comunicación interna de empleados (mecanismo de denuncia anónima)

- Los empleados pueden enviar informes **anónimamente** a través de un cifrado **portal de denuncia de irregularidades**.
- Este canal es monitoreado por **oficiales de cumplimiento y un comité de ética independiente** para garantizar un manejo justo de todos los informes.

Reporte directo al Departamento de Recursos Humanos o de Cumplimiento

- Los empleados pueden reportar inquietudes **directamente a los equipos de RR.HH. o Legal & Compliance** si prefieren revelar su identidad.

Política de denuncia anónima:

- Los empleados **no están obligados a revelar su identidad** al presentar un informe.
- Todos los informes son tratados con el **más alto nivel de confidencialidad** para proteger la privacidad del denunciante.
- **Los informes anónimos se tomarán con la misma seriedad**, según informes identificados e investigados a fondo.

⚠ **Importante: Acusaciones falsas** o informes realizados en **mala fe** (por ejemplo, por venganza personal o información engañosa) puede resultar en **acción disciplinaria**.

5.3 Política de no represalias

En **Live Now Technology SLU**, mantenemos una **política estricta de no represalias** para **proteger a los empleados** que denuncian sus preocupaciones de buena fe. **Ningún empleado debería temer el castigo, la degradación o el despido**, por plantear preocupaciones legítimas sobre violaciones.

Las protecciones para denunciantes incluyen:

- ✓ **Seguridad laboral:** Empleados **no puede ser despedido, degradado o penalizado** para informar inquietudes.
- ✓ **Confidencialidad:** Las identidades serán **Mantenido anónimo y protegido** a menos que el empleado elija lo contrario.
- ✓ **Protección contra represalias en el lugar de trabajo:** Nadie puede **acosar, aislar o intimidar** un empleado por hablar.

Ejemplo de represalia (estrictamente prohibido): Un gerente **Reduce la carga de trabajo de un empleado y lo excluye de las reuniones.** después de denunciar conductas poco éticas.

Ejemplo de cumplimiento: Una empresa **promueve una cultura de transparencia,** garantizando que los denunciantes se sientan seguros y escuchados.

5.4 Proceso de investigación

Todos los informes serán **investigarse con prontitud, imparcialidad y exhaustividad** para garantizar la equidad y la rendición de cuentas.

Cómo se llevan a cabo las investigaciones:

1 Acuse de recibo del informe:

- El **denunciante recibe confirmación** que su informe ha sido presentado.

2 Revisión inicial:

- El Departamento de Cumplimiento **evalúa la gravedad del reclamo** y determina si es necesaria una investigación completa.

3 Investigación del Comité de Ética:

- Un equipo de **investigadores independientes** Realizará entrevistas, recopilará evidencia y analizará informes.
- Los empleados involucrados serán **tratado justamente** y se les dio la oportunidad de presentar su versión.

4 Resolución y acciones correctivas:

- Si se confirma la mala conducta, **acciones disciplinarias apropiadas** (Se tomarán advertencias, suspensiones o acciones legales).
- Si es necesario, **Las políticas de la empresa pueden actualizarse** para prevenir futuras violaciones.

5 Seguimiento del denunciante:

- Los empleados que presentaron informes serán **actualizado sobre el resultado** manteniendo la confidencialidad.

Estricta confidencialidad: La identidad del denunciante **Nunca será revelado** sin su consentimiento.

Ejemplo de una investigación justa: Un equipo de RRHH revisa la evidencia y entrevista a los empleados antes de tomar una decisión sobre un caso denunciado de acoso laboral.

5.5 Fomentar una cultura de expresión abierta

En Live Now Technology SLU creemos que fomentar una cultura de la palabra abierta conduce a un lugar de trabajo más fuerte, más ético y transparente. Se anima a los empleados a:

- ✓ Informar sobre las preocupaciones con anticipación para evitar que los pequeños problemas se agraven.
- ✓ Apoyar a los colegas que denuncian mala conducta.
- ✓ Confíe en que la empresa manejará los informes de manera justa y confidencial.

Líderes y gerentes debe:

- Promocionar comunicación abierta y alentar a los empleados a que informen sobre sus inquietudes.
- Nunca desestime ni tomar represalias contra los denunciantes.
- Asegúrese de que todos los miembros del equipo comprendan procedimientos de denuncia y políticas de protección.

Conclusión

Live Now Technology SLU se compromete a proteger a los empleados, garantizar prácticas comerciales éticas y mantener un lugar de trabajo justo y respetuoso. Animamos a todos los empleados a denunciar infracciones y ayudarnos a mantener nuestros valores de transparencia, integridad y rendición de cuentas.

6. Acciones disciplinarias

En **Live Now Technology SLU** estamos comprometidos con **Manteniendo los más altos estándares de ética, integridad y profesionalismo** en el lugar de trabajo. Cumplimiento de nuestro **Código de conducta** es **obligatorio para todos los empleados**, y las violaciones no se tomarán a la ligera.

En esta sección se describen los **procedimientos para manejar la mala conducta**, la gama de **acciones disciplinarias que se pueden aplicar**, y el **proceso justo y transparente** para abordar las infracciones. Nuestro objetivo es garantizar que todos los empleados comprendan la **consecuencias del incumplimiento** y que se apliquen acciones disciplinarias **consistentemente y justamente**.

6.1 Propósito de las acciones disciplinarias

Las medidas disciplinarias **no pretende ser un castigo**, sino más bien como un medio para:

- ✓ **Defender los valores de la empresa y los estándares éticos.**
- ✓ **Garantizar el cumplimiento de los requisitos legales y reglamentarios.**
- ✓ **Mantener un lugar de trabajo profesional y respetuoso.**
- ✓ **Proteger a la empresa, empleados, clientes y partes interesadas de cualquier daño.**
- ✓ **Fomentar el comportamiento correctivo y prevenir la repetición de infracciones.**

Un **proceso disciplinario justo y estructurado** garantiza que todos los empleados estén **rendir cuentas** por sus acciones y al mismo tiempo se les dio la oportunidad de **Mejorar y corregir el comportamiento cuando sea posible**.

Ejemplo de una infracción menor: Un empleado llega tarde repetidamente a las reuniones sin una justificación válida.

Ejemplo de una infracción grave: Un empleador **roba datos confidenciales de clientes** y lo vende a la competencia.

6.2 Tipos de infracciones que pueden dar lugar a acciones disciplinarias

Se podrán tomar medidas disciplinarias por las siguientes infracciones, entre otras:

6.2.1 Mala conducta en el lugar de trabajo y violaciones de políticas

- **Acoso, intimidación, discriminación o cualquier forma de comportamiento abusivo.**

- Incumplimiento de **protocolos de seguridad en el lugar de trabajo** poniendo en peligro a los empleados o la propiedad de la empresa.
- **Uso de lenguaje ofensivo, inapropiado o discriminatorio** en el lugar de trabajo.

6.2.2 Violación de la confidencialidad y protección de datos

- No autorizado **divulgación de información sensible de la empresa**.
- Mal manejo de **datos confidenciales**, incluidos registros de clientes o empleados.
- **Incumplimiento de las políticas de ciberseguridad**, lo que podría dar lugar a posibles violaciones de datos.

6.2.3 Fraude, corrupción y mala conducta financiera

- Participar en **soborno, malversación de fondos, falsificación de registros o fraude financiero**.
- **Mal uso de fondos o bienes de la empresa** para beneficio personal.
- **Presentar reclamaciones de gastos falsas o falsificar documentos**.

6.2.4 Mal uso de los recursos de la empresa y de los sistemas informáticos

- **Acceso no autorizado a los sistemas, piratería o alteración de datos de la empresa**.
- **Utilizar los activos de la empresa con fines ilegales o poco éticos**.
- **Violación de las leyes de propiedad intelectual**, incluido el uso de software no autorizado.

6.2.5 Incumplimiento de los requisitos legales y reglamentarios

- **Incumplimiento del RGPD**, leyes de ciberseguridad o regulaciones de la industria.
- **Descuido de las normas de salud y seguridad en el trabajo**, creando entornos de trabajo inseguros.
- **Participar en prácticas comerciales poco éticas** que podrían dar lugar a responsabilidades legales.

6.3 Tipos de acciones disciplinarias

Se tomarán medidas disciplinarias **proporcional a la gravedad de la violación** y tendrá en cuenta **intención, impacto y recurrencia**. Las acciones pueden incluir:

6.3.1 Medidas correctivas informales (para infracciones menores)

Advertencia verbal: Una conversación privada con un supervisor para abordar problemas menores. **Coaching y formación adicional:** Es posible que se requiera que el empleado complete un programa de capacitación para mejorar el comportamiento o las lagunas de conocimiento.

Ejemplo: Si un empleado **viola inadvertidamente una política de la empresa**, podrán recibir orientación adicional en lugar de una acción disciplinaria inmediata.

6.3.2 Acciones disciplinarias formales

Advertencia escrita: Un documento formal que establece la naturaleza de la infracción, las acciones correctivas necesarias y las posibles consecuencias de una mayor conducta indebida.

Plan de Mejora del Desempeño (PIP): Si el problema está relacionado con el desempeño, el empleado puede ser incluido en una lista estructurada. **programa de mejora** con objetivos y plazos claros.

Ejemplo: Un empleado que **ignora continuamente los plazos y tiene un rendimiento inferior al esperado a pesar de los múltiples recordatorios**. Puede colocarse en un **Plan de mejora del rendimiento** antes de tomar más medidas.

6.3.3 Acciones disciplinarias graves (por infracciones graves o reiteradas)

● **Suspensión sin goce de sueldo:** En caso de infracciones graves, el empleado podrá ser suspendido temporalmente mientras se realiza una investigación.

● **Degradación o reasignación:** Si corresponde, un empleado puede ser trasladado a un puesto diferente con **menos responsabilidades**.

Ejemplo: Si un empleado **incumple repetidamente las políticas de seguridad** y expone datos sensibles, pueden ser **reasignado a un rol no sensible** o colocados en suspensión.

6.3.4 Terminación del empleo

✘ **Despido inmediato por mala conducta grave:** Los empleados podrán ser despedidos sin previo aviso si participan en:

- **Robo, fraude o daño intencional a la reputación de la empresa.**
- **Conducta violenta o criminal dentro del lugar de trabajo.**
- **Violaciones éticas graves, como corrupción o discriminación.**

Ejemplo: Si un empleado **comete un acto de violencia en el lugar de trabajo o participa en una actividad fraudulenta grave**, podrán ser rescindidos inmediatamente.

6.3.5 Acciones legales y cargos penales

⚖️ **Procedimientos legales:** En casos de conducta delictiva (por ejemplo, fraude, ciberdelito, robo de datos), la empresa podrá emprender acciones legales. **acción legal** contra el empleado.

⚖️ **Responsabilidad civil o penal:** Los empleados que sean declarados culpables de mala conducta grave podrían enfrentarse a... **demandas, multas o procesamientos.**

Ejemplo: Si un empleador **roba propiedad intelectual y la vende a competidores**, se podrán emprender acciones legales.

6.4 Proceso disciplinario y derechos de los empleados

Todas las acciones disciplinarias serán **manejados con imparcialidad, confidencialidad y debido proceso.**
Empleados **tener el derecho** a:

- ✓ **Recibir una explicación clara** de la supuesta violación.
- ✓ **Proporcionar su versión de la historia** antes de que se tomen medidas disciplinarias.
- ✓ **Tener un representante (de Recursos Humanos o asesor legal) presente** durante las audiencias.
- ✓ **Recurso contra decisiones** si consideran que la acción disciplinaria fue injusta.

6.5 Proceso de apelaciones y revisión

Empleados que **no estar de acuerdo con las acciones disciplinarias** puede presentar un recurso de apelación dentro de **10 días hábiles.** El **Departamento de RRHH y Comité de Ética** llevará a cabo una **revisión secundaria** antes de tomar una decisión final.

- ✓ **Las apelaciones deben presentarse por escrito.**, detallando por qué la acción disciplinaria no estaba justificada.
- ✓ **Se podrían realizar más investigaciones.**, incluyendo entrevistas y revisión de evidencia.
- ✓ **Las decisiones finales se comunicarán por escrito.** dentro de un plazo de tiempo determinado.

6.6 Medidas preventivas y compromiso de la empresa

En **Live Now Technology SLU** nuestro enfoque está en **prevención en lugar de castigo**
Creemos en:

- ✓ **Formación continua** para ayudar a los empleados a comprender las políticas de la empresa.
- ✓ **Comunicación clara de expectativas** para evitar malentendidos.
- ✓ **Animar a los empleados a buscar aclaraciones** antes de violar cualquier regla.
- ✓ **Mantener un proceso disciplinario justo y objetivo.**

Conclusión

Existen acciones disciplinarias para **Proteger a los empleados, a los clientes y la integridad de la empresa.** Al comprender y respetar las políticas de la empresa, los empleados contribuyen a una **Lugar de trabajo justo, seguro y ético.**

Reconocimiento

En **Live Now Technology SLU**, tomamos nuestro **Código de conducta** en serio. Este documento describe los valores, principios y políticas fundamentales que guían nuestras acciones, interacciones y responsabilidades dentro de la empresa y hacia nuestros grupos de interés.

Todo **empleados, contratistas y socios comerciales** se espera que **lea, comprenda y cumpla completamente** con las disposiciones de este Código. Al firmar la declaración de reconocimiento, las personas confirman su compromiso con una conducta ética y responsable, fomentando un ambiente de trabajo profesional y respetuoso.

1. ¿Quién debe reconocer este Código?

Todos los empleados—Todo empleado, independientemente de su puesto, antigüedad o departamento, debe adherirse a las políticas descritas en este Código.

Contratistas y consultores—Los profesionales externos que trabajen con la empresa o en su nombre también deben cumplir estas pautas.

Socios comerciales y proveedores—Cualquier organización o individuo que realice actividades comerciales con **Live Now Technology SLU** está obligado a mantener estándares éticos similares.

El incumplimiento de este Código puede resultar en acciones disciplinarias, incluida la rescisión del contrato, repercusiones legales o la descalificación para futuras colaboraciones.

2. Responsabilidades de empleados y contratistas

Leer y comprender—Todos los empleados y personal asociado deben revisar cuidadosamente todo el Código de Conducta.

Cumplir con las políticas—Se espera que las personas apliquen estos principios en sus actividades laborales diarias y en los procesos de toma de decisiones.

Busque aclaraciones cuando sea necesario—Si alguna sección del Código no está clara, los empleados deben consultar a su gerente o al **Departamento de RR.HH. y Cumplimiento** para ayuda. **Informar sobre preocupaciones éticas**—Los empleados deben denunciar de forma proactiva las violaciones, el comportamiento poco ético o la mala conducta a través de **Canal de comunicación interna de empleados (mecanismo de denuncia anónima)**.

Ejemplo: Si un empleado detecta una brecha de seguridad pero no la denuncia, esto podría acarrear graves consecuencias. La responsabilidad ética incluye tomar **medidas proactivas** para abordar los riesgos potenciales.

3. Socios comerciales y compromiso de los proveedores

Live Now Technology SLU requiere que todas las partes externas, incluidos vendedores, proveedores y socios, sigan los principios éticos descritos en este Código cuando realicen negocios con la empresa o en su nombre.

Expectativas clave de los socios comerciales:

- **Integridad en las transacciones:** Todos los acuerdos, contratos y transacciones financieras deben ser transparentes y libres de corrupción o prácticas fraudulentas.
- **Protección de datos y confidencialidad:** Cualquier acceso a datos de la empresa o de clientes debe gestionarse con la máxima seguridad y en cumplimiento de la normativa **Mejores prácticas en materia de RGPD y ciberseguridad**.
- **Ética y cumplimiento en el lugar de trabajo:** Los socios comerciales no deben participar en discriminación, acoso, trabajo forzado o cualquier práctica comercial poco ética.

Cualquier tercero que viole este Código podrá enfrentar **rescisión del contrato, repercusiones legales y pérdida de oportunidades de negocio** con nuestra empresa.

4. Compromiso con la Mejora Ética Continua

En **Live Now Technology SLU**, nosotros continuamente **revisar, actualizar y mejorar** Nuestro Código de Conducta para:

- ✓ Alinearse con **mejores prácticas de la industria** y la evolución de las regulaciones.
- ✓ Abordar nuevos desafíos en **protección de datos, ciberseguridad y ética en el trabajo**.
- ✓ Reforzar una **cultura de integridad y responsabilidad ética**.

Los empleados, contratistas y socios comerciales serán **notificado de cualquier cambio significativo** a este Código, y podrán requerirse reconocimientos actualizados cuando se produzcan revisiones importantes.

Política de seguridad de la información

El **Política de seguridad de la información** es un documento fundamental que describe los principios, reglas y procedimientos que **Live Now Technology SLU** sigue a **Proteger datos confidenciales, garantizar el cumplimiento de las regulaciones y mitigar los riesgos de seguridad**.

1. Introducción y propósito

1.1 Introducción

En **Live Now Technology SLU** la seguridad de la información es un pilar fundamental de nuestras operaciones. Como empresa especializada en **procesamiento de datos, ingeniería de sistemas y desarrollo de software científico**, nos encargamos **datos corporativos, de clientes y personales sensibles**. Eso debe ser **Protegido contra acceso, divulgación, alteración o destrucción no autorizados**.

La creciente sofisticación de las amenazas cibernéticas, los requisitos regulatorios y nuestro compromiso con **privacidad de datos** requieren un enfoque estructurado y proactivo. **marco de seguridad de la información**. Esta política describe los principios, reglas y responsabilidades que rigen **Cómo protegemos los activos digitales, mitigamos los riesgos y garantizamos la continuidad del negocio**.

1.2 Propósito de la Política

El objetivo de esta Política de Seguridad de la Información es:

Proteger la confidencialidad, integridad y disponibilidad (CIA) de los datos de la empresa y de los clientes. **Garantizar el cumplimiento de la normativa aplicable**, incluido **RGPD, ISO/IEC 27001 y leyes nacionales de ciberseguridad**.

Prevenir violaciones de datos, accesos no autorizados y amenazas cibernéticas mediante la implementación de estrictos controles de seguridad.

Educar a empleados, contratistas y terceros sobre sus responsabilidades en materia de seguridad.

Establecer un marco para la gestión de riesgos, respuesta a incidentes y continuidad del negocio. **Mantener la confianza con los clientes, socios y partes interesadas**, demostrando una postura de seguridad fuerte.

Al adherir a esta política, **Live Now Technology SLU** tiene como objetivo proteger su negocio, sus clientes y sus empleados de **pérdida de datos, ciberataques y daños a la reputación**.

2. Alcance y aplicabilidad

2.1 Alcance

Esta **Política de seguridad de la información** se aplica a todos **sistemas, redes, dispositivos, datos y personal** dentro de **Live Now Technology SLU**. Define principios de seguridad para **protegiendo los activos digitales** y garantizar la confidencialidad, integridad y disponibilidad de **Información de la empresa y del cliente**.

Cubre, pero no se limita a:

Infraestructura de TI propiedad de la empresa (servidores, bases de datos, entornos de nube y estaciones de trabajo).

Seguridad de la red (firewalls, VPN, controles de acceso y protocolos de comunicación seguros). **Datos de la empresa y del cliente** (documentos electrónicos, bases de datos, comunicaciones por correo electrónico y copias de seguridad).

Seguridad en el desarrollo e implementación de software (estándares de codificación, pruebas de vulnerabilidad y control de versiones).

Autenticación de usuarios y control de acceso (gestión de identidad, políticas de contraseñas y autenticación multifactor).

Proveedores de servicios externos y contratistas (servicios de TI subcontratados, proveedores de nube y socios comerciales).

Medidas de seguridad física (seguridad de la oficina, áreas restringidas y acceso controlado). **Planes de respuesta a incidentes y recuperación ante desastres** (protocolos de continuidad de negocio y restauración de datos).

2.2 Aplicabilidad

Esta política se aplica a **todos los empleados, contratistas y terceros** que interactúan con los sistemas y datos de la empresa. Es obligatorio para:

- **Empleados a tiempo completo y a tiempo parcial**, incluidos los trabajadores remotos.
- **Contratistas, autónomos y consultores** con acceso a datos de la empresa o sistemas informáticos.
- **Proveedores, vendedores y socios externos** manejar o almacenar datos de la empresa.
- **Pasantes, aprendices y personal temporal** utilizando dispositivos o software de la empresa.

Todo el personal debe:

Entender y cumplir con políticas, procedimientos y pautas de seguridad. **Informar sobre cualquier violación de seguridad, amenaza o incidente** inmediatamente.

Seguir las políticas de control de acceso y nunca comparta credenciales o datos confidenciales. **Adherirse a las mejores prácticas para el manejo de datos, dispositivos y comunicaciones en línea**.

El incumplimiento de esta política puede resultar en: **acciones disciplinarias, rescisión de contrato o consecuencias legales**.

3. Principios de seguridad de la información

En esta sección se describen los **principios básicos de seguridad** que gobiernan cómo **Live Now Technology SLU** protege sus datos, activos de TI y operaciones comerciales. Estos principios garantizan el cumplimiento de **Leyes europeas de protección de datos (RGPD), estándares de la industria y mejores prácticas** para proteger información sensible.

3.1 Confidencialidad

Proteger la información confidencial contra accesos o divulgaciones no autorizados es una máxima prioridad.

Clasificación de datos y control de acceso

- Todos los datos se clasifican como **Público, interno, confidencial o restringido** basado en la sensibilidad.
- Acceso a **Datos confidenciales y restringidos** se concede en un **base de la necesidad de saber** utilizando controles de acceso basados en roles (RBAC).
- **Autenticación multifactor (MFA)** Se aplica para acceder a sistemas sensibles.
- El acceso a los datos se revisa periódicamente para **eliminar privilegios innecesarios**.

Estándares de cifrado

- Todos los datos confidenciales son **cifrado en reposo y en tránsito** utilizando AES-256 o equivalente.
- Canales de comunicación seguros (por ejemplo, **SSL/TLS, VPN**) son necesarios para el acceso remoto.
- Los archivos confidenciales deben almacenarse en **bases de datos cifradas o almacenamiento seguro en la nube**.

Intercambio y transmisión de datos

- Los empleados deben utilizar **herramientas aprobadas por la empresa** (por ejemplo, **correo electrónico cifrado, VPN, servicios de transferencia segura de archivos**) para compartir datos.
 - **Cuentas de correo electrónico personales, dispositivos USB y almacenamiento en la nube no autorizado** Tienen terminantemente prohibido el manejo de datos de la empresa.
-

3.2 Integridad

Garantizar que los datos y los sistemas estén **Preciso, consistente y a prueba de manipulaciones.**

Control de versiones y gestión de cambios

- Las actualizaciones de software y los cambios del sistema deben seguir un **proceso controlado**, con aprobaciones y seguimiento de versiones.
- Se deben mantener registros para **todas las modificaciones a sistemas y aplicaciones críticos.**
- Las comprobaciones de integridad automatizadas garantizan **consistencia de los datos y evitar cambios no autorizados.**

Protección contra modificaciones no autorizadas

- Acceso a **sistemas críticos, bases de datos y código fuente** está estrictamente controlado.
- Se utilizan firmas digitales y algoritmos hash para **verificar la autenticidad del archivo.**
- Sistemas de detección de anomalías **equipos de seguridad de alerta** a cambios inusuales del sistema.

Validación de datos y manejo de errores

- Se deben aplicar técnicas de validación de entradas y saneamiento para prevenir **ataques de inyección.**
 - Se requieren pruebas automatizadas para **comprobaciones de consistencia de datos** Antes del despliegue de producción.
 - Las copias de seguridad deben realizarse **pruebas de integridad periódicas** para garantizar la recuperabilidad.
-

3.3 Disponibilidad

Garantizar que los sistemas, servicios y datos sean accesibles **cuando sea necesario** Sin interrupciones.

Continuidad del negocio y recuperación ante desastres

- Los sistemas críticos tienen **mecanismos de redundancia y conmutación por error** para evitar tiempos de inactividad.
- **Copias de seguridad periódicas** se mantienen en lugares seguros, con **pruebas de recuperación automatizadas.**
- **Plan de Continuidad de Negocio (PCN)** Describe los procedimientos para reanudar las operaciones después de las interrupciones.

Ciberresiliencia y mitigación de amenazas

- Protección DDoS, equilibrio de carga y **monitoreo en tiempo real** ayudar a prevenir interrupciones del servicio.
- Salud de la red y del sistema **Debe ser monitoreado continuamente para detectar problemas de rendimiento y seguridad..**

- Equipos de respuesta a incidentes **Debe estar de guardia para la mitigación inmediata de amenazas.**

Acceso remoto y tiempo de actividad del sistema

- El acceso remoto es **restringido a VPN y dispositivos aprobados por la empresa.**
 - Los proveedores de servicios e infraestructura en la nube deben cumplir **Acuerdos de nivel de servicio (SLA) con un tiempo de actividad del 99,9 %.**
- Los empleados deben informar **cualquier falla del sistema, problemas de conectividad o rendimiento lento de inmediato.**

4. Control de acceso y autenticación de usuarios

El control de acceso es un **pilar fundamental** de seguridad de la información en **Live Now Technology SLU**. Se asegura de que **Sólo personas autorizadas** puede acceder a los datos, sistemas y recursos de la empresa mientras **Prevenir accesos no autorizados, violaciones de datos y amenazas a la seguridad.**

4.1 Autenticación del usuario

Los mecanismos de autenticación adecuados protegen **sistemas, redes y datos confidenciales** contra accesos no autorizados.

Autenticación multifactor (MFA)

- Todos los empleados, contratistas y proveedores externos deben utilizar **Maestría en Bellas Artes** al acceder a los sistemas de la empresa.
- Los métodos de MFA incluyen **contraseña + OTP (contraseña de un solo uso), autenticación biométrica o tokens de seguridad.**
- Las cuentas de administrador deben usar **autenticación basada en hardware** (por ejemplo, YubiKeys, tarjetas inteligentes).

Seguridad y gestión de contraseñas

- Los empleados deben crear **contraseñas fuertes y únicas** utilizando al menos:
 - **12+ personajes** (incluyendo mayúsculas, minúsculas, números y símbolos).
 - **Sin palabras del diccionario ni frases comunes.**
- Las contraseñas deben ser **cambiado cada 90 días** y nunca debe reutilizarse.
- La empresa aplica una **política del administrador de contraseñas**, requiriendo que los empleados almacenen sus credenciales en un **administrador de contraseñas aprobado.**
- **Política de bloqueo de cuentas:** Después de **cinco intentos fallidos de inicio de sesión** las cuentas se bloquearán por **15 minutos.**

Inicio de sesión único (SSO) e identidad federada

- Los empleados se autentican mediante **SSO (inicio de sesión único)** para todos los servicios corporativos integrados.
- **Gestión de identidades federadas** (a través de Azure AD, Okta o Google Workspace) permite **autenticación segura y centralizada** en diferentes plataformas.

4.2 Políticas de control de acceso

Basado en roles y **acceso con privilegios mínimos** garantiza a los empleados **Sólo tienen acceso a lo que necesitan**.

Control de acceso basado en roles (RBAC)

- El acceso se concede en función de **rol y responsabilidades del trabajo** (Por ejemplo, administradores de TI, finanzas, RRHH).
- Los empleados reciben **permisos mínimos necesarios** para realizar su trabajo.
- Se requiere acceso con mayores privilegios (por ejemplo, derechos de administrador del sistema) **estrictamente controlado y monitoreado**.

Principio de privilegio mínimo (PoLP)

- Se conceden permisos a los usuarios y sistemas **Sólo el nivel mínimo de acceso necesario** para desempeñar sus funciones.
- **Acceso temporal o elevado** debe ser solicitada formalmente, justificada y **con restricción de tiempo**.
- Los datos sensibles y las acciones administrativas son **restringido únicamente al personal autorizado**.

Revisiones de acceso y revocación

- Los permisos de acceso de los usuarios son **revisado trimestralmente** para detectar y eliminar **cuentas inactivas o innecesarias**.
- Los empleados que abandonan la empresa tienen **Todo acceso revocado inmediatamente** en su último día de trabajo.
- Cuentas inactivas (inactivas por **90 días**) se ejecutan automáticamente **deshabilitado y marcado para revisión**.

4.3 Acceso de terceros y proveedores

Partes externas **Debe seguir estrictas políticas de seguridad** al acceder a los recursos de la empresa.

Gestión de riesgos de proveedores

- Los proveedores externos se someten a **una evaluación de seguridad** antes de que se le conceda el acceso.
- Los contratos incluyen **cláusulas de seguridad claras**, asegurando a los vendedores **Siga nuestras políticas de seguridad**.
- El acceso del proveedor es **restringido a entornos dedicados** (nunca en sistemas de producción).

Acceso remoto seguro

- Los usuarios externos deben **autenticarse mediante VPN** y **utilizar MFA** antes de acceder a los recursos de la empresa.
- Las sesiones de acceso remoto son **monitoreados, registrados y revisados** por violaciones de seguridad.
- Los vendedores deben **Desconectarse inmediatamente después de completar las tareas asignadas**.

Controles de intercambio de datos

- Acceso de terceros a datos confidenciales **requiere la aprobación de la gerencia**.
- Datos sensibles **debe ser anonimizado o enmascarado** antes de ser compartido externamente.
- Todas las transferencias de datos se realizan a través de **canales cifrados (TLS 1.2+, SFTP o API seguras)**.

4.4 Registro y supervisión del acceso

Para detectar actividades no autorizadas, todos los **eventos de autenticación e intentos de acceso** se registran y revisan.

Monitoreo y alertas en tiempo real

- Todos los intentos de inicio de sesión, eventos de autenticación fallidos y escaladas de privilegios son **registrado y analizado**.
- Las anomalías (por ejemplo, ubicaciones de inicio de sesión inusuales, fallas de acceso repetidas) se activan **alertas de seguridad inmediatas**.

Registros de auditoría y cumplimiento

- Se almacenan registros de acceso detallados **durante al menos 12 meses** para fines de auditoría y cumplimiento.
- Las auditorías de seguridad periódicas garantizan que **Las políticas de control de acceso siguen siendo efectivas**.

Respuesta a incidentes de acceso no autorizado

- Si se detecta acceso no autorizado, **elLa cuenta se suspende inmediatamente**, y se inicia una investigación.
- Empleados **debe informar** cualquier intento de acceso sospechoso a **laEquipo de seguridad informática**.

5. Manejo y cifrado de datos

La seguridad de los datos es el núcleo de **Live Now Technology SLU** estrategia de seguridad de la información. Garantizar que los datos estén **manipulados, almacenados, transmitidos y eliminados adecuadamente** es esencial para proteger los activos de la empresa, la propiedad intelectual y la información del cliente.

5.1 Clasificación de datos y niveles de sensibilidad

Todos los datos de la empresa están categorizados en función de **requisitos de sensibilidad y confidencialidad** aplicar los controles de seguridad adecuados.

Niveles de clasificación:

1. **Público**–Datos que se pueden compartir libremente sin riesgo (por ejemplo, contenido del sitio web, ofertas de empleo).
2. **Solo para uso interno**–Información empresarial no sensible, accesible para los empleados pero no para el público (por ejemplo, documentación interna, materiales de capacitación).
3. **Confidencial**–Datos que requieren protección debido **arazones comerciales, legales o regulatorias**(por ejemplo, contratos, registros de RRHH, información financiera).
4. **Restringido / Altamente confidencial**–La información más sensible, que requiere **estricto control de acceso y cifrado**(por ejemplo, secretos comerciales, datos personales, credenciales de seguridad).

Restricciones de acceso:

- **Datos públicos**Se puede compartir libremente.
- **Datos internos**Está restringido únicamente a los empleados.

- **Datos confidenciales** se comparte en un **base de la necesidad de saber**, requiriendo la aprobación gerencial.
- **Datos altamente confidenciales** requiere **autenticación multifactor, cifrado y registro de auditoría**.

5.2 Cifrado de datos y almacenamiento seguro

Políticas de cifrado:

- **Todos los datos sensibles** debe estar encriptado **en reposo y en tránsito** utilizando algoritmos de cifrado estándar de la industria.
- **Cifrado en reposo:**
 - Uso de bases de datos de la empresa **Cifrado AES-256**.
 - Estaciones de trabajo, computadoras portátiles y dispositivos móviles **Debe tener habilitado el cifrado de disco completo**.
- **Cifrado en tránsito:**
 - Todas las transferencias de datos utilizan **Cifrado TLS 1.2+** para evitar la interceptación.
 - Los correos electrónicos internos y externos que contengan información confidencial deben **cifrado mediante PGP o S/MIME**.

Mejores prácticas de almacenamiento seguro:

- Datos **no debe almacenarse en dispositivos personales** o servicios de almacenamiento en la nube no autorizados.
- Los datos confidenciales se almacenan en **repositorios cifrados aprobados por la empresa** (p.ej, **OneDrive para la Empresa, Google Workspace, AWS S3 con cifrado**).
- Los documentos en papel que contengan datos confidenciales deben **encerrados en armarios seguros**.

5.3 Retención y eliminación de datos

Para cumplir con **Legal, regulatorio y operativo** requisitos, los implementamos **políticas estrictas de retención y eliminación de datos**.

Periodos de conservación:

- Registros de empleados: **5 años** Después de la terminación.
- Registros financieros: **7 años** según la normativa fiscal.
- Datos del cliente y del proyecto: **Según acuerdos contractuales**.
- Copias de seguridad: **Revisado y depurado periódicamente según las necesidades del negocio..**

Eliminación segura de datos:

- **Datos digitales:** Debe borrarse de forma segura utilizando **herramientas de limpieza de grado militar** (p.ej, **Norma DoD 5220.22-M**).
- **Documentos físicos:** Debe ser **triturado y eliminado de forma segura**.
- **Eliminación de hardware:** Los dispositivos de almacenamiento deben ser **destruido físicamente o borrado de forma segura** Antes de su eliminación.

6. Seguridad de la red y protección de la infraestructura

Proteger nuestra infraestructura de red es fundamental para **Live Now Technology SLU** compromiso con la ciberseguridad. **A enfoque de defensa de múltiples capas** garantiza la integridad, disponibilidad y confidencialidad de los sistemas de la empresa, previniendo **acceso no autorizado, amenazas cibernéticas y violaciones de datos**.

6.1 Seguridad perimetral y firewalls

Nosotros implementamos **múltiples capas de seguridad** al **niveles de perímetro, red y punto final** para detectar y prevenir amenazas externas.

Sistemas de prevención de intrusiones y cortafuegos (IPS):

- Todas las conexiones externas pasan a través de **firewalls de nivel empresarial** configurado con **inspección profunda de paquetes (DPI)**.
- **IPS e IDS (Sistemas de detección de intrusiones)** se despliegan en **detectar y bloquear tráfico malicioso**.
- Regular **auditorías de seguridad y actualizaciones de reglas** asegurar **políticas de firewall** están alineados con las amenazas emergentes.

Bloqueo geográfico y restricciones de acceso:

- El tráfico procedente de países de alto riesgo y direcciones IP maliciosas conocidas es **bloqueado automáticamente**.
- **Políticas de acceso estrictas** aplicar a conexiones remotas, requiriendo **autenticación multifactor (MFA)**.

6.2 Segmentación de red interna y seguridad de confianza cero

Seguimos una **Modelo de seguridad de confianza cero**, que **elimina la presunción de confianza** dentro de la red y aplica una autenticación y verificación estrictas para cada solicitud de acceso.

Estrategia de segmentación de red:

- Las redes internas son **segmentado en zonas aisladas** **limitar la propagación del ataque** en caso de incumplimiento.
- **Datos sensibles y servicios críticos** (Por ejemplo, los servidores de finanzas, RR.HH. e I+D) residen en **VLAN separadas con acceso restringido**.
- A los empleados se les concede **acceso únicamente a los recursos necesarios para sus funciones laborales** (**Principio del Mínimo Privilegio**).

Modelo de seguridad de confianza cero:

- **Verificar la identidad antes de conceder acceso**—Todos los usuarios deben pasar comprobaciones de autenticación.
- **La microsegmentación garantiza** que diferentes departamentos y funciones **no comparten el mismo espacio de red**.

- **Monitoreo en tiempo real** Identifica patrones de acceso anormales y potenciales **amenazas internas**.

6.3 Política de Wi-Fi seguro y acceso remoto

Garantizar el acceso seguro a **sistemas corporativos** Tanto la protección contra ataques WiFi internos como la protección contra ataques a entornos remotos es fundamental para prevenir intrusiones no autorizadas.

Seguridad Wi-Fi corporativa:

- **Cifrado WPA3** Se aplica en todas las redes Wi-Fi de la empresa.
- Las redes de invitados son **completamente aislado** de la infraestructura corporativa.
- **Filtrado de direcciones MAC** restringe el acceso a **Solo dispositivos preaprobados**.

Acceso remoto a través de VPN:

- Empleados remotos **debe utilizar la VPN aprobada por la empresa** para acceder a los sistemas internos.
- La **tunelización dividida está deshabilitada** para garantizar que todo el tráfico fluya a través de la VPN.
- Se requiere acceso VPN **autenticación multifactor (MFA)**.

6.4 Seguridad de endpoints y administración de dispositivos

Para evitar ataques a nivel de punto final, como **ransomware, malware y phishing**, hacemos cumplir **políticas estrictas de seguridad de los dispositivos**.

Software de seguridad obligatorio:

- Todos los dispositivos de la empresa deben tener **antivirus de última generación (NGAV) y detección y respuesta de endpoints (EDR)** soluciones.
- **Parqueo automático** garantiza que las vulnerabilidades del software y del sistema operativo se aborden rápidamente.

Políticas de fortalecimiento de dispositivos:

- **Los puertos USB están restringidos** para evitar la transferencia de datos no autorizada.
- **Los privilegios de administrador son limitados** para evitar instalaciones de software no autorizadas.
- **Cifrado de disco completo** es requerido en todas **computadoras portátiles, de escritorio y dispositivos móviles**.

6.5 Operaciones seguras en la nube y el centro de datos

Como empresa impulsada por la tecnología, **Live Now Technology SLU** se basa en un **entorno de nube híbrida**, combinando **centros de datos locales** con **servicios de nube seguros**.

Mejores prácticas de seguridad en la nube:

- Los recursos en la nube son **Protegido con controles de acceso basados en identidad (IAM)**.
- **Los datos se cifran en reposo y en tránsito** con AES-256 y TLS 1.2+.
- **Auditorías periódicas de seguridad en la nube** para identificar configuraciones erróneas y vulnerabilidades.

Estándares de seguridad locales:

- Los centros de datos requieren **autenticación biométrica** y **Monitoreo 24/7**.
- **Planes de recuperación ante desastres** para garantizar la continuidad del negocio en caso de fallo.
- **Los registros de acceso se revisan continuamente** para evitar la entrada no autorizada.

6.6 Monitoreo continuo de la red e inteligencia de amenazas

Para detectar y mitigar amenazas de forma proactiva, implementamos **Monitoreo en tiempo real e inteligencia de amenazas**.

Gestión de eventos e información de seguridad (SIEM):

- Los registros de los firewalls, servidores y puntos finales son **centralizados** en un **Sistema SIEM**.
- **Algoritmos de aprendizaje automático** para identificar anomalías y comportamientos sospechosos.

Inteligencia de amenazas y respuesta automatizada:

- Los feeds de inteligencia sobre amenazas proporcionan **actualizaciones en tiempo real** en amenazas cibernéticas e indicadores de compromiso (IOC).
- Automatizado **mecanismos de respuesta a amenazas** Aislar los sistemas infectados antes de que se propague un ataque.

6.7 Cumplimiento de los estándares de seguridad de la industria

Live Now Technology SLU se adhiere a **marcos globales de ciberseguridad** para mantener los más altos estándares de seguridad.

Cumplimiento normativo y regulatorio:

- **ISO 27001**–Sistema de gestión de seguridad de la información (SGSI).
- **Marco de ciberseguridad del NIST**–Mejores prácticas de ciberseguridad basadas en riesgos.
- **RGPD y Reglamento de Privacidad de Datos**–Garantizar la protección y el cumplimiento de los datos de los usuarios.

Auditorías de seguridad periódicas y pruebas de penetración:

- Anual **pruebas de penetración de terceros** Identificar vulnerabilidades.
- Interno **Las auditorías de seguridad garantizan el cumplimiento** con las amenazas cibernéticas en evolución.

7. Respuesta a incidentes y gestión de infracciones

Una **estrategia de respuesta a incidentes proactiva y bien definida** es esencial para mitigar el impacto de las brechas de seguridad y las amenazas cibernéticas. **Live Now Technology SLU** sigue un **marco estructurado de respuesta a incidentes** para garantizar que todos los eventos de seguridad sean **rápidamente identificados, investigados, contenidos y resueltos** manteniendo al mismo tiempo el cumplimiento de **requisitos legales y reglamentarios**.

7.1 Clasificación e identificación de incidentes

Los incidentes de seguridad varían en alcance y gravedad. **Live Now Technology SLU** clasifica los incidentes según su impacto potencial y sigue un **matriz de priorización**:

Niveles de gravedad del incidente:

- **Bajo (Eventos menores)**–Intentos de inicio de sesión no autorizados, correos electrónicos de phishing menores o detecciones de malware aisladas.
- **Mediano (Amenazas moderadas)**–Cuentas de empleados comprometidas, acceso no autorizado a datos no confidenciales.
- **Alto (Incidentes críticos)**–Violaciones de datos, ataques de ransomware en todo el sistema, ataques de denegación de servicio (DoS) o amenazas internas.

Mecanismos de detección temprana de amenazas:

- **Gestión de eventos e información de seguridad (SIEM)**: Los registros y eventos se monitorean continuamente para detectar actividad inusual.
- **Análisis del comportamiento de usuarios y entidades (UEBA)**: La detección de anomalías impulsada por IA ayuda a **identificar comportamientos maliciosos** dentro de la red.
- **Alertas automatizadas**: Las actividades sospechosas desencadenan **alertas de seguridad inmediatas** para investigación.

7.2 Procedimientos de reporte y escalamiento de incidentes

Los empleados y el personal de seguridad informática deben **informar sobre cualquier incidente de seguridad sospechoso** inmediatamente a través de la **Sistema de respuesta a incidentes de seguridad interna**.

Canales de notificación de incidentes:

- Los empleados pueden informar problemas de seguridad a través de:
 - Línea directa de seguridad interna
 - Correo electrónico dedicado
 - Sistema de denuncia interna anónima
- Los equipos de seguridad de TI y respuesta a incidentes (SIRT) reciben alertas en tiempo real a través de **sistemas de monitoreo automatizado**.

Niveles de escalada y responsabilidades:

- **Nivel 1 (Equipo de soporte técnico y seguridad de TI):** Triage inicial y análisis de incidentes reportados.
- **Nivel 2 (Centro de Operaciones de Seguridad - SOC):** Investigación avanzada, análisis forense y esfuerzos de contención.
- **Nivel 3 (Equipo de respuesta ejecutiva y legal):** Gestión de crisis, evaluación de cumplimiento, acciones legales si es necesario.

7.3 Estrategias de contención y remediación

Una vez que se confirma un incidente, una respuesta rápida es esencial para evitar más daños y restablecer las operaciones.

Medidas de contención:

- **Aislar los sistemas afectados** inmediatamente (por ejemplo, desconectar los dispositivos infectados de la red).
- **Bloquear direcciones IP maliciosas** y suspender las cuentas comprometidas.
- **Desactivar el acceso remoto no autorizado** para evitar el movimiento lateral dentro de la infraestructura.

Análisis forense e investigación de causa raíz:

- **Expertos en análisis forense digital analizan patrones de ataque** y determinar puntos de entrada.
- **Registros de incidentes, instantáneas del sistema e informes de seguridad** se recogen como prueba.
- **Se realiza un análisis de vulnerabilidad** para prevenir incidentes similares en el futuro.

Erradicación y recuperación:

- **Eliminación de malware y limpieza del sistema** a través de herramientas antivirus y forenses avanzadas.
- **Restauración de datos desde copias de seguridad seguras** (garantizar la integridad antes de la reintegración).

- **Parquear vulnerabilidades** identificados durante el ataque y reforzar las configuraciones de seguridad.

7.4 Comunicación y notificación a las partes interesadas

Para incidentes que involucren **violaciones de datos o implicaciones legales**, Live Now Technology SLU sigue **protocolos de notificación estrictos** en cumplimiento de **RGPD, ISO 27001 y NIST**.

Plan de Comunicación Interna:

- Los equipos de seguridad informan **liderazgo ejecutivo, oficiales de cumplimiento y departamentos afectados**.
- Se proporcionan actualizaciones periódicas **agarantizar la transparencia y los esfuerzos coordinados**.

Notificaciones externas (cumplimiento del RGPD):

- Si se exponen datos personales, se debe notificar a los usuarios afectados **dentro de 72 horas** por **Artículo 33 del RGPD**.
- Si corresponde, se informa del incidente a la **Autoridad Europea de Protección de Datos (APD)**.
- Los clientes o partes interesadas afectados reciben información oficial **informes de incidentes** con los próximos pasos recomendados.

Manejo de Asuntos Legales y Relaciones Públicas:

- Si un evento de seguridad importante afecta **La reputación de Live Now Technology SLU**, el **Equipo de Relaciones Públicas (PR)** coordina la comunicación externa.
- Guía para asesores legales **Cumplimiento de las leyes de divulgación de infracciones** y posibles responsabilidades.

7.5 Análisis posterior al incidente y mejoras de seguridad

Después de cada incidente, **Se realiza una revisión completa** para fortalecer las defensas de seguridad y prevenir que se repitan.

Informe posterior al incidente (PIR):

- Análisis detallado de **Causas fundamentales, sistemas afectados y vectores de ataque.**
- Identificación de **brechas de seguridad y debilidades de control.**
- **Recomendaciones prácticas** para mejorar la postura en materia de ciberseguridad.

Mejoras de seguridad:

- **Parchear vulnerabilidades** explotados en el ataque.
- **Implementación de medidas de seguridad adicionales** (por ejemplo, controles de acceso más fuertes, herramientas de monitoreo mejoradas).
- **Capacitación en ciberseguridad para empleados** basado en las lecciones aprendidas del incidente.

7.6 Cumplimiento de las normas internacionales de seguridad

Live Now Technology SLU sigue estándares de seguridad globales para **gestión de respuesta a incidentes**:

- **ISO 27035**–Gestión de incidentes de seguridad de la información
- **NIST SP 800-61**–Guía de manejo de incidentes de seguridad informática
- **Artículos 33 y 34 del RGPD**–Notificación de violación de datos personales

Al adherirnos a estos marcos, garantizamos un **robusto, compatible y eficaz** enfoque a **Respuesta a incidentes y gestión de infracciones**.

8. Programas de concientización y capacitación en seguridad

Una fuerte cultura de ciberseguridad es una de las defensas más eficaces contra las amenazas cambiantes. **Live Now Technology SLU** se compromete a construir y mantener un **alto nivel de conciencia de seguridad** entre todos los empleados, contratistas y terceros. Lo logramos mediante **programas de capacitación obligatoria, iniciativas de educación continua y ejercicios simulados regulares**.

8.1 Importancia de la concienciación sobre la seguridad

El error humano es responsable de un porcentaje significativo de violaciones de seguridad en todo el mundo. **Empleados informados y vigilantes** Son nuestra primera línea de defensa contra amenazas como phishing, ingeniería social, ransomware y ataques internos.

La concientización sobre la seguridad permite a los empleados:

- Reconocer actividades sospechosas y amenazas potenciales.
- Reaccionar adecuadamente ante los incidentes de seguridad.
- Proteger la información confidencial y los activos de la empresa.
- Comprender los requisitos legales y reglamentarios como **RGPD** y **ISO 27001** normas.

8.2 Capacitación obligatoria en seguridad para todos los empleados

Todos los empleados, contratistas y terceros relevantes **debe completar la capacitación de seguridad inicial** Durante la incorporación y **participar en cursos anuales de actualización continua**.

Los temas principales de capacitación incluyen:

- Fundamentos de seguridad de la información (CIA: Confidencialidad, Integridad, Disponibilidad).
- Seguridad de contraseñas y mejores prácticas.
- Identificar y evitar ataques de phishing e ingeniería social.
- Protección de datos personales y sensibles (cumplimiento GDPR).
- Uso seguro de los recursos de TI (estaciones de trabajo, dispositivos móviles, servicios en la nube).
- Prácticas seguras de trabajo remoto y uso de VPN.
- Procedimientos adecuados de notificación de incidentes o violaciones de seguridad.

Requisitos de capacitación:

- La capacitación debe completarse dentro de **30 días de alquiler**.
- La capacitación anual en seguridad es obligatoria y su finalización se monitorea mediante **Departamentos de RR.HH. y Cumplimiento**.
- Pasar una **evaluación de conocimientos** (Se requiere un mínimo del 80% de respuestas correctas) después de cada sesión.

8.3 Capacitación especializada en seguridad para roles clave

Ciertos roles tienen acceso a **sistemas críticos y datos sensibles** y por lo tanto requieren **formación avanzada en seguridad**:

Capacitación adicional para:

- **Personal de TI:** Seguridad de red, respuesta a incidentes y gestión de vulnerabilidades.
- **Desarrolladores:** Prácticas de codificación segura (OWASP Top 10, técnicas de revisión de código).
- **Gerentes de proyecto:** Normativa sobre manejo de datos y gestión de riesgos de proveedores externos.
- **Dirección Ejecutiva:** Responsabilidades en gestión de riesgos cibernéticos y cumplimiento normativo.

8.4 Iniciativas de concientización continua

La conciencia de seguridad debe ser **Continuo, dinámico y atractivo**.

Campañas periódicas de concienciación:

- Mensual **boletines de seguridad** con estudios de casos del mundo real y amenazas emergentes.
- Carteles e infografías en todos los espacios de oficina que refuerzan las mejores prácticas.
- Vídeos cortos que destacan consejos de seguridad sencillos.

Pruebas de phishing simuladas:

- **Simulaciones trimestrales de phishing** Se llevan a cabo para medir la vigilancia de los empleados.
- Los empleados que no aprueben las simulaciones deberán: **asistir a sesiones adicionales de entrenamiento de seguridad.**

Talleres interactivos y seminarios web:

- Expertos invitados en ciberseguridad brindan **talleres bianuales** sobre amenazas en evolución como ransomware, ingeniería social y ataques impulsados por IA.
- Los seminarios web brindan acceso conveniente a actualizaciones importantes y repaso de habilidades.

8.5 Promover una mentalidad de seguridad ante todo

Más allá de la formación obligatoria, **Live Now Technology SLU** se esfuerza por **Incorporar la seguridad en la cultura de la empresa** fomentando:

- **Comportamiento proactivo:** Se insta a los empleados a **Reportar actividad sospechosa inmediatamente**, aunque sea incierto.
- **Programas de recompensa:** Reconocer a los empleados que contribuyen activamente a **mejorar las prácticas de seguridad.**
- **Comunicación abierta:** Fomentar preguntas, aclaraciones y debates sobre temas relacionados con la seguridad sin temor a ser juzgados.
- **Campeones de la seguridad:** Designar voluntarios en diferentes departamentos para **Promover las mejores prácticas de seguridad a nivel local.**

8.6 Seguimiento y supervisión del cumplimiento

Registros de entrenamiento:

- Se realiza un seguimiento de la finalización de la capacitación y se informa trimestralmente a la alta dirección.
- El incumplimiento desencadena recordatorios, escaladas y, si es necesario, medidas disciplinarias.

Mejora continua:

- Se recopilan los comentarios de los empleados para **Mejorar los futuros programas de formación.**

- Se revisan los programas **anualmente** basado en los cambios en el panorama de amenazas y las necesidades comerciales cambiantes.

8.7 Alineación con los estándares de seguridad

Nuestro programa de capacitación en seguridad está alineado con los principales estándares y mejores prácticas, que incluyen:

- **Anexo A.7.2.2 de la norma ISO/IEC 27001**—Concientización, educación y capacitación en seguridad de la información.
- **Publicación especial 800-50 del NIST**—Construcción de un programa de concientización y capacitación en seguridad de tecnologías de la información.
- **Artículo 32 del RGPD**—Requisitos de seguridad del procesamiento y concienciación de los empleados.

9. Cumplimiento de las normas legales y reglamentarias

El cumplimiento de las normas legales y reglamentarias es una **piedra angular** de **Live Now Technology SLU** Estrategia de seguridad de la información. Como organización que opera en Europa y maneja datos sensibles, nos comprometemos a...**estricta adherencia** a aplicable **leyes, reglamentos y normas internacionales** que rigen la protección de datos, la privacidad y la seguridad de la información.

9.1 Marcos regulatorios y obligaciones de cumplimiento

Reglamento General de Protección de Datos (RGPD)

- **Alcance:** Se aplica a todas las organizaciones que procesan datos personales de personas dentro del Espacio Económico Europeo (EEE).
- **Áreas clave de cumplimiento:**
 - Tratamiento de datos lícito, justo y transparente.
 - Minimización de datos y limitación de la finalidad.
 - Garantizar la precisión de los datos y la limitación del almacenamiento.

- Proteger los datos personales contra acceso no autorizado, alteración o pérdida.
- Defender los derechos de los interesados (acceso, rectificación, supresión, portabilidad).
- Notificación de violaciones de datos personales dentro de **72 horas** a las autoridades supervisoras.

ISO/IEC 27001 — Sistemas de Gestión de Seguridad de la Información (SGSI)

- **Alcance:** Norma internacional que proporciona un enfoque sistemático para la gestión de información confidencial de la empresa.
- **Áreas clave de cumplimiento:**
 - Establecer un marco de gestión de riesgos para la seguridad de la información.
 - Implementar controles de seguridad basados en las mejores prácticas de la norma ISO 27002.
 - Auditorías internas periódicas y certificaciones externas (cuando corresponda).
 - Mejora continua a través del ciclo PDCA (Planificar, Hacer, Verificar, Actuar).

Directiva NIS2 (próxima prioridad en materia de cumplimiento para las entidades de la UE)

- **Alcance:** Directiva sobre redes y sistemas de información que afecta a entidades esenciales e importantes en toda la UE.
- **Áreas clave de cumplimiento:**
 - Fortalecer la resiliencia en materia de ciberseguridad en todos los sectores.
 - Notificación obligatoria de incidentes dentro de **24 horas**.
 - Mayor escrutinio de los riesgos de terceros y de las cadenas de suministro.

Otras regulaciones aplicables:

- **LOPDGDD (Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales):** Implementación nacional que complementa el RGPD.

- **Directiva de privacidad electrónica (Ley de cookies):** Cumplimiento de la privacidad de las comunicaciones electrónicas (cookies, correos electrónicos comerciales, etc.).
- **Derecho laboral:** Protección de datos personales de los trabajadores según la normativa laboral.

9.2 Medidas implementadas para el cumplimiento normativo

Rol del Delegado de Protección de Datos (DPD):

- **ADPO** (interna o externa) supervisa las estrategias de protección de datos y garantiza el cumplimiento del RGPD y las leyes locales de privacidad de datos.
- El DPO actúa como **punto de contacto principal** con las autoridades reguladoras y los interesados.

Acuerdos de procesamiento de datos (DPA):

- Se firman DPA obligatorios con todos **procesadores de terceros** manejo de datos personales.
- Las DPA garantizan el cumplimiento de los requisitos del Artículo 28 del RGPD (por ejemplo, controles de subprocesamiento, medidas de seguridad, auditorías).

Privacidad por diseño y por defecto:

- Se desarrollan nuevos sistemas, servicios y procesos con **protección de datos integrados** desde el principio.
- Solo el **cantidad necesaria de datos personales** se recoge y procesa para cada finalidad.

Evaluaciones de impacto sobre la protección de datos (EIPD):

- Realizado para actividades de procesamiento de alto riesgo que involucran datos confidenciales, elaboración de perfiles a gran escala o nuevas tecnologías.
- Las evaluaciones de impacto de la protección de la privacidad evalúan los posibles impactos sobre la privacidad y proponen medidas de mitigación antes de su implementación.

Transferencias internacionales seguras de datos:

- Las transferencias de datos fuera de la UE/EEE se realizan bajo:
 - **Cláusulas contractuales estándar (CCE)** aprobado por la Comisión Europea.
 - **Decisiones de adecuación** donde se aplica.
 - **Medidas complementarias apropiadas** Si es necesario.

Respuesta a incidentes y notificación de infracciones:

- Los planes de respuesta a incidentes garantizan que las violaciones de datos personales se informen rápidamente a las autoridades supervisoras y, cuando sea necesario, a las personas afectadas.

9.3 Monitoreo, Auditoría y Documentación

Auditorías de Cumplimiento Interno:

- Las auditorías anuales evalúan la eficacia de las medidas de seguridad, el cumplimiento normativo y las prácticas de gestión de riesgos.
- Se documentan los hallazgos y se implementan acciones correctivas.

Mantenimiento de registros:

- **A Registro de Actividades de Tratamiento (ROPA)** se mantiene según el artículo 30 del RGPD.
- Los incidentes de seguridad, los informes de violaciones de datos y las evaluaciones de impacto de protección de datos se documentan exhaustivamente.

Monitoreo de proveedores:

- Revisiones periódicas del cumplimiento de las obligaciones contractuales de seguridad y privacidad por parte de proveedores externos.
- Cuestionarios de seguridad de terceros y auditorías in situ (para proveedores de alto riesgo).

9.4 Consecuencias del incumplimiento

El incumplimiento de las normas legales y reglamentarias puede resultar en:

- Multas administrativas (por ejemplo, multas del RGPD de hasta **20 millones de euros** o **4% de la facturación global anual**, el que sea mayor).
- Daño reputacional y pérdida de confianza del cliente.
- Acciones legales, sanciones civiles y sanciones regulatorias.
- Terminación de relaciones con proveedores por parte de terceros que no cumplan con las normas.

9.5 Compromiso con el cumplimiento continuo

Live Now Technology SLU se compromete a:

- Mantenerse informado sobre la evolución de las normativas de ciberseguridad y protección de datos.
- Actualizar las políticas de seguridad y privacidad de forma proactiva.
- Educar a los empleados sobre sus obligaciones legales. Colaborar con los reguladores de forma transparente y cooperativa.

10. Revisión y actualizaciones de políticas

Para garantizar que nuestro marco de seguridad de la información se mantenga **eficaz, relevante y conforme** con amenazas, tecnologías y regulaciones en constante evolución, **Live Now Technology SLU** está comprometido con un **proceso de revisión y mejora continua** para esta Política de Seguridad de la Información.

Una política estática no puede proteger adecuadamente a una organización dinámica; por lo tanto, **actualizaciones periódicas, auditorías y revisiones** son esenciales para mantener **postura de seguridad óptima y cumplimiento normativo**.

10.1 Frecuencia de revisión

Revisión anual:

- Esta Política de Seguridad de la Información se revisa **al menos una vez cada 12 meses** para garantizar que siga siendo precisa, completa y alineada con las amenazas, tecnologías y requisitos legales actuales.

Reseñas basadas en eventos:

La política también se revisará y actualizará inmediatamente si ocurre cualquiera de las siguientes situaciones:

- **Cambios organizativos significativos**(por ejemplo, fusiones, adquisiciones o reestructuraciones importantes).
- **Implementación de nuevas tecnologías**que podrían suponer un riesgo para la seguridad.
- **Nuevos requisitos legales o reglamentarios**(por ejemplo, actualizaciones del RGPD, Directiva NIS2).
- **Después de un importante incidente de seguridad**incorporar lecciones aprendidas y mejorar las defensas.

Monitoreo Regulatorio:

- Cambios en **Leyes europeas, nacionales o internacionales de ciberseguridad**son monitoreados regularmente por el **Departamentos de Cumplimiento y Legal**para activar actualizaciones de políticas.

10.2 Responsabilidades de revisión y actualización

Propietario de la póliza:

- El **Director de Seguridad de la Información (CISO)**o un asignado **Oficial de Gobernanza de Seguridad**es responsable de coordinar y supervisar el proceso de revisión de políticas.

Participación de las partes interesadas:

- Las revisiones implican la colaboración entre:
 - **Equipos de seguridad informática**(controles técnicos y defensas).
 - **Departamentos de Cumplimiento y Legal**(requisitos reglamentarios).
 - **Recursos humanos**(capacitación sobre conducta y concienciación de los empleados).
 - **Liderazgo ejecutivo**(planificación estratégica de seguridad y asignación de recursos).

Comunicación con los empleados:

- Cualquier **cambios sustanciales** La Política de Seguridad de la Información será **comunicado a todos los empleados**, contratistas y terceros afectados.
- Los empleados deben **acusar reciboyrevisión de políticas actualizadas** a través de procesos formales de reaceptación.

10.3 Control de versiones y documentación

Mecanismo de control de versiones:

- A cada iteración de la política se le asigna un **Número de versión, fecha de actualización y un resumen de los cambios**.
- Se mantiene un archivo de versiones anteriores para **finés de auditoría y referencia**.

Pistas de auditoría:

- Se realizan revisiones y actualizaciones de políticas **registrado y documentado** como parte de la organización **requisitos de preparación para auditorías** bajo marcos como **ISO/IEC 27001**.

Validación de cumplimiento:

- Las políticas actualizadas se validan de forma cruzada con:
 - Normas de seguridad de la información ISO/IEC 27001.
 - Requisitos del RGPD.
 - Marco de ciberseguridad del NIST (si corresponde).

10.4 Filosofía de Mejora Continua

En **Live Now Technology SLU** tratamos la seguridad de la información como un **proceso dinámico y continuo**, no una tarea de cumplimiento única.

Buscamos continuamente:

- **Adaptara** las amenazas y vulnerabilidades emergentes.

- **Mejorar** Las habilidades y la concienciación de los empleados en materia de seguridad.
- **Fortalecer** defensas tecnológicas a través de la innovación y las mejores prácticas.
- **Promover** una cultura de seguridad proactiva en toda la organización.

Declaración de compromiso:

Live Now Technology SLU se dedica a la mejora continua de las prácticas de seguridad de la información, garantizando la protección continua de nuestros datos, sistemas, clientes y reputación.

Política de Seguridad y Salud en el Trabajo

1. Introducción y propósito

En **Live Now Technology SLU** la salud, la seguridad y el bienestar de nuestros empleados, contratistas, visitantes y partes interesadas son fundamentales para nuestro éxito.

Reconocemos que mantener un ambiente de trabajo seguro, saludable y de apoyo no es sólo una **obligación legal y ética** pero también un facilitador crítico de **Productividad, innovación y satisfacción de los empleados**.

Esta Política de Seguridad y Salud en el Trabajo (SST) establece el compromiso de la empresa con:

Prevenición de lesiones, enfermedades y accidentes relacionados con el trabajo.

Promover una cultura de seguridad, responsabilidad y mejora continua.

Cumplir plenamente con las normas de seguridad y salud ocupacional aplicables en **el europeo** (p.ej, **Directiva 89/391/CEE de la UE**) y **niveles nacionales españoles** (p.ej, **Ley 31/1995 de Prevención de Riesgos Laborales - PRL**).

Integrar consideraciones de salud y seguridad en todas las decisiones operativas y de gestión.

A través de esta política, pretendemos garantizar que todas las personas que trabajan para o con **Live Now Technology SLU** pueden desempeñar sus funciones de una manera **un entorno seguro, saludable y de apoyo**, independientemente de si están ubicados en el sitio, de forma remota o en la ubicación del cliente.

2. Alcance y aplicabilidad

Esta Política de Seguridad y Salud en el Trabajo se aplica a:

- **Todos los empleados** (trabajadores permanentes, temporales, de tiempo completo, de tiempo parcial y remotos).
- **Contratistas, autónomos, consultores y pasantes** participar en cualquier actividad relacionada con la empresa.
- **Visitantes y clientes** que accedan a las instalaciones de la empresa o a los lugares del proyecto.

Ubicaciones cubiertas:

- Todos **Live Now Technology SLU** oficinas, instalaciones y ubicaciones operativas.
- **Entornos de trabajo remotos**, incluidas las oficinas en casa de los empleados cuando trabajan desde casa.
- **Sitios de clientes** donde los empleados de la empresa desempeñan funciones en virtud de acuerdos contractuales.

Actividades cubiertas:

- Actividades laborales diarias (incluido trabajo de oficina, trabajo remoto, trabajo de campo y servicios técnicos).
- Viajes de negocios, conferencias, reuniones fuera de la oficina y sesiones de capacitación.
- Uso de equipos, vehículos o infraestructura digital proporcionados por la empresa (trabajo relacionado con TI).

Todas las personas bajo el alcance de esta política son: **obligado a cumplir con sus principios y Contribuir activamente a mantener un entorno de trabajo seguro y saludable.**

3. Compromiso de la empresa con la salud y la seguridad

Live Now Technology SLU está plenamente comprometido a:

Cumplimiento legal:

- Cumplir con toda la legislación, normativa y estándares aplicables en materia de seguridad y salud, incluidas las leyes nacionales españolas y las directivas de la Unión Europea.
- Cumplir o superar las mejores prácticas de la industria en gestión de seguridad y salud ocupacional.

Prevención de Riesgos y Control de Peligros:

- Identificar y evaluar los riesgos en el lugar de trabajo de forma proactiva.
- Implementar medidas preventivas y de protección efectivas.
- Investigar todos los incidentes y cuasi accidentes para evitar que se repitan.

Promoción de la salud y el bienestar:

- Apoyar iniciativas que promuevan **salud física, mental y emocional**.
- Alentar **mejores prácticas ergonómicas**, especialmente para trabajadores remotos y de oficina.
- Ofrecer acceso a **programas y recursos de bienestar** cuyo objetivo es mejorar el equilibrio entre la vida laboral y personal y prevenir el estrés laboral.

Participación y consulta de los empleados:

- Fomentar la comunicación abierta y la participación activa de los empleados en asuntos relacionados con la salud y la seguridad.
- Establecer mecanismos formales para que los empleados **informar sobre peligros, inquietudes y sugerencias** confidencialmente.
- Involucrar a los empleados en **comités o grupos de trabajo de salud y seguridad**, cuando corresponda.

Mejora continua:

- Establecer objetivos y metas claros y medibles para el desempeño en materia de salud y seguridad.
- Seguimiento del desempeño mediante auditorías, inspecciones e informes.
- Revisar esta política periódicamente y actualizarla para reflejar los cambios en la legislación, las actividades organizacionales y los panoramas de riesgo.

Rendición de cuentas en todos los niveles:

- La dirección predica con el ejemplo y es responsable de la implementación de la política de salud y seguridad.
- Cada individuo comparte la responsabilidad de garantizar su propia seguridad y la de sus colegas.

Fomentando una fuerte cultura de seguridad Protegemos a nuestra gente, fortalecemos nuestra organización y demostramos nuestra responsabilidad con la sociedad.

“La seguridad no es solo una política: es un valor fundamental que define cómo trabajamos”.

4. Responsabilidades en materia de salud y seguridad

La salud y seguridad en el trabajo es una **responsabilidad compartida** en Live Now Technology SLU. Cada individuo dentro de la organización tiene un papel vital que desempeñar en el mantenimiento de un **ambiente de trabajo seguro y saludable**.

4.1 Responsabilidades del liderazgo de la empresa

- Demostrar **liderazgo visible y proactivo** en la promoción de la salud y la seguridad.
- Asegúrese de que **recursos adecuados (tiempo, personal y presupuesto)** se asignan para implementar programas de salud y seguridad.
- Incorporar objetivos de salud y seguridad en **procesos de planificación empresarial y toma de decisiones**.
- Fomentar un entorno donde **Los empleados se sienten empoderados** denunciar condiciones o comportamientos inseguros sin temor a represalias.
- Designar personal calificado para gestionar las responsabilidades de seguridad y salud en el trabajo.

4.2 Responsabilidades de los gerentes y supervisores

- Asegurarse de que los empleados bajo su supervisión estén **debidamente capacitado y equipado** para realizar sus tareas con seguridad.
- Conduct **inspecciones de seguridad periódicas** y **evaluaciones de riesgos** en sus áreas de responsabilidad.
- Inmediatamente **abordar conductas o condiciones inseguras** e iniciar acciones correctivas.
- Apoyar las investigaciones de incidentes mediante **recopilación de información precisa** y **Participar en análisis de causa raíz.**
- Dar ejemplo **adhiriéndose a todos los procedimientos de salud y seguridad.**

4.3 Responsabilidades de los empleados y contratistas

- **Cumplir con todas las instrucciones, procedimientos y capacitaciones de seguridad.**
- **Tome precauciones razonables** de su propia salud y seguridad y la de otras personas que puedan verse afectadas por sus acciones.
- **Informar rápidamente** cualquier peligro, práctica insegura o incidente a los supervisores o al Oficial de Salud y Seguridad.
- **Utilice equipo de protección (EPP)** apropiadamente cuando sea necesario.
- **Participar en sesiones de capacitación sobre salud y seguridad** y actualizaciones según sea necesario.
- **Cooperar con las investigaciones de incidentes** y las iniciativas de seguridad.

4.4 Responsabilidades del Oficial de Salud y Seguridad (o Proveedor Externo de Servicios de SST)

- **Desarrollar, implementar y actualizar** El sistema de gestión de seguridad y salud de la empresa.

- **Asesorar a la gerencia** sobre cumplimiento de salud y seguridad, mitigación de riesgos y mejores prácticas.
- **Realizar auditorías periódicas, inspecciones del lugar de trabajo y evaluaciones de riesgos.**
- **Impartir formación en salud y seguridad** a todo el personal.
- **Mantener registros de incidentes, auditorías e inspecciones.**, y realizar un seguimiento de las acciones correctivas.
- **Garantizar la preparación ante emergencias**, incluidos procedimientos de evacuación y capacitación en primeros auxilios.

5. Evaluación de riesgos y gestión de peligros

Enfoque proactivo Identificar y controlar los riesgos es esencial para mantener un entorno de trabajo seguro.

5.1 Identificación y evaluación de riesgos

- **Evaluaciones periódicas de riesgos** Se llevan a cabo para todas las operaciones de la empresa, incluidas oficinas, estaciones de trabajo remotas y sitios de proyectos.
- **Los peligros se identifican y documentan**, considerando riesgos físicos, ergonómicos, psicosociales y tecnológicos.
- **Niveles de riesgo** (Se evalúan la probabilidad y la gravedad y se priorizan las estrategias de mitigación en consecuencia).

5.2 Control y mitigación de riesgos

- Aplicar la **jerarquía de controles** acercarse:

1. **Eliminar** el peligro si es posible.
2. **Sustituir** con alternativas más seguras.

3. **Implementar controles de ingeniería** (por ejemplo, muebles ergonómicos, sistemas de ventilación).

4. **Implementar controles administrativos** (Por ejemplo, procedimientos de trabajo seguros, señalización).

5. **Utilice equipo de protección personal (EPP)** en último caso.

5.3 Informes y gestión de incidentes

- Todos **Accidentes, cuasi accidentes, condiciones inseguras y enfermedades** debe ser **reportado inmediatamente**.
- **Investigaciones de incidentes** Se llevan a cabo para determinar las causas fundamentales y prevenir que se repitan.
- Se asignan acciones correctivas, se realiza un seguimiento y se evalúa su eficacia.

5.4 Documentación y mantenimiento de registros

- Las evaluaciones de riesgos, los informes de incidentes y los planes de acción correctiva son **documentado y almacenado de forma segura**.
- Las revisiones periódicas de incidentes pasados ayudan a identificar **patrones y tendencias** para una mayor reducción del riesgo.

6. Preparación y respuesta ante emergencias

La preparación para emergencias es fundamental para **minimizar los daños y las perturbaciones** Durante eventos inesperados.

6.1 Procedimientos de emergencia

- **Planes de emergencia integrales** (Se mantienen los protocolos de seguridad (evacuación de incendios, emergencias médicas, desastres naturales) para todos los sitios.

- **Mapas de evacuación, extintores y botiquines de primeros auxilios.** Están claramente marcados y son de fácil acceso.
- **trabajadores remotos** También se les proporciona orientación de emergencia para sus oficinas en casa.

6.2 Equipos de respuesta a emergencias

- **Entrenado Equipos de respuesta a emergencias (ERT)** Se designan en cada sitio físico.
- Los ERT son responsables de:
 - Coordinar los esfuerzos de evacuación.
 - Proporcionar primeros auxilios básicos hasta que llegue ayuda profesional.
 - Comunicarse con los servicios de emergencia y el liderazgo interno.

6.3 Entrenamiento y ejercicios

- **Simulacros anuales de evacuación de emergencia** Se llevan a cabo en todas las instalaciones.
- **Formación en primeros auxilios** obligatorio para empleados seleccionados en cada ubicación.
- Los planes de emergencia son **Revisado y actualizado anualmente** después de cambios significativos (por ejemplo, reubicación, expansión).

6.4 Comunicación de crisis

- En caso de emergencia, limpie y **canales de comunicación oportunos** Se establecen (correos electrónicos, alertas SMS, sistemas de notificación internos).
- Los roles de comunicación de crisis y las vías de escalada son **predefinido y ensayado**.

6.5 Recuperación post-emergencia

- Después de cualquier emergencia, un **revisión posterior al incidente** Se lleva a cabo para analizar la efectividad y recomendar mejoras.

- Los Planes de Continuidad de Negocio (BCP) se activan si es necesario para garantizar la resiliencia operativa.

7. Promoción de la salud, el bienestar y la ergonomía

En **Live Now Technology SLU** creemos que la salud ocupacional se extiende más allá de prevenir accidentes físicos: también abarca **salud mental, ergonomía y bienestar holístico**. Nos comprometemos a crear un **ambiente de trabajo saludable y de apoyo** donde los empleados puedan prosperar física y mentalmente.

7.1 Mejores prácticas ergonómicas

- Todas las estaciones de trabajo (de oficina y remotas) están diseñadas siguiendo **estándares ergonómicos** para prevenir lesiones musculoesqueléticas.
- Se ofrecen evaluaciones ergonómicas a los empleados al momento de su incorporación o cuando lo solicitan.
- Se ponen a disposición sillas ajustables, soportes para monitores, teclados y otros equipos cuando sea necesario.
- Orientación para **trabajadores remotos**. Se proporciona información sobre cómo configurar oficinas en casa seguras y cómodas a través de recursos y consultas especializadas.

7.2 Salud mental y bienestar

- La empresa promueve la concienciación de **problemas de salud mental** y proporciona recursos para el manejo del estrés, la resiliencia y el equilibrio entre el trabajo y la vida personal.
- Los empleados tienen acceso confidencial a **servicios de apoyo a la salud mental** (Por ejemplo, programas de asistencia a empleados, asesores externos o asociaciones).
- Se gestionan las cargas de trabajo y los plazos para evitar **estrés excesivo relacionado con el trabajo**.

7.3 Iniciativas para un entorno de trabajo saludable

- Fomento de **descansos regulares**, incluido el uso de "microdescansos" para reducir la fatiga visual y las lesiones por movimientos repetitivos.
- Provisión de **recursos para un estilo de vida saludable**, incluidos programas de nutrición, ejercicio y bienestar.
- Soporte para **acuerdos de trabajo flexibles** Siempre que sea posible, para satisfacer las necesidades personales y promover la integración entre el trabajo y la vida personal.

8. Formación y Concienciación

La formación es esencial para **empoderar a los empleados** Reconocer peligros, comprender prácticas seguras y responder eficazmente en emergencias.

8.1 Requisitos de capacitación en salud y seguridad

- **Capacitación de incorporación obligatoria** sobre procedimientos de salud, seguridad y emergencia para todos los nuevos empleados.
- **Capacitación anual de actualización** para todos los empleados para reforzar los conceptos críticos de seguridad y actualizarlos sobre cualquier cambio de políticas o procedimientos.
- **Formación específica para cada puesto** para empleados que realizan actividades de mayor riesgo (por ejemplo, mantenimiento de salas de servidores, visitas al sitio, trabajo de campo).

8.2 Campañas de concienciación y comunicación

- En curso **iniciativas de concienciación** (Por ejemplo, carteles, boletines informativos y seminarios web promueven conductas seguras y resaltan los riesgos emergentes.
- **Días Mundiales de la Salud y la Seguridad** Se celebran internamente semanas de concientización sobre la salud mental y otros eventos.

8.3 Entrenamiento de simulacros de emergencia

- Regular**simulacros de incendio**Se llevan a cabo prácticas de evacuación y simulacros de respuesta de primeros auxilios para garantizar la preparación.
- Los trabajadores remotos reciben pautas sobre cómo responder ante emergencias en sus propios entornos de trabajo.

8.4 Mejora continua mediante retroalimentación de la capacitación

- Los comentarios de los empleados después de las sesiones de capacitación se recopilan y se utilizan para:**Mejorar el contenido y la impartición de la formación.**

9. Cumplimiento y Mejora Continua

El cumplimiento no es estático**mejora continua**Es vital garantizar los más altos estándares de salud y seguridad en el trabajo.

9.1 Cumplimiento normativo

- **Live Now Technology SLU**cumple con:
 - **Directiva 89/391/CEE de la UE**sobre la introducción de medidas para fomentar la mejora de la seguridad y la salud de los trabajadores.
 - **Ley 31/1995 de Prevención de Riesgos Laborales**(Ley de Prevención de Riesgos Laborales).
 - Normas ISO pertinentes (como**Sistemas de Gestión de Seguridad y Salud en el Trabajo ISO 45001**, cuando corresponda).

9.2 Auditorías periódicas de salud y seguridad

- Se realizan auditorías periódicas para identificar brechas, riesgos y oportunidades de mejora.
- Las acciones correctivas se priorizan y se implementan rápidamente después de los hallazgos de la auditoría.

9.3 Mecanismo de notificación de incidentes y peligros

- Se anima a todos los empleados a **informar sobre peligros, incidentes y cuasi accidentes de forma confidencial**.
- Todos los informes se registran, investigan y utilizan para mejorar las medidas de seguridad.

9.4 Revisiones de gestión y planes de mejora

- El desempeño en materia de salud y seguridad es **revisado anualmente por la alta dirección**.
- Las métricas de desempeño (por ejemplo, tasas de incidentes, hallazgos de auditoría, tasas de finalización de la capacitación) guían las iniciativas de mejora continua.

10. Reconocimiento y ejecución

Para garantizar un lugar de trabajo seguro es necesario: **participación activa y compromiso** de todas las personas asociadas a la empresa.

10.1 Reconocimiento del empleado

- Todos los empleados y contratistas deben **acusar recibo** de la Política de Seguridad y Salud en el Trabajo durante el onboarding.
- Al reconocer la política, las personas aceptan:
 - Cumplir** con todos los procedimientos de seguridad.
 - Tome medidas proactivas** para protegerse a sí mismos y a sus colegas.

- Informar sobre cualquier riesgo o violación de la salud y la seguridad**.inmediatamente.

10.2 Cumplimiento y acciones disciplinarias

- El incumplimiento de esta política, o cualquier desprecio deliberado por los procedimientos de salud y seguridad, puede resultar en **acción disciplinaria**, hasta e incluyendo:
 - Advertencias verbales o escritas.
 - Suspensión.
 - Terminación de la relación de trabajo o contrato.
 - Acciones legales si corresponde según la legislación laboral o penal.

10.3 Compromiso con la responsabilidad compartida

- La salud y la seguridad son un **esfuerzo colectivo**—una responsabilidad compartida entre la dirección, los empleados, los contratistas y los visitantes.
- Al trabajar juntos, creamos un **Un lugar de trabajo más seguro, saludable y productivo** Para todos.

Política ambiental

1. Introducción y propósito

En **Live Now Technology SLU** reconocemos que la responsabilidad ambiental es esencial para garantizar un **futuro sostenible**, y estamos comprometidos **minimizando el impacto ambiental** de nuestras operaciones, servicios y cadena de suministro.

Como empresa de consultoría e ingeniería digital que opera en toda Europa, puede que no seamos un gran contaminante en el sentido tradicional, pero comprendemos la importancia **impactos indirectos** Generamos a través de **consumo de energía, infraestructura digital, viajes y adquisiciones**.

Esta Política Ambiental describe nuestros **principios, objetivos y acciones** para proteger el medio ambiente y contribuir a esfuerzos globales como el **Pacto Verde Europeo, el Objetivos de Desarrollo Sostenible (ODS) de las Naciones Unidas**, y el cumplimiento de **legislación ambiental** en **ambos niveles de la UE y nacionales**.

Nuestro compromiso no es sólo cumplir con las leyes ambientales sino **ir más allá del cumplimiento** Al incorporar la sostenibilidad en el **núcleo de nuestra cultura, procesos de toma de decisiones y operaciones**.

2. Alcance y aplicabilidad

Esta Política Ambiental se aplica a:

Todas las operaciones y actividades realizado por Live Now Technology SLU, incluyendo funciones administrativas, técnicas, de consultoría y de trabajo en remoto.

Todos los empleados, contratistas, consultores y pasantes, ya sea trabajando en el sitio o de forma remota.

Proveedores, vendedores y prestadores de servicios externos, particularmente aquellos con impactos ambientales relacionados con nuestro negocio.

La política es relevante para todos los aspectos ambientales, incluidos, entre otros:

- **Consumo de energía** en oficinas, infraestructuras de servidores y estaciones de trabajo de empleados.

- **emisiones de gases de efecto invernadero** relacionados con el uso de energía, los desplazamientos y los viajes.
- **Sostenibilidad digital**, incluida la carga del servidor, el almacenamiento de datos y la eficiencia computacional.
- **Generación de residuos**, incluidos residuos electrónicos y materiales de oficina.
- **Obtención**, incluidos los estándares ambientales de los productos adquiridos y las prácticas de sostenibilidad de los proveedores.

Esta política también está alineada con **Sistemas de Gestión Ambiental ISO 14001:2015**, y sirve como base para nuestros esfuerzos de gestión ambiental y planes de mejora.

3. Compromisos y principios ambientales

En el centro de nuestros esfuerzos ambientales se encuentra un sólido conjunto de compromisos. Estos guían nuestra **estrategia, toma de decisiones, comportamiento de los empleados y relaciones con los proveedores**:

3.1 Cumplimiento y más allá

- Garantizar el pleno cumplimiento de **leyes, directivas y reglamentos ambientales aplicables** en todos los países donde operamos.
- Monitorear los cambios legislativos y actualizar proactivamente nuestras prácticas en consecuencia.
- Cuando sea posible, **adoptar normas internas más estrictas** que van más allá de los mínimos legales.

3.2 Prevención de la contaminación y reducción del impacto

- Prevenir la contaminación mediante **reducir los residuos, minimizar el consumo de recursos y eliminar sustancias peligrosas** de las operaciones.

- Fomentar **flujos de trabajo sin papel**, documentación digital y computación en la nube eficiente.
- Promocionar **colaboración remota** para reducir las emisiones de los desplazamientos y viajes.

3.3 Eficiencia de recursos y gestión energética

- Esforzarse por **uso eficiente de energía, agua y materiales**, especialmente en operaciones de oficina e infraestructura de TI.
- Migrar servicios a **proveedores de nube energéticamente eficientes y neutrales en carbono** Siempre que sea posible.
- Implementar estrategias para reducir la **huella de carbono** asociado con herramientas digitales, plataformas e infraestructura interna.

3.4 Economía circular y compras sostenibles

- Fomentar la reutilización, reparación y reciclaje de **equipos electrónicos y de oficina**.
- Dar preferencia a **productos y proveedores con certificación ecológica** con políticas de sostenibilidad transparentes.
- Ampliar los ciclos de vida de los productos y reducir el consumo excesivo de recursos.

3.5 Transparencia, colaboración y mejora continua

- Monitorear periódicamente el desempeño ambiental y **establecer objetivos ambientales mensurables**.
- Mejorar continuamente a través de **auditorías, revisiones y compromiso de los empleados**.
- Comunicarnos de manera transparente con las partes interesadas y los clientes sobre nuestra trayectoria y resultados en materia de sostenibilidad.

En Live Now Technology SLU, **La sostenibilidad no es un esfuerzo aislado**—Es parte integral de nuestra identidad y compromiso de ser una **Empresa responsable y preparada para el futuro**.

4. Áreas de enfoque clave

Para garantizar la implementación efectiva de nuestros compromisos ambientales, **Live Now Technology SLU** concentra sus esfuerzos de sostenibilidad en los siguientes pilares estratégicos:

4.1 Eficiencia energética y emisiones de carbono

- Optimizar el uso energético en oficinas e infraestructura digital.
- Priorizar el uso de **proveedores de energía renovable** en oficinas alquiladas y servicios en la nube.
- Fomentar **Uso inteligente de los sistemas de iluminación, calefacción y refrigeración**, apoyado por dispositivos de automatización y ahorro energético.
- Monitorear las emisiones de carbono de las operaciones de la empresa y **identificar oportunidades de reducción** anualmente.
- Usar **programas de compensación de carbono** donde la reducción directa no es factible.

4.2 Gestión de residuos y reciclaje

- Aplicar **principios de reducción de residuos** a todas las áreas de operación.
- Implementar **sistemas de separación selectiva de residuos** en las oficinas de la empresa (papel, plásticos, residuos electrónicos, orgánicos).
- Minimizar **materiales de un solo uso** y promover **suministros de oficina reutilizables**.
- Asegúrese de que los equipos obsoletos se eliminen mediante **programas certificados de reciclaje de residuos electrónicos**.

4.3 Compras sostenibles

- Dar preferencia a **avendedores y proveedores** que siguen prácticas ambientalmente sostenibles.
- Evaluar a los proveedores en función de sus **certificaciones ambientales, emisiones y prácticas laborales**.
- Adquirir **hardware de bajo consumo energético y con etiqueta ecológica**, materiales reciclados y consumibles de bajo impacto.
- Evitar la adquisición de **bienes físicos no esenciales**, especialmente si existen alternativas digitales.

4.4 TI verde y sostenibilidad digital

- Reducir el consumo de energía y las emisiones de **almacenamiento y procesamiento de datos** a través de:
 - Uso de **Servicios en la nube eficientes (por ejemplo, con garantías ISO 50001, ISO 14001 o neutralidad en carbono)**.
 - **Optimización del rendimiento del software** para reducir la carga computacional.
 - **Limpieza del almacenamiento digital** Periódicamente para reducir el uso innecesario de la nube.
- Concientizar sobre el **costo ambiental de la infraestructura digital** (centros de datos, entrenamiento de modelos grandes, almacenamiento excesivo de correo electrónico, etc.).

4.5 Viajes de negocios y trabajo remoto

- Fomentar **trabajo remoto** para reducir las emisiones derivadas de los desplazamientos y los viajes.
- Establecer políticas para **limitar los viajes de negocios** sólo a fines esenciales.
- Priorizar **viajes en tren en lugar de vuelos** para el transporte regional.

- Utilice reuniones virtuales y herramientas de colaboración para reemplazar eventos físicos cuando sea posible.
-

5. Roles y responsabilidades

La responsabilidad ambiental se comparte en toda la organización, con roles específicos definidos para garantizar la rendición de cuentas:

5.1 Liderazgo de la empresa

- Establecer el tono y la dirección de la política ambiental a través de la toma de decisiones estratégicas.
- Asignar **recursos y presupuesto** para iniciativas medioambientales.
- Garantizar el cumplimiento de los marcos legales y reglamentarios a nivel nacional y de la UE.
- Aprobar y monitorear los indicadores clave de desempeño (KPI) relacionados con la sostenibilidad.

5.2 Empleados

- Aplicar principios ambientales en sus tareas diarias (por ejemplo, reducir residuos, apagar los dispositivos que no se utilizan).
- Utilice políticas de trabajo y viajes remotos de manera responsable para limitar el impacto ambiental.
- Informar sugerencias, riesgos o problemas relacionados con las prácticas ambientales.
- Participar en campañas de formación y sensibilización.

5.3 Coordinador Ambiental (o Funcionario Asignado)

- Desarrollar y mantener **la sistema de gestión ambiental**.
- Seguimiento e informes **indicadores de desempeño** y métricas de cumplimiento.

- Establecer vínculos con departamentos y proveedores para integrar estándares ambientales.
- Coordinar campañas de concientización, auditorías y revisiones de políticas.

5.4 Proveedores y contratistas

- Debe adherirse a **requisitos ambientales** incluido en los contratos.
- Proporcionar prueba de certificaciones o compromisos de sostenibilidad cuando se le solicite.
- Colaborar en la reducción de envases, emisiones y residuos cuando sea posible.

6. Monitoreo, Cumplimiento y Mejora Continua

Para garantizar la eficacia de nuestros esfuerzos de gestión ambiental, Live Now Technology SLU establece un marco sólido para **medir, revisar y mejorar continuamente** Nuestro impacto ambiental.

6.1 Monitoreo del rendimiento

- Definir y realizar seguimiento **Indicadores Clave de Desempeño Ambiental (eKPI)**, como:
 - Consumo de electricidad y energía.
 - Emisiones de carbono de los viajes y los servicios digitales.
 - Volúmenes de residuos y tasas de reciclaje.
 - Métricas de impacto de las adquisiciones.
- Informe anual y análisis de resultados y avances.

6.2 Cumplimiento legal y regulatorio

- Garantizar el cumplimiento de las leyes y directivas ambientales aplicables:
 - **Directiva 2004/35/CE de la UE** sobre responsabilidad ambiental.
 - **Ley española 26/2007** sobre la responsabilidad ambiental.
 - Normas ISO 14001 cuando sea aplicable.
- Conducta **auditorías anuales de cumplimiento** para detectar brechas e implementar acciones correctivas.

6.3 Revisión de políticas y mejora continua

- Esta política se revisa al menos **una vez al año** después de cambios operativos significativos.
- La revisión incluye **evaluación de iniciativas actuales, comentarios de las partes interesadas y actualizaciones regulatorias**.
- Se implementan medidas correctivas y preventivas según sea necesario.

6.4 Comunicación externa y transparencia

- El desempeño ambiental puede incluirse en **divulgaciones anuales de sostenibilidad**.
- Los clientes y las partes interesadas pueden solicitar documentación o KPI relacionados con las prácticas ambientales.

7. Conciencia, compromiso y comunicación

Una política ambiental fuerte requiere no sólo compromisos definidos, sino también **compromiso y participación activos** en toda la organización. En **Tecnología Live Now**

SLU Nos esforzamos por construir una cultura donde la sostenibilidad sea **comprendido, practicado y promovido por todos los empleados y partes interesadas.**

7.1 Capacitación y educación ambiental

- Todos los empleados reciben **capacitación en concienciación ambiental** como parte del proceso de incorporación.
- Periódicos **sesiones de actualización y módulos de aprendizaje electrónico** Se proporcionan para mantener al personal informado sobre nuevas prácticas, regulaciones y objetivos internos.
- Equipos específicos (por ejemplo, adquisiciones, operaciones, infraestructura) pueden recibir **capacitación ambiental específica para cada función** relacionados con sus funciones.

7.2 Compromiso y participación de los empleados

- Se anima a los empleados a **Presentar sugerencias o iniciativas** que apoyan los objetivos de sostenibilidad.
- Campañas a nivel de toda la empresa, como **Semanas Verdes** o **Días de limpieza digital**, se organizan para reforzar el cambio de comportamiento.
- Las comunicaciones internas (boletines informativos, canales de Slack, intranet) incluyen contenido periódico sobre consejos, logros y oportunidades de sostenibilidad.

7.3 Comunicación externa y colaboración con las partes interesadas

- Somos transparentes con los clientes, proveedores y socios sobre nuestros objetivos y avances ambientales.
- Los compromisos de sostenibilidad pueden ser **incluido en propuestas, contratos con proveedores y documentación del cliente**, cuando corresponda.
- Nosotros apoyamos **esfuerzos de colaboración** con socios externos (grupos industriales, ONG, organismos reguladores) para amplificar nuestro impacto ambiental.

7.4 Promoción de una cultura de sostenibilidad

- La sostenibilidad no se trata como una iniciativa aislada, sino como un **parte integral de cómo trabajamos, pensamos y crecemos**.
- Se espera que los gerentes **predicar con el ejemplo**, incorporando criterios ambientales en la planificación, adquisiciones y actividades del equipo.
- Los trabajadores remotos y los equipos híbridos participan por igual a través de campañas virtuales y orientación sobre prácticas de sostenibilidad en el hogar.

8. Reconocimiento y gobernanza de políticas

Para garantizar la implementación efectiva de esta política, **Live Now Technology SLU** Define mecanismos claros de gobernanza, responsabilidad y aplicación.

8.1 Reconocimiento de responsabilidad

- Todos los empleados y contratistas deben **Reconocer su comprensión de esta Política Ambiental** y comprometerse a cumplir con sus principios.
- La póliza está incluida en **documentación de incorporación de empleados**, y podrá requerirse una reafirmación periódica durante las revisiones o auditorías anuales.

8.2 Disponibilidad y accesibilidad de la política

- Esta política está disponible para todos los empleados, clientes, proveedores y partes interesadas a través de nuestros sistemas de documentación interna y el sitio web de la empresa (cuando corresponda).
- Se podrán proporcionar copias impresas o digitales a pedido para fines de cumplimiento o documentación relacionada con el proyecto.

8.3 Cumplimiento e incumplimiento

- Las violaciones de esta política pueden resultar en **acción correctiva o disciplinaria**, dependiendo de la naturaleza y gravedad de la infracción.
- Los gerentes y el coordinador ambiental son responsables de investigar el incumplimiento, emitir recomendaciones y garantizar la resolución.

8.4 Ciclo de revisión y actualización de políticas

- Esta política se revisa **anualmente** y se actualizará según sea necesario para reflejar:
 - Cambios en la legislación o mejores prácticas.
 - Cambios operativos dentro de la empresa.
 - Resultados de desempeño ambiental o hallazgos de auditoría.

La responsabilidad ambiental es una obligación compartida. Mediante la concienciación, la innovación y la rendición de cuentas, podemos marcar una diferencia duradera para nuestro planeta y las generaciones futuras.

Política de Calidad

1. Introducción y propósito

En **Live Now Technology SLU** la calidad no es solo un objetivo, sino un valor fundamental que define nuestra identidad, nuestra ética de trabajo y nuestra visión a largo plazo. Nos dedicamos a ofrecer... **servicios y soluciones de alta confiabilidad** que cumplan o superen las expectativas de nuestros clientes, socios y partes interesadas.

Esta Política de Calidad establece nuestro compromiso estratégico con:

- **Brindar servicios que sean técnicamente sólidos, compatibles y alineados con los objetivos de la misión del cliente..**
- **Fomentar una cultura empresarial basada en mejora continua, excelencia operativa y atención al detalle.**
- **Alinear nuestras prácticas de gestión de calidad con normas internacionales, como ISO 9001:2015.**

En un entorno empresarial impulsado por **procesamiento de datos, desarrollo de software, ingeniería de sistemas y cumplimiento de los programas espaciales y medioambientales europeos**, el **fiabilidad y trazabilidad** de nuestros entregables es esencial. Nuestros clientes confían en nosotros para obtener soluciones que son **seguro, escalable, bien documentado y rigurosamente validado**—y estamos comprometidos a ganarnos y mantener esa confianza.

2. Alcance y aplicabilidad

Esta Política de Calidad se aplica a:

Todas las actividades, procesos y servicios realizado por Live Now Technology SLU.

Todos los empleados, contratistas y unidades de negocio, independientemente de la ubicación, ya sea trabajando en operaciones internas, proyectos de clientes o iniciativas de colaboración.

Todas las fases del proyecto, desde la ingeniería de preventa y el diseño del sistema hasta la entrega, el mantenimiento y el soporte posterior a la implementación.

La póliza cubre:

- **Ingeniería y desarrollo de software**(incluidos prototipos, sistemas operativos y software científico).
- **Soluciones de procesamiento y análisis de datos**, particularmente en contextos de observación de la Tierra y vigilancia ambiental.
- **Ingeniería de sistemas**, incluidas las fases de diseño, verificación, integración y validación.
- **Gestión de proyectos y servicios**, incluidas las comunicaciones y la documentación del cliente.
- **Interacciones con terceros/proveedores**, donde existen dependencias de calidad.

Se espera que cada persona involucrada en la prestación de nuestros servicios, ya sea interna o externamente, cumpla con los **estándares de calidad, procedimientos y prácticas éticas** definidos en esta política.

3. Compromisos de calidad

Live Now Technology SLU se compromete a mantener una **cultura de calidad robusta** basado en los siguientes principios:

3.1 Satisfacción del cliente

- Colocamos **Las necesidades del cliente en el centro** de nuestro trabajo.
- Nos esforzamos por ofrecer **A tiempo, dentro del alcance y al nivel de rendimiento esperado**.
- Buscamos activamente comentarios y los utilizamos para mejorar los servicios y las relaciones.
- Nuestro objetivo es convertirnos en un **socio de confianza a largo plazo**, no sólo un proveedor de una sola vez.

3.2 Cumplimiento de normas y requisitos

- Nos adherimos **requisitos contractuales, legales y reglamentarios**, incluidas las normas europeas e internacionales aplicables (por ejemplo, ECSS, ISO 9001, GDPR).
- Mantenemos **trazabilidad, reproducibilidad y validación** en todos los entregables técnicos.
- Implementamos **controles de calidad y revisiones formales** en cada hito crítico del proyecto.

3.3 Mejora continua

- Regularmente **Revisar nuestros procesos y herramientas internas** para identificar y eliminar ineficiencias.
- Promovemos una mentalidad de **aprendizaje, intercambio de conocimientos y evolución de prácticas** entre equipos.
- Las no conformidades se abordan mediante **análisis estructurado de causa raíz y planes de acción correctiva**.
- Se fomenta y apoya la innovación y la excelencia en todas las áreas de la empresa.

3.4 Confiabilidad, integridad y profesionalismo

- Nos aseguramos de que nuestros resultados sean **técnicamente preciso, seguro y confiable**.
- Nos comunicamos de forma transparente con nuestros clientes y mantenemos **integridad profesional** en todos los aspectos de la entrega.
- La calidad no solo se verifica, se **Diseñado en cada etapa** de nuestro trabajo.

4. Sistema de Gestión de Calidad (SGC)

En **Live Now Technology SLU** Nuestro Sistema de Gestión de Calidad (SGC) está diseñado para garantizar que todos los proyectos, procesos y entregables cumplan consistentemente con ambos **estándares de desempeño interno y requisitos contractuales y reglamentarios externos**.

4.1 Componentes clave del SGC

- **Procesos documentados** para desarrollo de software, ingeniería de datos, diseño de sistemas, gestión de proyectos y validación.
- **Pensamiento basado en el riesgo** y enfoques preventivos aplicados a lo largo del ciclo de vida de cada servicio o producto.
- Uso de **sistemas de gestión de configuración y control de versiones** para garantizar la trazabilidad.
- Integración de **puntos de control de calidad**, revisiones y auditorías de los planes del proyecto y los hitos de entrega.

4.2 Herramientas digitales y automatización

- Uso de **plataformas de seguimiento de proyectos (por ejemplo, Jira, Git, paneles internos)** para gestionar tareas y controles de calidad.
- **Pruebas automatizadas, pipelines de CI/CD** y se emplean flujos de trabajo de revisión de código para reducir errores y mejorar la repetibilidad.
- La documentación y los entregables están versionados y almacenados de forma segura, con **control de acceso y registros de auditoría**.

4.3 Alineación con la norma ISO 9001 y las mejores prácticas de la industria

- El SGC se alinea con la **ISO 9001:2015** Norma para Sistemas de Gestión de Calidad.
- Cuando corresponda, los controles de calidad se adaptan para cumplir con **Estándares ECSS** (para sistemas espaciales) y otros marcos específicos del dominio.
- El SGC evoluciona a través de **bucles de retroalimentación, sesiones de lecciones aprendidas y auditorías internas**.

5. Roles y responsabilidades

5.1 Dirección ejecutiva

- Definir la empresa **objetivos y visión de calidad**.
- Proporcionar **recursos, liderazgo y visibilidad** para el SGC.
- Revisar los datos de rendimiento y **validar mejoras estratégicas** anualmente.

5.2 Gerentes de proyecto y líderes de equipo

- Asegurarse **La ejecución del proyecto se adhiere a los procedimientos de calidad definidos**.
- Monitorear los entregables para **integridad técnica, satisfacción del cliente y cumplimiento contractual**.
- Facilitar **Revisiones de calidad y aprobaciones** en etapas clave.
- Informar problemas o desviaciones de forma proactiva e impulsar su resolución.

5.3 Función de garantía de calidad / Responsable designado

- Mantener y actualizar el **Documentación del sistema de gestión de calidad**.
- Conducta **auditorías internas periódicas y revisiones de calidad**.
- Realizar seguimiento y analizar no conformidades y oportunidades de mejora.
- Apoyar los esfuerzos de certificación y garantizar la alineación con los estándares externos.

5.4 Todos los empleados y contratistas

- Comprender y seguir los procedimientos del SGC relevantes para sus funciones.
- Asumir la responsabilidad personal por **la calidad de su trabajo**.
- Informar a los líderes de su equipo sobre cualquier riesgo, cuello de botella o desviación relacionada con la calidad.

- Participar activamente en **Lecciones aprendidas, retrospectivas y esfuerzos de mejora continua.**

6. Seguimiento, evaluación y mejora continua

Nuestra estrategia de calidad está impulsada por **datos, medición y rendición de cuentas.**

6.1 Indicadores clave de calidad (KQI)

- Entrega oportuna de los hitos del proyecto.
- Densidad de defectos y tiempo de resolución de problemas.
- Métricas de satisfacción del cliente (feedback, encuestas, NPS).
- Cumplimiento de procesos internos y puntuaciones de auditoría.
- Efectividad de las acciones correctivas y preventivas (CAPA).

6.2 Auditorías y revisiones internas

- **Auditorías planificadas** Se realizan periódicamente para evaluar el cumplimiento y detectar ineficiencias.
- **Revisiones y retrospectivas posteriores al proyecto** ayudar a capturar conocimientos y mejoras.
- Las desviaciones y no conformidades son **documentado, rastreado y resuelto** a través de un proceso estructurado.

6.3 Aprendizaje continuo y optimización de procesos

- Las mejores prácticas y los activos reutilizables (por ejemplo, plantillas, listas de verificación, herramientas) se comparten entre los equipos.

- El análisis de causa raíz (RCA) se aplica sistemáticamente para evitar la recurrencia de problemas críticos.
- Se anima al personal a **Proponer mejoras de procesos y enfoques innovadores.**

7. Revisión y reconocimiento de políticas

7.1 Ciclo de revisión de políticas

- Esta Política de Calidad es revisada **anualmente** por la alta dirección y el responsable de calidad designado.
- Puede actualizarse antes en respuesta a:
 - Cambios en la estrategia o alcance operativo.
 - Hallazgos de auditoría o cambios significativos en el proceso.
 - Actualizaciones regulatorias o requerimientos del cliente.

7.2 Reconocimiento y cumplimiento

- Todos los empleados y colaboradores deben **Lea, comprenda y comprométase con esta Política de Calidad** como parte de la incorporación.
- Se puede solicitar un reconocimiento continuo durante las revisiones anuales, las evaluaciones de cumplimiento o las auditorías de certificación.

7.3 Disponibilidad de la política

- La política está disponible a través de los sistemas de documentación internos y puede compartirse con clientes, socios y organismos de certificación previa solicitud.
- Refleja la **El compromiso de la empresa con la transparencia, la confiabilidad y la excelencia profesional.**

En Live Now Technology SLU, la calidad no es una tarea única; es nuestra forma de operar, entregar y crecer. Nos permite cumplir con los altos estándares de nuestros clientes y la integridad de nuestra misión. ✓

Política de Continuidad de Negocio y/o Crisis de Seguridad de la Información Plan de Gestión

1. Introducción y propósito

En **Live Now Technology SLU** reconocemos que la prestación ininterrumpida de servicios, la integridad de los datos y la resiliencia operativa son vitales para el éxito de nuestro negocio y para la confianza que nuestros clientes depositan en nosotros. Como proveedor de soluciones de ingeniería, software y procesamiento de datos para entornos de alta fiabilidad, incluidos los programas espaciales y medioambientales europeos, debemos garantizar que nuestros servicios... **Soportar las perturbaciones y recuperarse rápidamente de las crisis.**

Esta política establece nuestro marco para:

- **Asegurarse continuidad del negocio** Ante interrupciones internas y externas.
- Responder con rapidez y eficacia a **incidentes de seguridad de la información y amenazas cibernéticas.**
- Protegiendo a nuestros **clientes, infraestructura, propiedad intelectual y reputación.**

Esta política se alinea con las mejores prácticas y estándares de la industria, incluidos:

- **ISO 22301**–Sistemas de Gestión de Continuidad de Negocio (BCMS)
- **ISO/IEC 27035**–Gestión de incidentes de seguridad de la información
- **NIST SP 800-61**–Guía de manejo de incidentes de seguridad informática

El propósito de esta política es **Prevenir, prepararse, responder y recuperarse de eventos disruptivos**, ya sea causado por ciberataques, fallas del sistema, desastres naturales o errores humanos, y para **Mantener la confianza, el cumplimiento y la integridad operativa** en todo momento.

2. Alcance y aplicabilidad

Esta política se aplica a:

- **Todas las operaciones, empleados, contratistas y sistemas de TI de Live Now Technology SLU**, ya sea en el sitio, de forma remota o en la nube.
- **Funciones críticas de negocio**, incluyendo entrega de software, procesamiento de datos, consultoría técnica, soporte de sistemas y gestión de proyectos.
- Todas las etapas de **gestión de incidentes y planificación de la continuidad**, desde la detección de amenazas hasta la restauración del servicio.

La política es aplicable a ambos:

- **Gestión de la Continuidad del Negocio (BCM)**: Garantizar que la organización pueda mantener los servicios esenciales durante y después de una interrupción.
- **Gestión de crisis de seguridad de la información (ISCM)**: Detección, respuesta y recuperación ante brechas de seguridad e incidentes cibernéticos.

Esta política es **integrado con** los siguientes marcos internos:

- Política de seguridad de la información
- Política de Gestión de Riesgos
- Política de Calidad
- Marco de protección de datos (RGPD)
- Protocolos de comunicación interna

3. Objetivos de la Continuidad del Negocio

Los principales objetivos de esta Política de Continuidad de Negocio y Gestión de Crisis son:

3.1 Proteger a las personas y los activos

- Proteger la salud y la seguridad de los empleados y las partes interesadas durante las interrupciones operativas.
- Proteger datos, sistemas, infraestructura y activos físicos contra daños o pérdidas.

3.2 Minimizar el impacto empresarial

- Asegúrese de que **Las operaciones críticas pueden continuar** con una interrupción mínima.
- Reducir el tiempo de inactividad y la pérdida de datos mediante... **Objetivos de tiempo de recuperación (RTO)** y **Objetivos de punto de recuperación (RPO)**.
- Limitar el impacto financiero, legal y reputacional de las crisis.

3.3 Respuesta rápida y recuperación

- Proporcionar procedimientos claros y rutas de escalamiento para **responder con rapidez y eficacia** a los incidentes.
- **Restablecer las operaciones normales dentro de los plazos predefinidos**, respaldado por redundancia, copias de seguridad y soporte externo cuando sea necesario.

3.4 Mantener la confianza y el cumplimiento

- Cumplir con las obligaciones con los clientes, socios y reguladores, incluidas **acuerdos de nivel de servicio contractuales (SLA)**.
- Cumplir con las normas de protección de datos (por ejemplo, GDPR) y los requisitos de notificación de incidentes (por ejemplo, notificación dentro de las 72 horas posteriores a una infracción).

3.5 Preparación continua

- Probar y revisar periódicamente los planes de continuidad del negocio y de respuesta a incidentes.
- Fomentar una **cultura de resiliencia** en toda la organización, garantizando que el personal esté consciente, capacitado y preparado.

4. Planificación de la Continuidad del Negocio (PCN)

Nuestro **Plan de Continuidad de Negocio (PCN)** está diseñado para garantizar la continuidad de las operaciones críticas, incluso ante eventos disruptivos. El plan describe estrategias para **preparación, mitigación, respuesta y recuperación** en todas las funciones clave.

4.1 Identificación de funciones críticas del negocio

Cada departamento es responsable de identificar sus **actividades de misión crítica** y el **recursos** necesarios para mantenerlos o restaurarlos. Estos suelen incluir:

- Acceso al código fuente y repositorios.
- Servicios digitales y hosting de cara al cliente.
- Tuberías de procesamiento de datos e infraestructura en la nube.
- Herramientas de comunicación y colaboración.
- Operaciones legales y de cumplimiento.

4.2 Objetivos de recuperación

- **Objetivo de tiempo de recuperación (RTO):** El tiempo máximo aceptable para restaurar un servicio después de una interrupción.
- **Objetivo de punto de recuperación (RPO):** La máxima pérdida de datos tolerable expresada en tiempo.

Estos se definen por sistema o proceso y se documentan dentro del BCP.

4.3 Estrategias de continuidad

- Uso de **Infraestructura basada en la nube con alta disponibilidad (HA)** y redundancia regional.
- **Capacidades de trabajo remoto** para todo el personal esencial.
- Seguro y frecuente **copias de seguridad de datos**, almacenados en entornos externos o en la nube.

- Preaprobado **proveedores alternativos** para servicios o infraestructuras críticas.
- **Entornos virtuales preconfigurados** para desarrollo y operaciones.

4.4 Propiedad y mantenimiento del BCP

- Cada departamento nombra a un **Coordinador de Continuidad de Negocio**.
- **El BCP se revisa al menos anualmente**, y después de incidentes importantes o cambios organizativos.
- Todos los empleados reciben capacitación sobre sus responsabilidades bajo el BCP.

5. Gestión de incidentes y crisis de seguridad de la información

El **Plan de Respuesta a Incidentes (PRI)** define cómo detectar, responder y recuperarse de **incidentes de ciberseguridad** y **violaciones de datos**. Garantiza que todos los incidentes se gestionen de manera eficiente y en cumplimiento de las obligaciones legales y contractuales.

5.1 Detección y notificación de incidentes

- Todos los empleados están obligados a informar cualquier incidente sospechoso **inmediatamente** al equipo de seguridad designado.
- Las categorías de incidentes incluyen:
 - Acceso no autorizado o fuga de datos
 - Infección por ransomware o malware
 - Intentos de phishing o ingeniería social
 - Compromiso de credenciales o sistemas de autenticación

5.2 Equipo de Respuesta a Incidentes (IRT)

- El IRT incluye Seguridad de TI, Legal, Comunicaciones y Gestión Ejecutiva.
- Las responsabilidades incluyen:
 - **Evaluación y contención** del incidente
 - Preservación de evidencia
 - **Coordinación de la remediación y la recuperación**
 - Comunicación con las partes interesadas afectadas

5.3 Escalada y clasificación

Los incidentes se clasifican por **nivel de gravedad**, con rutas de escalada claras:

- **Bajo**: Sin impacto en las operaciones.
- **Medio**: Interrupción temporal o exposición limitada de datos.
- **Alto**: Interrupción importante, violación de datos confidenciales, exposición regulatoria.

Cada nivel tiene predefinidos **plazos de respuesta** y las acciones requeridas.

5.4 Obligaciones legales y regulatorias

- Todas las violaciones de datos personales se informan a las autoridades pertinentes de conformidad con **Artículo 33 del RGPD**.
- Los clientes afectados por el incidente son notificados de acuerdo con los SLA contractuales.

6. Comunicación durante la interrupción

Una comunicación eficaz es esencial para mantener **confianza y control** durante un evento disruptivo.

6.1 Comunicación interna

- Se mantienen árboles de contactos de emergencia y canales seguros (por ejemplo, Signal, correo electrónico cifrado).
- Los boletines internos específicos de cada crisis informan al personal sobre las acciones y actualizaciones.
- Los líderes departamentales coordinan la comunicación con sus equipos.

6.2 Comunicación externa

- **A Portavoz designado** Maneja todas las comunicaciones con los clientes y los medios.
- Los clientes son informados de forma proactiva si sus servicios o datos pueden verse afectados.
- Se mantienen plantillas de comunicación para:
 - Avisos de interrupción del servicio
 - Notificaciones de violación de datos
 - Actualizaciones del estado de las garantías y la mitigación

6.3 Plataformas de comunicación

- Sitio web de la empresa o página de estado (si está disponible)
- Boletines informativos por correo electrónico a clientes o partes interesadas
- Portales seguros para documentación (por ejemplo, informes de incidentes)

7. Pruebas, mantenimiento y revisión

Para garantizar la eficacia, los Planes de Continuidad de Negocio y Respuesta a Incidentes deben ser **Probado, mantenido y mejorado continuamente.**

7.1 Pruebas periódicas

- **Simulaciones anuales de continuidad a escala real**(Por ejemplo, falla del centro de datos o escenario de ransomware.
- Periódico**ejercicios de mesa**para simular procedimientos de respuesta.
- **Revisiones posteriores al ejercicio**con elementos de acción y lecciones aprendidas documentadas.

7.2 Mantenimiento y actualizaciones del plan

- Los planes se revisan al menos**anualmente**, o cuando:
 - Cambios críticos en los sistemas
 - Cambios en la estructura organizacional
 - Se actualizan los marcos legales o regulatorios
 - Después de cualquier interrupción o incidente importante

7.3 Concientización y capacitación de los empleados

- Todo el personal está capacitado en reconocimiento de incidentes, informes y protocolos de recuperación.
- Formación dirigida a:
 - Equipos de respuesta de seguridad
 - Gerentes de proyectos
 - Personal de atención al cliente

La resiliencia no se construye durante una crisis, sino con la preparación. En Live Now Technology SLU, nos comprometemos a mantenernos operativos, receptivos y confiables incluso ante una disrupción.

Procedimiento de respuesta a incidentes de seguridad

1. Introducción y propósito

En **Live Now Technology SLU**, asegurando la **confidencialidad, integridad y disponibilidad** de datos y sistemas es una prioridad fundamental. Como empresa que opera en entornos de alta confiabilidad como **software científico, ingeniería de sistemas y procesamiento de datos de observación de la Tierra** Nuestra capacidad para detectar y responder a incidentes de seguridad es crucial para mantener la confianza del cliente, el cumplimiento normativo y la resiliencia operativa.

El **Procedimiento de respuesta a incidentes de seguridad (SIRP)** proporciona un **enfoque estructurado y estandarizado** para detectar, gestionar, mitigar y aprender de los incidentes de seguridad de la información. Este procedimiento respalda nuestro enfoque más amplio: **Política de seguridad de la información, Plan de Continuidad de Negocio**, y nuestras obligaciones de cumplimiento bajo **ISO/IEC 27001, ISO/IEC 27035**, y el **Reglamento General de Protección de Datos (RGPD)**.

Este documento tiene como objetivo:

- Minimizar el impacto de las violaciones de seguridad y los compromisos del sistema.
- Garantizar un proceso consistente y repetible para todo tipo de incidentes de seguridad.
- Permitir la toma de decisiones rápida, el cumplimiento legal y la comunicación con el cliente.
- Integrar las lecciones aprendidas en nuestro **marco de mejora continua**.

2. Alcance y definiciones

2.1 Alcance

Este procedimiento se aplica a:

- **Todos los sistemas de información, infraestructura y servicios** gestionado o utilizado por Live Now Technology SLU.

- **Todos los empleados, contratistas, colaboradores externos, y proveedores de servicios externos.**

- Todos los incidentes que impliquen infracciones potenciales o reales de:
 - Confidencialidad de los datos**

 - Integridad del sistema**

 - Disponibilidad del servicio**

 - Obligaciones legales o reglamentarias**

Incluye incidentes que afectan a:

- Sistemas corporativos internos (correo electrónico, RR.HH., finanzas)

- Entornos de proyecto (datos o software específicos del cliente)

- Plataformas en la nube, API y repositorios de código fuente (por ejemplo, GitHub, AWS, Firebase)

2.2 Definiciones

- **Incidente de seguridad:**Cualquier evento o serie de eventos que comprometan o amenace con comprometer la confidencialidad, integridad o disponibilidad de sistemas o datos.

- **Incumplimiento:**Un evento confirmado en el que se ha accedido, divulgado, alterado o destruido datos o sistemas sin autorización.

- **Respuesta a incidentes (IR):**Las actividades coordinadas para identificar, contener, mitigar, investigar y recuperarse de un incidente de seguridad.

- **CSIRT (Equipo de respuesta a incidentes de seguridad informática):**Un grupo designado responsable de gestionar el ciclo de vida del incidente.

- **RCA (Análisis de causa raíz):**Un proceso estructurado para determinar las causas subyacentes de un incidente.

3. Objetivos del procedimiento de respuesta a incidentes

Los principales objetivos del Procedimiento de Respuesta a Incidentes de Seguridad son:

3.1 Habilitar la detección y contención rápidas

- Asegúrese de que todos los empleados y sistemas puedan **Detectar rápidamente anomalías o amenazas**.
- Aplicar **Mecanismos de monitoreo, alerta y registro en tiempo real** a sistemas y servicios críticos.
- Contener el impacto para evitar la escalada o el movimiento lateral de los ataques.

3.2 Estandarizar los procedimientos de respuesta

- Proporcionar un **proceso claro paso a paso** para responder a incidentes en todos los equipos y ubicaciones.
- Garantizar la clasificación, escalada y documentación consistentes de cada caso.
- Definir **roles, responsabilidades y vías de escalamiento** desde el momento en que se reporta un incidente.

3.3 Mantener el cumplimiento normativo y contractual

- Garantizar el cumplimiento de **Artículo 33 del RGPD**, incluido:
 - Informar a las autoridades sobre violaciones de datos personales dentro de **72 horas**.
 - Notificar a los clientes o usuarios afectados cuando sea necesario.
- Garantizar que se respeten los SLA contractuales con los clientes durante la respuesta a incidentes.

3.4 Proteger la confianza de las partes interesadas y la reputación de la empresa

- Mantener la transparencia y el profesionalismo en la comunicación durante los incidentes.
- Tranquilizar a los clientes y socios de que **controles efectivos, investigación y recuperación** están en su lugar.

3.5 Apoyar la mejora continua

- Realizar **revisiones posteriores al incidente** para identificar causas fundamentales, fallas de procesos y futuras estrategias de prevención.
- Actualizar políticas, procedimientos y capacitación en función de incidentes reales e inteligencia de amenazas.

4. Clasificación y priorización de incidentes

Clasificar los incidentes con precisión es clave para determinar la respuesta adecuada. **estrategia de respuesta, asignación de recursos y requisitos de comunicación.**

4.1 Criterios de clasificación

Los incidentes se clasifican en función de cuatro dimensiones:

1. **Impacto en la confidencialidad, integridad o disponibilidad (CIA)**
2. **Alcance de los sistemas o usuarios afectados**
3. **Implicaciones legales y regulatorias** (por ejemplo datos personales involucrados)
4. **Posible daño a la reputación o financiero**

4.2 Niveles de gravedad

Gravedad y	Descripción	Ejemplos
---------------	-------------	----------

Crítico	Interrupción grave de los servicios básicos, filtración de datos confirmada y riesgo regulatorio importante	Ransomware que afecta la infraestructura de la nube y vulneración de datos de clientes
Alto	Interrupción parcial del servicio, violación de credenciales, acceso no autorizado	Inicio de sesión remoto sospechoso en la consola de administración
Medio	Compromiso aislado del sistema, clic de phishing sin ejecución	Computadora portátil de usuario infectada sin acceso a sistemas internos
Bajo	Intento de ataque fallido, configuración incorrecta sin exposición de datos	Escaneo de puertos, ataque de fuerza bruta fallido

4.3 Ventanas de respuesta prioritaria

Cada nivel de gravedad tiene un valor correspondiente. **Objetivo de tiempo de respuesta (RTO):**

- **Crítico:**<1 hora
- **Alto:**<4 horas
- **Medio:**<24 horas
- **Bajo:**<72 horas

5. Proceso de gestión de incidentes (detección a cierre)

5.1 Fase 1: Detección y generación de informes

- Los eventos de seguridad son **monitoreado a través de sistemas automatizados, registros, alertas**, y los informes de los usuarios.
- Todos los empleados deben reportar inmediatamente cualquier actividad sospechosa a la **Equipo de respuesta a emergencias de CSIRT** a través de canales seguros.
- Se realiza un triaje inicial para determinar la validez y la gravedad potencial.

5.2 Fase 2: Contención

- Para los incidentes confirmados, el objetivo es **limitar la propagación y el daño**:
 - Aislar los puntos finales o servicios afectados.
 - Revocar o restablecer credenciales comprometidas.
 - Deshabilite las cuentas vulnerables o las reglas de firewall si es necesario.

5.3 Fase 3: Erradicación y mitigación

- Eliminar componentes maliciosos (por ejemplo, malware, puertas traseras).
- Parchear vulnerabilidades explotadas o corregir configuraciones incorrectas.
- Revisar y limpiar registros, objetos de la nube o artefactos de red.

5.4 Fase 4: Recuperación

- Restaurar los servicios y sistemas afectados utilizando **copias de seguridad limpias**.
- Conduct **validación del sistema** y reintegración a la producción.
- Monitorear de cerca después de la recuperación para detectar reinfecciones o ataques relacionados.

5.5 Fase 5: Documentación y cierre

- Informe completo del incidente: cronograma, impacto, acciones, partes afectadas.
- Registrar incidentes en el sistema interno con etiquetas y severidad.
- Disparador **análisis de causa raíz (RCA)** para incidentes críticos y de alta gravedad.

6. Funciones y responsabilidades de respuesta a incidentes

Una estructura de equipo bien definida garantiza **respuesta rápida y coordinada**.

6.1 Equipo de respuesta a incidentes de seguridad informática (CSIRT)

Liderado por el **Oficial de Seguridad de la Información**, incluye:

- **Operaciones de TI**
- **Infraestructura en la nube / DevOps**
- **Legal / Cumplimiento**
- **Líder de Comunicaciones**
- **Patrocinador ejecutivo (opcional para casos críticos)**

6.2 Responsabilidades del rol

Role	Responsabilidades
Gerente de incidentes	Coordina todos los esfuerzos de respuesta, asigna tareas y gestiona el seguimiento del estado.
Líder técnico	Analiza la causa raíz, aplica parches/correcciones y restaura sistemas.
Oficial de Cumplimiento	Garantiza la presentación de informes regulatorios (por ejemplo, GDPR) y documenta decisiones.
Comunicaciones Dirigir	Gestiona actualizaciones de las partes interesadas, mensajería externa y alertas de clientes.
Patrocinador ejecutivo	Aprueba decisiones de nivel de crisis y se comunica con el asesor legal si es necesario.

6.3 Disponibilidad y guardia

- **Alista de guardia rotatoria** Se mantiene para la disponibilidad del equipo de respuesta a incidentes.
- **Rutas de escalamiento y árboles de contacto** Se definen y prueban trimestralmente.

7. Protocolos de comunicación y escalamiento

Una comunicación clara y oportuna es esencial durante un incidente de seguridad para reducir la confusión, mantener la confianza de las partes interesadas y cumplir con las obligaciones legales.

7.1 Comunicación interna

- Todos los empleados están obligados a informar sobre actividades sospechosas o incidentes confirmados. **inmediatamente** a través de canales internos seguros (por ejemplo, alias de correo electrónico dedicado, chat encriptado).
- El **Actualizaciones de coordenadas del CSIRT** internamente durante incidentes en curso, utilizando plantillas de notificación predefinidas.
- Se emiten actualizaciones semanales para investigaciones de larga duración o fases de recuperación.

7.2 Procedimientos de escalamiento

- Los incidentes se escalan según **nivel de gravedad y alcance del impacto**:
 - **Medio o superior** debe ser reportado a la **Patrocinador ejecutivo** y Oficial de Cumplimiento.
 - **Incidentes críticos** desencadenar un **reunión de emergencia del CSIRT**, incluidos los altos directivos.
- Los árboles de escalamiento y los cronogramas de respuesta se documentan y ensayan trimestralmente.

7.3 Comunicación externa

● **El Líder de comunicaciones designado** es la única persona autorizada a:

- Notificar a los clientes sobre la interrupción del servicio o el posible impacto en los datos.
- Comunicarse con los reguladores (por ejemplo, **AEPD** en España, **Comisión Nacional de Informática y Libertades** en Francia).
- Responder consultas de prensa/medios.

● **Preaprobado plantillas de notificación** se utilizan para:

- Avisos de interrupción del servicio.
- Avisos de divulgación de infracciones.
- Notificaciones exigidas por el RGPD (en un plazo de 72 horas).

7.4 Confidencialidad e integridad de la mensajería

- Todas las comunicaciones relacionadas con incidentes se almacenan de forma segura.
- El cifrado se utiliza para:
 - Envío de informes a clientes.
 - Chat interno y correo electrónico si el contenido del incidente es confidencial.
- Toda la documentación está restringida al personal "que necesita conocer".

8. Actividades posteriores al incidente (lecciones aprendidas, análisis de causa raíz, documentación)

Después de cualquier incidente, especialmente uno calificado **Medio o superior**, la empresa lleva a cabo una estructura **revisión posterior al incidente (PIR)**.

8.1 Análisis de causa raíz (RCA)

- El RCA lo lleva a cabo el líder técnico y el gerente de incidentes.

- Se centra en identificar:
 - El punto de entrada inicial o la vulnerabilidad explotada.
 - Brechas en la detección o respuesta retrasada.
 - Contribuir a fallos de proceso o malas comunicaciones.
- Las conclusiones del RCA se documentan formalmente y se revisan con los equipos pertinentes.

8.2 Acciones correctivas y preventivas (CAPA)

- Todos los incidentes dan lugar a un plan CAPA que incluye:
 - Remediación inmediata de vulnerabilidades.
 - Mejoras del sistema o del proceso.
 - Actualizaciones de documentación o controles de seguridad.
 - Actualizaciones de capacitación interna, si hubo error humano.

8.3 Lecciones aprendidas

- Entre equipos **sesiones informativas** se llevan a cabo dentro de los 7 días siguientes a la resolución del incidente.
- Los hallazgos clave se comparten (de forma anónima si es necesario) con los empleados como material de concientización.
- Participación de RR.HH. y Legal si el incidente tiene implicaciones disciplinarias o contractuales.

8.4 Documentación

- Cada incidente se registra en el **sistema de registro de incidentes** con:
 - Cronología con marca de tiempo

- Partes involucradas
- Gravedad e impacto
- Resumen técnico y procedimental completo

- Los registros se revisan trimestralmente para identificar tendencias y amenazas recurrentes.

9. Revisión de políticas y mejora continua

Para seguir siendo eficaz y estar alineado con las amenazas y regulaciones emergentes, el Procedimiento de Respuesta a Incidentes de Seguridad es:

9.1 Revisado y actualizado anualmente

- El **Oficial de Seguridad de la Información** garantiza que el procedimiento esté actualizado:

- Después de incidentes importantes.
- En respuesta a los hallazgos de auditoría.
- Cuando haya cambios en la infraestructura, obligaciones legales o servicios.

9.2 Auditado y probado

- El procedimiento está sujeto a:

- Auditorías internas anuales**
- Pruebas de penetración** para validar las capacidades de detección y respuesta.
- Simulacros de ataques simulados (por ejemplo, simulación de phishing, simulación de ransomware).

9.3 Capacitado y aplicado

- Todos los empleados reciben capacitación obligatoria sobre:
 - Cómo reconocer y reportar incidentes de seguridad.
 - Qué esperar durante el proceso de respuesta a incidentes.
 - Se imparte formación especializada a:
 - Miembros del CSIRT
 - Equipos de DevOps
 - Gerentes de proyectos con entregas de clientes de alto riesgo
-

La seguridad es un objetivo en constante evolución. Nuestro proceso de respuesta evoluciona con cada incidente, cada lección y cada avance tecnológico.

Política de gestión de vulnerabilidades

1. Introducción y propósito

En **Live Now Technology SLU** reconocemos que las vulnerabilidades en el software, la infraestructura y las dependencias de terceros plantean un **riesgo crítico** a nuestras operaciones, la confianza de nuestros clientes y el cumplimiento normativo. Como empresa que desarrolla y gestiona sistemas digitales en entornos de alta integridad, incluyendo el procesamiento de datos de observación de la Tierra, software científico e ingeniería de sistemas, es nuestra responsabilidad mantener un **enfoque proactivo y disciplinado** a la gestión de vulnerabilidades.

Esta política establece un marco integral para:

- Identificar, evaluar, priorizar y mitigar las vulnerabilidades de seguridad en todos los sistemas y entornos.
- Mantener el cumplimiento de las mejores prácticas y estándares de seguridad como **ISO/IEC 27001, OWASP, NIST SP 800-40, y Guía de ENISA**.
- Minimizar la superficie de ataque y garantizar la integridad, disponibilidad y confidencialidad de los servicios.

El propósito de este documento es:

- Prevenir la explotación de vulnerabilidades conocidas en nuestros activos y bases de código.
- Mantener visibilidad en tiempo real de la exposición a fallas técnicas y lógicas.
- Promover un ciclo de vida de desarrollo y un proceso de parcheo seguros por diseño.
- Alinearse con las prácticas internas de gestión de riesgos, seguridad de la información y garantía de calidad.

2. Alcance y aplicabilidad

Esta política se aplica a:

- Todos los activos digitales propiedad de, operados o administrados por **Live Now Technology SLU**, incluido:

- Aplicaciones web, API, servicios backend y plataformas móviles.
- Sistemas internos (por ejemplo, correo, almacenamiento en la nube, herramientas de gestión de proyectos).
- Entornos de nube, pipelines de CI/CD, bases de datos y repositorios de código fuente.
- Servicios de terceros, bibliotecas e integraciones de proveedores.
- Todo el personal involucrado en:
 - Desarrollo de software
 - DevOps / administración de sistemas
 - Seguridad y cumplimiento
 - Gestión de proyectos y técnica
- Todas las etapas del ciclo de vida de los activos:
 - Diseño y desarrollo
 - Implementación y mantenimiento
 - Sistemas heredados y en desuso

La gestión de vulnerabilidades es necesaria en todos los ámbitos **entornos de producción, preparación y desarrollo**, e incluye ambos **código personalizado y dependencias de terceros**.

3. Objetivos del Programa de Gestión de Vulnerabilidad

Los objetivos principales de este programa son:

3.1 Identificar vulnerabilidades de forma proactiva

- Implementar herramientas automatizadas y manuales para detectar fallas de seguridad conocidas.
- Supervisar bases de datos de vulnerabilidades, fuentes de inteligencia sobre amenazas y avisos de proveedores (por ejemplo, CVE, NVD, avisos de GitHub, alertas específicas de proveedores).
- Integrar el escaneo en el ciclo de vida del SDLC y de la infraestructura.

3.2 Priorizar la remediación basada en riesgos

- Clasificar las vulnerabilidades en función de **Gravedad técnica, explotabilidad, impacto comercial y criticidad de los activos**.
- Centrar los esfuerzos en solucionar los problemas con **riesgo más alto** primero (por ejemplo, CVSS ≥ 7 , explotable de forma remota, que afecta a los servicios que prestan servicio al cliente).
- Realice un seguimiento del tiempo de exposición y asegúrese **resolución oportuna** contra SLA predefinidos.

3.3 Mantener el cumplimiento y la alineación con las mejores prácticas

- Garantizar el cumplimiento de los controles de seguridad requeridos en:
 - **ISO 27001 / Anexo A.12.6.1** (gestión de vulnerabilidades técnicas)
 - **NIS2, RGPD** (protección de datos)
 - **Obligaciones contractuales específicas del cliente**
- Esté preparado para **auditorías y evaluaciones externas** manteniendo registros detallados e informes de vulnerabilidad.

3.4 Fomentar la concienciación y la colaboración en materia de seguridad

- Educar a los desarrolladores, DevOps y las partes interesadas sobre la codificación segura, la higiene de las dependencias y las implicaciones de la vulnerabilidad.
- Fomentar una mentalidad de seguridad ante todo y la colaboración entre los equipos de seguridad y entrega.

4. Identificación de vulnerabilidades (fuentes y herramientas)

Las vulnerabilidades deben detectarse lo antes posible utilizando una combinación de **escaneo automatizado, revisión manual, y fuentes de inteligencia**.

4.1 Herramientas de escaneo y monitoreo

- **Pruebas de seguridad de aplicaciones estáticas (SAST):** Integrado en la canalización CI/CD para identificar problemas a nivel de código durante el desarrollo.
- **Pruebas dinámicas de seguridad de aplicaciones (DAST):** Escaneos periódicos de aplicaciones implementadas para identificar vulnerabilidades en tiempo de ejecución.
- **Escaneo de dependencias:** Herramientas como **auditoría de npm**, **auditoría de hilados**, **auditoría de pip**, o **Comprobación de dependencias de OWASP** para identificar paquetes vulnerables.
- **Escaneo de infraestructura:** Herramientas como **Sostenible**, **Cualidades**, o **OpenVAS** se utiliza en infraestructura de nube, contenedores y máquinas virtuales.
- **Gestión de la postura de seguridad en la nube (CSPM):** Herramientas de monitoreo (por ejemplo, AWS Security Hub, GCP Security Command Center) para detectar configuraciones incorrectas o exposición pública.

4.2 Fuentes de inteligencia externas

- Bases de datos públicas: **CVE**, **NVD**, **ExploitDB**, **Avisos de seguridad de GitHub**.
- Avisos específicos de proveedores (por ejemplo, de Microsoft, Atlassian, AWS, GitLab).
- CERT (por ejemplo, **INCIBE-CERT**, **ENISA**, **CERT-UE**).
- Participación en **grupos de inteligencia de amenazas específicos de la industria** donde se aplica.

4.3 Pruebas manuales de descubrimiento y penetración

- Programado **pruebas de penetración interna** **simulaciones de recompensas por errores**.
- Revisiones de código seguras durante los procesos de revisión por pares.
- Pruebas de penetración de terceros según lo requieran los clientes o auditorías.

5. Clasificación y priorización de riesgos

No todas las vulnerabilidades suponen el mismo riesgo. **Live Now Technology SLU** sigue un enfoque de priorización basado en riesgos utilizando una puntuación estándar de la industria y un análisis específico del contexto.

5.1 Clasificación de gravedad

La gravedad se determina inicialmente utilizando el **Sistema común de puntuación de vulnerabilidades (CVSS v3.x)**:

CVSS Puntaje	Gravedad Nivel
9.0 – 10.0	Crítico
7.0 – 8.9	Alto
4.0 – 6.9	Medio
0,1 – 3,9	Bajo

Factores contextuales adicionales considerados:

- **Explotabilidad**(PoC público, explotación activa en la naturaleza)
- **Sensibilidad de los datos**(PII, activos del cliente)
- **criticidad empresarial**del sistema afectado
- **Exposición en red**(público vs interno)

5.2 Acuerdos de nivel de servicio (SLA) de remediación

Gravedad y	Es hora de Remediar
Crítico	≤ 24 horas
Alto	≤ 5 días hábiles
Medio	≤ 30 días
Bajo	Como recursos permiso

Las desviaciones de estos plazos requieren **aceptación formal del riesgo** por el Oficial de Seguridad de la Información.

6. Proceso de remediación y mitigación

6.1 Flujo de trabajo de remediación

1. **Detección:** La vulnerabilidad se identifica mediante un escaneo automático o una entrada manual.
2. **Verificación:** El líder técnico o analista de seguridad confirma que el hallazgo es válido y no es un falso positivo.
3. **Priorización:** La severidad y el impacto se evalúan utilizando una matriz de clasificación de riesgos.
4. **Venta de entradas:** El problema se registra en el rastreador de problemas de la empresa con metadatos (CVSS, CWE, sistema afectado).
5. **Asignación:** Al propietario/equipo responsable se le asigna un SLA y una fecha límite.
6. **Remediación:** Se implementa un parche, un cambio de configuración o una corrección de código.
7. **Pruebas:** El cambio se prueba en un entorno seguro.
8. **Cierre:** El problema se marca como resuelto y se conservan los registros.

6.2 Estrategias de mitigación

Si no es posible una remediación inmediata:

- **Segmentación de red o restricción de acceso** se hace cumplir.
- **Firewall de aplicaciones web (WAF)** Las reglas se actualizan para bloquear la explotación.
- **Alertas de monitoreo** Están configurados para detectar intentos de abuso.
- **Comunicación con las partes interesadas** Se emite si la exposición está orientada al cliente.

6.3 Seguimiento y documentación

- Todas las vulnerabilidades se rastrean en un sistema central. **Registro de vulnerabilidades** con:
 - Fecha de detección, estado de remediación, equipo responsable, riesgo residual.
- Los KPI (por ejemplo, tiempo promedio de remediación, tasa de cumplimiento del SLA) se revisan mensualmente.

7. Gestión de parches y dependencias de terceros

Mantener componentes de software, sistemas y bibliotecas de terceros **A hoyes** un pilar fundamental de la estrategia de gestión de vulnerabilidades.

7.1 Proceso de gestión de parches

- **Los parches se aplican según la gravedad y la criticidad.**, de acuerdo con los SLA definidos en la Sección 5.
- **Todos sistemas de producción** están incluidos en el programa de parcheo.
- Los cambios se prueban en **entornos de puesta en escena** antes de implementarlo en producción para evitar regresiones.
- Existen protocolos de parcheo de emergencia para **vulnerabilidades de día cero** (por ejemplo, Log4Shell, Heartbleed).
- Se mantienen ventanas de parches mensuales para actualizaciones estándar en toda la infraestructura interna.

7.2 Software de terceros y dependencias

- Los proyectos de software deben utilizar **herramientas de gestión de dependencias** (por ejemplo, npm, pip, Maven) con controles de seguridad automatizados.
- Las actualizaciones periódicas de bibliotecas de terceros se implementan a través de canales de CI.
- Todas las bibliotecas externas deben tener:

- Versiones claras y registros de cambios.
- Licencias revisadas por el equipo legal o de cumplimiento (cuando corresponda).
- Avisos de seguridad monitoreados activamente.

7.3 Software sin soporte y al final de su vida útil

- Los sistemas o paquetes que ya no reciben soporte del proveedor deben:
 - Desmantelado** reemplazado.
 - Aislado** en entornos segmentados.
 - Sujeto a seguimiento adicional y controles compensatorios.

8. Monitoreo, Métricas y Mejora Continua

Para garantizar la eficacia del programa de gestión de vulnerabilidades, **Live Now Technology SLU** realiza un seguimiento de los indicadores clave y realiza revisiones continuas del proceso.

8.1 Indicadores clave de rendimiento (KPI)

- Número de vulnerabilidades detectadas (por categoría/gravedad).
- Tiempo medio de remediación (MTTR).
- Tasa de cumplimiento del SLA por gravedad.
- Porcentaje de activos escaneados periódicamente.
- Frecuencia de actualización de dependencias en proyectos activos.

8.2 Herramientas de monitoreo y paneles de control

- Los paneles centralizados (por ejemplo, a través de Jira, GitHub o monitoreo personalizado) rastrean los flujos de trabajo de remediación.
- Se configuran alertas para artículos vencidos o problemas críticos no resueltos.
- Los informes semanales o mensuales son revisados por el **Líderes de seguridad e ingeniería**.

8.3 Mejora continua

- Las lecciones aprendidas de los incidentes de seguridad se incorporan a:
 - Procesos de desarrollo (por ejemplo, prácticas de codificación segura).
 - Revisiones de infraestructura (por ejemplo, ajuste de IAM, reglas de firewall).
 - Tuberías de CI/CD (por ejemplo, verificaciones mejoradas o automatización).
- Los ajustes del proceso se realizan después de:
 - El nuevo panorama de amenazas cambia.
 - Tendencias de explotación de vulnerabilidades.
 - Cambios regulatorios o contractuales.

9. Roles, responsabilidades y gobernanza

9.1 Responsable de seguridad/CISO (o funcionario designado)

- Supervisa todo el programa de gestión de vulnerabilidades.
- Aprueba las justificaciones de aceptación de riesgos y realiza el seguimiento de los riesgos residuales.
- Lidera la selección e implementación de herramientas de escaneo.
- Reporta periódicamente a la dirección ejecutiva.

9.2 Equipos de DevOps e ingeniería

- Implementar parches, cambios de configuración y acciones de mitigación.
- Integrar el escaneo de seguridad en el ciclo de vida del desarrollo de software (SDLC).
- Mantenga los archivos de dependencia actualizados y evite versiones obsoletas.

9.3 Gerentes de proyecto y propietarios de productos

- Priorizar el trabajo de remediación durante los sprints o ciclos de mantenimiento.
- Comunicar a los clientes si sus entornos o entregables se ven afectados.
- Alinear los esfuerzos de remediación con las obligaciones contractuales o regulatorias.

9.4 Todos los empleados

- Manténgase informado sobre las mejores prácticas de higiene y seguridad.
- Informar de inmediato sobre comportamientos inusuales o vulnerabilidades sospechosas.
- Evite el uso de paquetes de software no aprobados u obsoletos.

9.5 Auditorías y revisiones

- Las auditorías internas anuales evalúan la adherencia al proceso.
- Se revisa la política **al menos una vez al año**, o después de cualquier incidente importante o evento de vulnerabilidad.
- Los resultados se comunican al equipo de gestión y se incluyen en la documentación de cumplimiento.

“La gestión de vulnerabilidades es una responsabilidad compartida: todos en la organización contribuyen a un entorno seguro y confiable”.

Canal de comunicación interna de empleados

1. Propósito y compromiso

Live Now Technology SLU se compromete a mantener una cultura en el lugar de trabajo basada en **transparencia, ética y rendición de cuentas** Para apoyar esto, ofrecemos un **mecanismo de denuncia interna y confidencial** para empleados, contratistas y colaboradores **denunciar mala conducta, violaciones de políticas o riesgos** de forma anónima o abierta.

Hacemos cumplir estrictamente una **política de no represalias** para todos los informes de buena fe.

2. Alcance de los problemas notificables

Este mecanismo cubre, pero no se limita a:

- Mala conducta ética (por ejemplo, discriminación, acoso, conflicto de intereses)
- Irregularidades financieras (por ejemplo, fraude, corrupción, malversación de fondos)
- Infracciones de seguridad, protección de datos o políticas de la empresa
- Violaciones de leyes, contratos u obligaciones regulatorias

3. Cómo denunciar

Los empleados, colaboradores y socios externos pueden reportar incidentes o inquietudes utilizando el sitio web de la empresa **canal de denuncia interna designado**, diseñado para garantizar **confidencialidad, accesibilidad y cumplimiento** con las leyes de denuncia de irregularidades de la UE y de España.

3.1 Métodos de presentación de informes:

- **Formulario seguro en línea** Accesible desde la intranet o el portal interno, disponible 24/7. Permite envíos tanto identificados como anónimos.
- **Dirección de correo electrónico dedicada:** (p.ej, informe@livenowtech.com) configurado con acceso restringido y cifrado.
- **Contacto telefónico opcional:** Para asuntos sensibles o urgentes, también se puede proporcionar un sistema de correo de voz seguro.
- **Informes escritos:** Puede presentarse directamente al Oficial de Cumplimiento en un sobre sellado marcado como "Confidencial – Informe de Ética".

3.2 El contenido del informe debe incluir (si se conoce o corresponde):

- Una descripción clara del evento, problema o mala conducta.
- Fecha y lugar de ocurrencia.
- Partes involucradas o afectadas.
- Cualquier evidencia o documento de respaldo.
- Información de contacto (opcional, si no se solicita el anonimato).

No se requieren datos personales para denuncias anónimas. El sistema no recopilará direcciones IP ni otros metadatos identificables.

4. Manejo y seguimiento

Una vez enviado un informe, **Live Now Technology SLU** sigue un proceso de investigación estandarizado y compatible para garantizar la imparcialidad y la confidencialidad.

4.1 Recepción y registro de informes

- Todos los informes son recibidos por el **Oficial de Ética y Cumplimiento** o una persona específicamente designada (no involucrada en los hechos).

- Cada informe se registra con una identificación única y se marca con tiempo en un registro seguro (digital o físico).

4.2 Evaluación inicial

- **Dentro 7 días naturales** Se realiza un triaje inicial para:
 - Confirmar la recepción al denunciante (si está identificado).
 - Determinar si el informe cae dentro del alcance de la política.
 - Decidir si se requieren acciones inmediatas (por ejemplo, prevenir más daños).

4.3. Proceso de investigación

- Si es admisible, se inicia una investigación interna confidencial.
- El proceso incluye entrevistas de investigación, revisión de documentación y consulta con expertos cuando sea necesario.
- Las investigaciones concluyen dentro de **un máximo de 90 días**, ampliable en casos complejos (según Directiva UE).

4.4 Comunicación de seguimiento

- Si el denunciante ha proporcionado información de contacto, recibirá actualizaciones:
 - Confirmación de recepción.
 - Avance general (sin revelar detalles sensibles o legales).
 - Resultado final o estado de resolución.

5. Protección y confidencialidad

Nos aseguramos de un **entorno seguro para hablar**. Nadie será penalizado ni discriminado por realizar un informe de buena fe.

5.1 Garantía de no represalias

- Queda estrictamente prohibida la represalia (por ejemplo, despido, degradación, acoso) contra cualquier persona que presente un informe de buena fe.
- La represalia confirmada tendrá como resultado **acciones disciplinarias hasta el despido**.

5.2 Protección de denuncias anónimas

- Los informes anónimos se aceptan y procesan por igual.
- El sistema de informes está configurado para **no registra metadatos, direcciones IP ni detalles del usuario**.
- Los remitentes anónimos pueden usar códigos de seguimiento para verificar el estado de su caso (si el sistema lo permite).

5.3 Medidas de confidencialidad

- Toda la información se maneja bajo **estricta confidencialidad**.
- Sólo el personal autorizado involucrado directamente en la investigación tiene acceso al informe.
- Las divulgaciones se limitan a lo que es legalmente requerido o necesario para la resolución.

“Plantear inquietudes fortalece nuestra organización, y quienes lo hacen merecen protección absoluta”.