POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE SOLUCIONES INFORMÁTICAS EXTRANET, S.L.

Para el cumplimiento de la presente Política de Seguridad y Privacidad de la Información de **Soluciones Informáticas Extranet, S.L.** (en adelante, **EXTRANET**) dispone de un sistema de gestión de seguridad y privacidad de la información (en adelante, **SGSPI**), de conformidad con estándares internacionales, que da cobertura a los requisitos necesarios para garantizar la confidencialidad, la integridad, la autenticidad y la trazabilidad de la información, así como de la disponibilidad de los servicios que se prestan a los clientes.

Para la eficacia y eficiencia del sistema de gestión de seguridad de la información, la Dirección de **EXTRANET** ha tomado las decisiones siguientes:

1. Adoptar los estándares ISO/IEC 27001 y 27701 como marco normativo del SGSPI.
2. Asignar los recursos humanos y materiales para el desarrollo del ciclo de vida del SGSPI.
3. Designar un responsable de seguridad de la información, con la autoridad delegada para el desarrollo, mantenimiento y mejora del SGSPI.
4. Establecer la organización, con una definición clara de roles y responsabilidades, para la gestión de seguridad y privacidad de la información.
5. Planificar la formación y concienciación del personal para saber actuar preventivamente y reaccionar, en su caso, ante las amenazas a la seguridad y privacidad de la información.
6. Analizar los riesgos a la seguridad y privacidad de la información como proceso esencial para prevenir los incidentes de seguridad y privacidad de la información.
7. Cumplir proactivamente los requisitos legales, normativos y reglamentarios aplicables.
8. Medir y analizar los indicadores que permitan a la Dirección el seguimiento de los objetivos de seguridad y privacidad.

9. Monitorizar, revisar y auditar regularmente el SGSPI.

En consecuencia, con lo anterior, la Dirección de **EXTRANET** ha establecido las políticas que, a continuación, se resumen.

1. La seguridad de la información es responsabilidad de todos

La Dirección supervisará las medidas de seguridad y privacidad de la información, siendo su observancia responsabilidad de todo el personal y colaboradores.

La Dirección aportará los medios necesarios y proporcionales, de acuerdo con un modelo de mejora continua, con especial énfasis en la formación de los recursos humanos, así como el control y análisis de los resultados para verificar la eficiencia y eficacia de las medidas.

2. La gestión proactiva de ciberriesgos

Para gestionar los riesgos derivados de las amenazas a los activos de información se seguirán las siguientes medidas:

- La asignación de los recursos especializados necesarios para la realización del análisis de riesgos.
- Registrar los análisis de riesgo realizados y someter la aceptación del nivel de riesgo residual a la aprobación de la Dirección General.
- Establecer un valor objetivo de puntuación media máxima, identificándose asimismo un valor inadmisible de riesgo y un rango como intervalo tolerable.
- El Responsable de Seguridad de la Información de **EXTRANET** actualizará el análisis de riesgos con periodicidad máxima anual o, bien, cuando ocurra un incidente relevante, estableciendo las medidas para su debido tratamiento.

3. Protección de los dispositivos, los aplicativos y las comunicaciones.

Para garantizar el uso aceptable de los dispositivos y aplicativos, que **EXTRANET** pone a disposición de los usuarios de su sistema de información se seguirán las siguientes medidas:

- Los dispositivos son propiedad de **EXTRANET** puestos a disposición de los usuarios únicamente para su desempeño laboral.

- La instalación y uso de cualquier aplicativo, programa software o contenido digital, ajeno a los instalados o autorizados, está terminantemente prohibido. Tampoco se admitirán modificaciones a los elementos del hardware de los dispositivos de **EXTRANET** salvo aquellas que sean realizadas por el responsable de sistemas de **EXTRANET**.
- Todos los aplicativos o programas software instalados en los dispositivos de **EXTRANET** deberán cumplir con el modelo de licenciamiento de sus fabricantes.

4. Control del acceso físico

Para garantizar el debido acceso a oficinas e instalaciones de **EXTRANET**, se siguieron las siguientes medidas:

- La entrada y salida a las oficinas e instalaciones de personas no pertenecientes a la organización serán autorizadas por un responsable y registradas en la recepción.
- Las personas autorizadas no pertenecientes a la organización que accedan a las zonas donde se ubiquen dispositivos y/o equipos de comunicaciones estarán supervisadas por un responsable.

5. Protección de infraestructuras e instalaciones

Para garantizar la protección de infraestructuras e instalaciones de **EXTRANET** se seguirán las siguientes medidas:

- El suministro eléctrico a los sistemas de información críticos en caso de fallo del suministro general.
- La instalación de medios de detección y extinción de incendios.
- La instalación de medios de detección de intrusiones.
- La protección, mediante canalizaciones, de incidentes fortuitos o deliberados, del cableado principal de redes de datos y voz, considerando como principal aquel que provee de comunicaciones a la oficina de **EXTRANET** con el exterior.
- La existencia de instalaciones alternativas para la continuidad de las operaciones en caso de que las instalaciones habituales no estén disponibles.

6. Control de acceso de los usuarios.

Para garantizar el debido acceso a los dispositivos o programas software de **EXTRANET** se seguirán las siguientes medidas:

- A todo usuario se le asignará un nombre de usuario único y una contraseña, que tendrán carácter estrictamente personal e intransferibles, otorgada en función de sus necesidades y autorización de acceso a la información.
- Las contraseñas iniciales serán configuradas por **EXTRANET**.
- Las contraseñas tendrán una caducidad no superior a 45 días, tendrán una longitud mínima de 8 caracteres y cumplir requisitos de complejidad conforme a la política de seguridad de contraseñas de **EXTRANET**.
- Los nombres de usuarios y contraseñas serán cambiadas o eliminadas cuando se produzca un cambio de funciones o baja, respectivamente o bien un incidente que haya comprometido su confidencialidad.

7. Control del uso de Internet.

Para garantizar el acceso y uso aceptable de Internet por los usuarios se seguirán las siguientes medidas:

- El acceso y navegación por Internet de los usuarios podrá estar monitorizado con fines de garantizar la seguridad de la información y los equipos de los usuarios.
- La utilización de Internet, como herramienta de trabajo útil, se ajustará a las necesidades del desempeño laboral de cada usuario.
- El acceso de los usuarios a páginas inseguras o inapropiadas de Internet está prohibido de acuerdo con las prácticas reconocidas de buen uso y/o de conformidad con la legislación vigente.

8. Protección del correo electrónico.

Para garantizar el uso aceptable del correo electrónico por los usuarios, se seguirán las siguientes medidas:

- Las cuentas de correo electrónico asignadas a los usuarios para el desempeño de sus actividades profesionales son propiedad de **EXTRANET**.
- Los contenidos de los correos electrónicos serán confidenciales ajustándose al ordenamiento legal.
- A todos los usuarios de las cuentas de correo electrónico se les asigna una dirección electrónica única y una contraseña, de carácter estrictamente personal e intransferible.

- Las contraseñas iniciales serán configuradas por **EXTRANET**.
- Las contraseñas de los usuarios se renovarán cada 180 días.
- Las contraseñas de los usuarios con permisos de administración se renovarán cada 90 días.

9. Filtrado de contenidos dañinos.

Para garantizar la identificación, bloqueo y eliminación de contenidos dañinos, se seguirán las siguientes medidas:

- La instalación en los dispositivos de los usuarios de una aplicación antivirus
- La prohibición de desactivación de los programas antivirus por parte de los usuarios.
- Reiniciar siempre el dispositivo para finalizar la instalación de las actualizaciones.

10. Protección de los sistemas operativos y otras utilidades.

Para garantizar la eliminación de vulnerabilidades en los sistemas operativos y otras utilidades instaladas en los dispositivos de los usuarios, se seguirán las siguientes medidas:

- La prohibición de desactivar las herramientas de actualización automática del sistema operativo.
- La recomendación a los usuarios es reiniciar el dispositivo para finalizar la instalación de las actualizaciones siempre que así lo requiera la herramienta de actualización.

11. Protección de los dispositivos personales.

Para garantizar el uso aceptable de los dispositivos personales de los usuarios (BYOD) se seguirán las siguientes medidas:

- La autorización de los usuarios y dispositivos (teléfonos inteligentes, tabletas) para el uso de los servicios de correo electrónico, de conectividad a Internet y de los aplicativos de negocio.
- La instalación en los dispositivos personales de los usuarios de antivirus y antispam.
- La actualización del software del sistema operativo y otras utilidades del sistema de los dispositivos personales de los usuarios.
- La disposición en los dispositivos personales de los usuarios de clave o pin de acceso.

- Los aplicativos o programas software instalados en los dispositivos personales de los usuarios autorizados deberán contar con las licencias de uso y/o mantenimiento de sus fabricantes.
- La suscripción de un compromiso de uso aceptable por parte de los usuarios de los dispositivos personales autorizados para el acceso y uso de los servicios de correo electrónico, de conectividad a Internet y de los aplicativos de negocio.

12. Protección del teletrabajo o movilidad.

Para garantizar la seguridad en situaciones de movilidad y/o teletrabajo se seguirán las siguientes medidas:

- La autorización de los usuarios y dispositivos en situaciones de movilidad y/o teletrabajo para el uso de los servicios de correo electrónico, de conectividad a Internet y/o de los aplicativos de negocio.
- La instalación en los dispositivos de los usuarios autorizados para situaciones de movilidad y/o teletrabajo, y que requieran de conectividad con la oficina, del aplicativo para acceso remoto seguro (VPN) proporcionado por **EXTRANET**. No está permitido el uso de otros aplicativos de acceso seguro remoto.
- La utilización de un nombre de usuario y un certificado de usuario personal seguros para la identificación de los usuarios del aplicativo para acceso remoto seguro (VPN).
- La revisión de los usuarios con acceso a la VPN y la revocación de los usuarios que no deban hacer uso del aplicativo de acceso remoto seguro cada 90 días.
- La actualización puntual del software del aplicativo para el acceso remoto seguro (VPN) proporcionado por **EXTRANET**
- La habilitación de la protección de dispositivo desatendido mediante su bloqueo por inactividad conforme a la política establecida en el dominio.
- La recomendación de uso de candado de anclaje cuando el usuario desempeñe su actividad en una instalación pública o ajena a las oficinas de **EXTRANET** o su domicilio de teletrabajo.
- La suscripción de un compromiso de uso aceptable por parte de los usuarios de los dispositivos autorizados para el acceso remoto seguro en movilidad y/o teletrabajo.

13. Protección de las comunicaciones.

Para garantizar la eliminación de vulnerabilidades en los servidores y equipos de electrónica de red (routers, switches, puntos de acceso, proxis) se seguirán las siguientes medidas:

- La actualización puntual del software de servidores y firmware de los equipos de la electrónica de red.
- La segregación lógica de las redes no esenciales para la prestación del servicio a los clientes (redes wifi de invitados, de unidades de apoyo a negocio, etc.).
- La monitorización periódica de servidores y equipos de electrónica de red.

14. Protección de la información

Para evitar la pérdida, robo o transferencia no autorizada de la información clasificada o propiedad intelectual de **EXTRANET** se seguirán las siguientes medidas:

- La identificación y clasificación de toda la información, en cualquier soporte, considerada de especial protección (confidencial de negocio, datos personales de categoría especial).
- La monitorización de los controles para el acceso, manejo, transmisión y reproducción de dicha información.
- El seguimiento por los usuarios de la buena práctica de puesto de trabajo despejado de documentación.
- La implementación, mediante una política del dominio corporativo, del bloqueo de pantalla mediante contraseña cuando el equipo esté desatendido o no esté en uso.

15. Copias de seguridad.

Para garantizar la recuperación de los datos esenciales, en caso de pérdida, secuestro o destrucción se seguirán las siguientes medidas:

- La información de los usuarios deberá consolidarse de manera periódica sobre elementos o aplicaciones que garanticen la seguridad y disponibilidad de la información:
    - Código desarrollado sobre el repositorio de código GIT corporativo o facilitado por el cliente
    - Documentación sobre una unidad de almacenamiento en la nube corporativa o facilitada por el cliente (Drive, Teams, Dropbox, …).

- Se realizarán copias de seguridad periódicas en la nube de los datos contenidos en las aplicaciones internas que lo requieran o sean exigibles a nivel legal.
- Las copias de seguridad serán probadas regularmente para asegurar su recuperación.

16. Continuidad de las operaciones.

Para reducir las consecuencias de un incidente (suplantación de identidad, robo o secuestro de información, denegación de servicios, brecha de datos personales, accidente, catástrofe, atentado o sabotaje) se seguirán las siguientes medidas:

- La documentación y actualización de un plan de contingencia y recuperación de las operaciones de negocio.
- La realización de pruebas del plan de contingencia y recuperación de las operaciones de negocio.
- La difusión y entrenamiento en las medidas del plan de contingencia y recuperación de las operaciones de negocio entre el personal y los colaboradores.

17. Cumplimiento legal.

Para prevenir proactivamente y evitar los potenciales perjuicios reputacionales y/o económicos derivados de incumplimientos de la normativa legal, se seguirán las siguientes medidas:

- El registro y actualización regular de los requisitos legales o contractuales en materia de seguridad y privacidad de la información y comunicaciones.
- La implantación y supervisión de controles de cumplimiento normativo, con especial incidencia, aquellos derivados de la legislación vigente de protección de datos personales, propiedad intelectual, transmisión de telecomunicaciones, etc.
- La realización de una auditoría regular del cumplimiento normativo en materia de protección de datos personales para verificar y poner a disposición, de reguladores y autoridades, de las evidencias de cumplimiento, así como para detectar potenciales incumplimientos y proceder a la realización de las necesarias acciones correctivas y preventivas, en su caso.

18. Gestión de incidentes.

Para garantizar la contención, mitigación y recuperación ante eventos desfavorables que puedan afectar a la seguridad y privacidad de la información y/o la disponibilidad de los servicios, se seguirán las siguientes medidas:

- La comunicación puntual de cualquier usuario de un evento sospechoso, (pérdida de control de los dispositivos o aplicativos, desconexión súbita del sistema, recepción de un correo electrónico, SMS y/o llamada sospechosa, presencia de personas desconocidas no autorizadas en las oficinas o dependencias, etc.)
- La comunicación se realizará por correo electrónico (seguridad@solucionesextranet.com), comunicación telefónica o WhatsApp, cuando se estime urgente.
- El registro, evaluación y notificación a los afectados y/o a las Autoridades Reguladoras nacionales (AEPD, INCIBE) e internacionales, en su caso.
- La convocatoria de la Dirección de **EXTRANET,** cuando el incidente se estime pueda ser de elevada peligrosidad y/o impacto.
- El seguimiento y remediación del incidente hasta su resolución.
- La documentación y el análisis de causa raíz del incidente, con la propuesta de acciones de corrección y/o de prevención.
- La denuncia del incidente ante las Fuerzas y Cuerpos de Seguridad del Estado (Policía, Guardia Civil) si se observa la posible comisión de un delito y/o el incidente sea de elevada peligrosidad y/o impacto o bien cuando se produzca o sea previsible la reclamación por parte de clientes o la apertura de expediente por Autoridades Reguladoras.

19. Mejora continua.

Para garantizar la vigencia y mejora de la gestión de la seguridad y privacidad de la información, se seguirán las siguientes medidas:

- Promover la propuesta de cualquier sugerencia, medida o acción de mejora, por parte de los usuarios.
- El registro de cualquier sugerencia, medida o acción de mejora, por parte de los usuarios y su debida evaluación y seguimiento, desde su aceptación hasta su implantación.
- La evaluación objetiva de todas las mejoras propuestas y la implantación de las aceptadas por la Dirección.

- El reconocimiento público y la compensación, en su caso, de los usuarios y las propuestas de elevado impacto.

20. Actualización, distribución y aceptación

La Política de Seguridad y Privacidad será revisada con regularidad anual o, bien, siempre cuando se produzca un cambio significativo, para asegurar su vigencia, idoneidad, adecuación y eficacia.

Los cambios a la Política de Seguridad de la Información serán aprobados por la Dirección de **EXTRANET** y distribuidos puntualmente a todo el personal, los clientes, los colaboradores y otras partes interesadas.

La Política de Seguridad y Privacidad de la Información y sus cambios será distribuida a todo el personal y colaboradores de **EXTRANET** para su aceptación.