

Política de Seguridad de la Información

Seguridad, calidad, continuidad y privacidad como pilares de confianza

Up Spain está comprometida con la prestación de servicios de calidad y con la protección responsable de la información que gestiona. La confianza de clientes, beneficiarios, usuarios, Administraciones Públicas, proveedores y demás partes interesadas depende de nuestra capacidad para prestar servicios fiables, preservar la información y responder de forma adecuada ante los cambios, los riesgos y los incidentes.

La Dirección establece y mantiene esta Política como marco de referencia del Sistema de Gestión Integrado. Su contenido se alinea con los principios de ISO 9001 e ISO/IEC 27001 y, para los sistemas incluidos en el alcance correspondiente, con los requisitos del Esquema Nacional de Seguridad en categoría MEDIA. En ese ámbito se incluyen UpOne y GourmetPay/Orders, junto con las dependencias que les prestan soporte directo, sin revelar en esta versión pública configuraciones ni información técnica sensible.

Un compromiso que se traduce en decisiones

La seguridad se integra en la estrategia, los procesos, los proyectos y la relación con terceros. Cada medida se aplica de forma proporcionada al riesgo, se asigna a responsables identificados y se revisa mediante evidencias, indicadores, pruebas y auditorías.

1. Integración estratégica y liderazgo

La Dirección integra la seguridad de la información y la calidad en los objetivos y procesos de negocio, asignando los recursos necesarios y promoviendo una cultura de responsabilidad. Las funciones de gobierno, seguridad, operación, servicio, información y privacidad se definen de forma clara, favoreciendo la diferenciación de responsabilidades, la supervisión independiente y la toma de decisiones basada en información fiable.

2. Conocimiento del contexto y de las partes interesadas

Up Spain analiza su contexto interno y externo y considera las necesidades de clientes, usuarios, personal, Administraciones, proveedores, autoridades y otras partes relevantes. Los requisitos legales, reglamentarios, contractuales y de negocio, así como los cambios tecnológicos, organizativos, sociales o ambientales que puedan afectar a los servicios, se incorporan a la planificación, a la gestión de riesgos y a la mejora del sistema.

3. Protección integral de la información

La información se protege frente a amenazas internas y externas, deliberadas o accidentales, mediante controles técnicos, organizativos, físicos y contractuales. La protección busca preservar la confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad y conservación, aplicando líneas de defensa, seguridad desde el diseño y por defecto, prevención, detección, respuesta y recuperación a lo largo de todo el ciclo de vida.

4. Gestión de activos y clasificación

La organización mantiene inventarios de información, servicios, aplicaciones, infraestructuras, dispositivos, proveedores y dependencias relevantes, asignando propietarios y criterios de clasificación. Los accesos, configuraciones, cambios, traslados, conservación y retirada de los activos se gestionan de acuerdo con su criticidad y sensibilidad, bajo los principios de necesidad de conocer y mínimo privilegio.

5. Continuidad, resiliencia y recuperación

Up Spain desarrolla planes de continuidad y recuperación orientados a mantener o restablecer los servicios prioritarios ante fallos, incidentes, indisponibilidades o desastres. Las dependencias críticas, los objetivos de recuperación, las copias de seguridad, los procedimientos alternativos y la capacidad de respuesta se revisan y prueban periódicamente, incorporando las lecciones obtenidas y coordinando a los proveedores que participan en la prestación.

6. Gestión de riesgos y cadena de suministro

La seguridad se gestiona mediante un proceso sistemático de identificación, análisis, evaluación, tratamiento y seguimiento de riesgos. Este proceso se aplica a los sistemas, proyectos, cambios, servicios externalizados y relaciones de suministro, de forma que las medidas sean proporcionales y verificables. Los riesgos residuales que excedan los niveles aceptables son elevados a los responsables competentes para su decisión, condiciones de aceptación y seguimiento.

7. Gestión de incidentes y aprendizaje

Se mantienen mecanismos para comunicar, detectar, registrar, analizar, contener, erradicar y recuperar los servicios ante incidentes de seguridad. La respuesta protege a las personas y a la organización, preserva las evidencias necesarias y coordina las comunicaciones con clientes, proveedores, autoridades y otras partes cuando

corresponda. Cada incidente relevante se revisa para identificar causas, acciones correctivas y oportunidades de aprendizaje.

8. Protección de datos personales y privacidad

Los datos personales se tratan de forma lícita, leal, transparente y segura, respetando los principios de minimización, limitación de la finalidad, exactitud, conservación y responsabilidad proactiva. La privacidad se considera desde el diseño y por defecto, con participación del Delegado de Protección de Datos cuando proceda, evaluación de riesgos para los derechos de las personas y procedimientos para atender derechos, incidentes y obligaciones de comunicación.

9. Protección de información sensible y servicios digitales

La información financiera, transaccional, contractual, comercial o confidencial recibe medidas reforzadas de protección. Estas medidas pueden incluir cifrado, autenticación robusta, segregación de redes y funciones, desarrollo y cambios seguros, control de accesos, registros de actividad, monitorización y protección de las comunicaciones. Las integraciones con terceros y los medios de pago se someten a requisitos de seguridad, responsabilidades compartidas y controles proporcionales al riesgo.

Seguridad en todo el ciclo de vida

Los nuevos servicios, aplicaciones, integraciones y cambios deben incorporar requisitos de seguridad y privacidad desde su concepción, pasar controles de autorización y prueba, mantener trazabilidad y disponer de mecanismos de reversión y mejora.

10. Formación y concienciación

La seguridad depende también de las personas. Up Spain promueve la formación y concienciación continua del personal y de los colaboradores externos, desde su incorporación y durante el desempeño de sus funciones. La capacitación se adapta a los riesgos y responsabilidades de cada colectivo e incluye buenas prácticas de uso, prevención del fraude y del phishing, protección de credenciales, trabajo remoto seguro, gestión de incidentes, desarrollo seguro y administración de sistemas.

11. Seguimiento, cumplimiento y mejora continua

La eficacia del sistema se evalúa mediante objetivos, indicadores, revisiones, pruebas, seguimiento de controles y auditorías internas o externas. Los incumplimientos,

desviaciones y no conformidades se registran, analizan y corrigen, verificando la eficacia de las acciones adoptadas. La Dirección revisa periódicamente el sistema y actualiza esta Política cuando cambian el contexto, la normativa, los riesgos, la tecnología, los servicios, los proveedores o las expectativas de las partes interesadas.

Aplicación y comunicación

Esta Política es de obligado cumplimiento para todas las personas de Up Spain y para los colaboradores externos en el ámbito de sus funciones, contratos y accesos. Sus principios se desarrollan mediante normas, procedimientos, instrucciones y controles operativos, disponibles en los canales corporativos que correspondan. Las dudas, incidentes o posibles incumplimientos deben comunicarse a través de los mecanismos internos habilitados.

La versión pública resume los compromisos de la Dirección y facilita su comunicación a clientes, usuarios, proveedores y otras partes interesadas. La Política interna controlada, sus documentos de desarrollo y las evidencias asociadas prevalecen ante cualquier discrepancia y contienen el detalle de gobierno, alcance, responsabilidades y controles.

Declaración de la Dirección

Up Spain asume la seguridad de la información como una responsabilidad permanente y compartida. Nuestro objetivo es proteger la confianza depositada en la organización, asegurar la calidad y continuidad de los servicios y mejorar de forma constante nuestra capacidad para prevenir, responder y recuperarnos ante los riesgos.