POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN (REV. 00)

El ámbito de aplicación de este documento aplica a todas las actividades llevadas a cabo por **FOMENTO DE TÉCNICAS EXTREMEÑAS S.L.,** en adelante FOTEX, así como las correspondientes empresas proveedoras, para el desarrollo de aplicaciones informáticas.

Todo el personal vinculado con la organización que tenga que utilizar los sistemas de información o disponga de acceso a los recursos informáticos en general de FOTEX, debe tener conocimiento y comprometerse formalmente a acatar esta Política de Seguridad.

Es obligación de las empresas proveedoras poner en conocimiento de su personal la presente política de Seguridad de la Información. Para ello, los contratos o pedidos que se formalicen entre FOTEX y las empresas proveedoras de servicios, recogerán de forma explícita que son conocedores de esta política y se comprometen a respetarla, así como que asumen las responsabilidades en las que pueden incurrir en caso de no cumplirlas.

La dirección de FOTEX, como política general de la empresa, garantiza la adecuada gestión de la seguridad de la información procesada y/o albergada por los sistemas y servicios contemplados en el alcance. Para desarrollar esta política, la dirección de FOTEX se compromete a:

- ✓ Llevar a cabo un análisis de riesgos periódico que permita mantener una adecuada visión de los riesgos de seguridad de la información a los que están expuestos los activos de la empresa y a desarrollar las medidas necesarias para limitar y reducir dichos riesgos, definiendo así mismo las medidas de seguridad a establecer.
- ✓ Desarrollar una completa normativa de seguridad que regule las condiciones en las que la empresa, dentro de su alcance, debe desarrollar su actividad para respetar los requerimientos de seguridad establecidos.

- ✓ Destinar los recursos y medios necesarios a desarrollar todas las medidas de seguridad que se consideren oportunas teniendo siempre presente el balance entre los costes y el beneficio.
- ✓ Elaborar un plan de formación y concienciación en materia de Seguridad de la Información que ayude a todo el personal implicado a conocer y cumplir las medidas de seguridad establecidas y a participar de forma proactiva en la gestión de la Seguridad de la Información.
- ✓ Llevar a cabo todas las medidas necesarias para garantizar la adecuada gestión de los incidentes de seguridad que puedan producirse, y que permitan resolver tanto las incidencias menores como las situaciones que puedan poner en riesgo la continuidad de las actividades contempladas.
- ✓ Establecer periódicamente una serie de objetivos e indicadores en materia de seguridad de la información que permitan realizar un seguimiento de la evolución en materia de Seguridad de la Información de la empresa.
- ✓ Implantar una metodología de revisión, una serie de auditorías y un objetivo de mejora continua del sistema que permitan garantizar un buen mantenimiento del nivel de seguridad deseado. FOTEX establece cuáles serán los procedimientos y la forma de proceder para garantizar el cumplimiento de esta política, ofreciendo por tanto un sistema de seguridad, bien documentado, conocido por todo el personal de FOTEX, y que cumple los requisitos establecidos en la norma 27001.

Todo el personal que acceda a los sistemas de información de **FOTEX** deberá seguir las siguientes normas de actuación:

- ✓ Proteger la información confidencial perteneciente o cedida por terceros a FOTEX de toda revelación no autorizada, modificación, destrucción o uso indebido, ya sea accidental o no.

- ✓ Proteger todos los sistemas de información y redes de telecomunicaciones contra accesos o usos no autorizados, interrupciones de operaciones, destrucción, mal uso o robo.
- ✓ Será necesario un acceso autorizado para acceder a los sistemas de información propios de FOTEX y el previo conocimiento y aceptación de la presente política. De forma adicional, todo el personal con responsabilidades específicas dentro del ámbito de actuación indicado deberá asegurarse de que se cumplen las siguientes medidas:
    - Con carácter general, todo diseño, desarrollo, implementación y operación deberá incorporar mecanismos de identificación, autenticación, control de acceso, auditoría e integridad, que se especificarán para cada caso concreto.
    - Se deberán incorporar identificaciones seguras y únicas para la autenticación de usuarios.
    - Para un correcto funcionamiento en materia de seguridad deberán compartirse las labores de seguridad entre usuarios, administradores y los encargados directos de la propia seguridad.
    - Deberán tomarse todas las precauciones posibles para proteger físicamente los sistemas y prevenirlos frente al robo, destrucción o interrupción.
    - Deberá existir un plan de recuperación del sistema para el caso en que se dé robo, destrucción o interrupción del servicio.
    - Deberá asegurarse la confidencialidad de la información almacenada, tanto en formato electrónico como no electrónico.
    - Todos los intervinientes en el plan de continuidad de negocio deberán conocer y saber aplicar cuando sea necesario dicho plan.

- El personal del área de operación deberá tener conocimiento de los procedimientos de recuperación de datos de carácter personal, de somatización de los soportes de datos de carácter personal y del procedimiento de registro entrada/salida de dichos soportes.

Badajoz, febrero 2018

Director General de FOTEX