stk asset management

POLÍTICA DE GESTIÓN DE LA INFORMACIÓN DE STAKE AFPISA
ACTA DE DIRECTORIO 27/2022

1. GENERALIDADES

1.1. Los accesos privilegiados serán otorgados de manera restringida a la necesidad de trabajo o serán centralizadas en el Director Ejecutivo responsable de la supervisión correspondiente.

1.2. No está permitido el acceso remoto de terceros externos a la firma a las sesiones de usuarios de cuentas a ninguno de los sistemas empleados.

1.3. La firma tiene como principio general de selección de servicios y sistemas que operen enteramente en la nube ("Software as a Service"), empleando rígidos mecanismos de autenticación de usuarios, control de acceso y respaldo de datos.

2. CONTRASEÑAS

2.1. Las contraseñas deben ser secretas; sólo deben conocerlas el propio usuario y nunca debe ser la contraseña inicial del servicio.

2.2. No debe ser posible averiguar las contraseñas y éstas no deben ser predecibles ni deducibles a partir de información disponible de forma pública.

2.3. No se debe emplear la misma contraseña para varias cuentas, servicios o plataformas.

2.4. Las contraseñas deben ser cambiadas al menos una vez al año por el usuario y al momento del primer acceso al servicio o cuenta.

2.5. Siempre debe utilizarse un segundo factor de autenticación además de la contraseña, cuando estuviere disponible, para todas cuentas, servicios o plataformas.

3. CORREO ELECTRÓNICO Y MENSAJERÍA INSTANTÁNEA

3.1. Los usuarios tienen prohibido utilizar el correo electrónico o las cuentas de Teams u equivalente de otra persona sin su consentimiento.

3.2. Toda información almacenada o enviada a través de cuentas de comunicaciones de la firma no es considerada privada para la firma.

3.3. Todos los correos electrónicos y mensajes de Teams enviados y recibidos con cuentas de la firma deben ser resguardados y trazables.

4. SEGURIDAD EN TRANSMISIÓN DE DATOS

4.1. Todos los datos de la firma deben ser encriptados cuando son transmitidos por redes externas.

4.2. En las conexiones a Internet que realice la firma se debe utilizar un protocolo de comunicación encriptada del tipo SSL o similar.

4.3. Los usuarios que accedan a datos propiedad de la firma sólo deben hacerlo mientras están conectadas a redes mediante vínculos de comunicaciones encriptadas.

4.4. Las computadoras o redes de la firma solo deben ser conectadas a otras computadoras o redes externas mediante vínculos de comunicaciones encriptadas.

4.5. Todos los datos e información utilizadas por la firma le pertenecen a éste, excepto que un contrato exprese lo contrario.

5. PROTECCIÓN DE DATOS

5.1. Toda información confiada por terceros para ser almacenada, transmitida o procesada por la firma debe ser tratada y protegida como lo especifique el contrato correspondiente, o en su defecto debe ser considerada como información confidencial propia de la firma.

5.2. Todo archivo de datos almacenado, transmitido o procesado es propiedad de la firma y por lo tanto está prohibida su venta o divulgación sin autorización.

5.3. Todos los datos recibidos, generados y modificados por la firma para el giro normal de sus operaciones deben ser respaldados al menos en tres copias, en dos medios diferentes y uno de ellos debe estar fuera de sus oficinas.

5.4. Todos los equipos empleados para tratar datos en el curso normal de las operaciones de la firma deben contar con software antivirus y deben estar en un estado que razonablemente permita la protección general del soporte físico de los datos.

5.5. Los datos sensibles que deben ser compartidos con partes autorizadas deben ser puestos a disposición mediante carpetas compartidas en las se empleen contraseñas y la disponibilidad del acceso para los terceros debe tener una fecha de vencimiento.

HISTÓRICO DE REVISIONES			
REVISIÓN	**FECHA**	**DESCRIPCIÓN DE LA MODIFICACIÓN**	**RESPONSABLE**

ELABORADO POR				**APROBADO POR**			
Director Financiero				Directorio			
Firma: JULIO JOSE RECALDE LARA				Acta N° 27/2022			
Fecha	02	05	2022	**Fecha**	02	05	2022

STAKE AFPISA
hola@stkasset.com