POLÍTICA DEL USO DEL ENCRIPTADO	PRO-17
	Revisión 00

REV.	FECHA	DESCRIPCIÓN

ELABORADO POR:	REVISADO Y APROBADO POR: DIRECCIÓN
FECHA: 05/05/2018	

POLÍTICA DEL USO DEL ENCRIPTADO	PRO-17
	Revisión 00

ÍNDICE

POLÍTICA DEL USO DEL ENCRIPTADO	PRO-17
	Revisión 00

1.-OBJETO

El objetivo del presente documento es definir reglas para el uso de los controles y claves encriptado para proteger la confidencialidad, integridad, autenticidad e inviolabilidad de la información.

Este documento se aplica a todas las actividades de procesamiento de datos.

Los usuarios de este documento son la Dirección y los Responsable de Seguridad y Encargados.

2.-ALCANCE

Este procedimiento es aplicable a todo el personal de la empresa.

3.-DEFINICIONES

4.-DESCRIPCIÓN

Uso de encriptado

4.1. Controles encriptados

De acuerdo con la Política de clasificación de la información, como también con obligaciones legales y contractuales, la organización debe proteger a los sistemas individuales o a la información a través de los siguientes controles encriptados:

POLÍTICA DEL USO DEL ENCRIPTADO	PRO-17
	Revisión 00

Nombre del sistema / tipo de información	*Herramienta encriptada*	*Algoritmo de encriptación*	*Longitud de la clave*
Emails con información confidencial	Fichero cifrado de Windows	Proporcionado por windows	Superior a 1024 bits

El Responsable de Seguridad es el responsable de redactar instrucciones detalladas sobre el uso de las mencionadas herramientas de encriptación. Los propietarios de los activos individuales sobre los cuales se aplican controles encriptados, son los responsables por la correcta aplicación de los controles encriptados particulares.

4.2. Claves criptográficas

En la mayoría de los casos, la empresa no podrá controlar las claves criptográficas porque están integradas en el canal de comunicación, p. el uso del protocolo HTTPS / SSL mientras navega por el sitio web. En el caso de que pueda hacerlo, el Responsable de Seguridad es el responsable de establecer las siguientes reglas sobre la gestión de claves:

- Generación de claves criptográficas privadas y públicas.
- Activación y distribución de claves criptográficas.
- Definición del plazo para el uso de las claves y de su actualización periódica (de acuerdo con la evaluación de riesgos).
- Archivo de claves inactivas que son necesarias para archivos electrónicos encriptados. Destrucción de claves.

Las claves son administradas por sus propietarios, en conformidad con las reglas mencionadas precedentemente.

Las claves criptográficas serán protegidas por llave. En el caso de pérdida, corrupción o destrucción, las claves serán recuperadas por el Responsable de Seguridad, generando una nueva clave que el usuario deberá cambiar en el primer registro que se utilice.

5.-ARCHIVO Y CODIFICACIÓN DE REGISTROS

POLÍTICA DEL USO DEL ENCRIPTADO	PRO-17
	Revisión 00

Nombre del registro	Ubicación de archivo	Persona responsable del archivo	Controles para la protección del registro	Tiempo de retención
Registros de gestión de claves	Carpeta RGPD	Responsable de Seguridad	Solamente el Responsable de Seguridad tiene derecho de acceso a estos registros.	Los registros son almacenados por el plazo de 10 años.