EthicsGlobal

POLÍTICA DE CLAVES

Código:	SOS-PCLV-PO-36-v3
Versión:	3.0
Fecha de la versión:	17-ene-2022
Creado por:	Javier Flores
Aprobado por:	Dirección General
Nivel de confidencialidad:	Uso Interno

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
24-oct-2018	1.0	Javier Flores	Primera versión.
06-nov-2019	2.0	Javier Flores	Autentificación doble factor
17-ene-2022	3.0	Denice Arroyo	Resguardo y procedimiento para divulgación de contraseñas

Tabla de contenido

1. Objetivo, alcance y usuarios

El objetivo del presente documento es establecer reglas para garantizar la gestión y utilización seguras de las claves.

Este documento se aplica a todo el alcance del Sistema de gestión de seguridad de la información (SGSI); es decir, a todos los puestos de trabajo y sistemas ubicados dentro del alcance del SGSI.

Los usuarios de este documento son todos los empleados de EthicsGlobal.

2. Documentos de referencia

- Norma ISO/IEC 27001, capítulos A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.3, A.6.1.2
- Política de seguridad de la información
- Declaración de aceptación de los documentos del SGSI

3. Obligaciones de los usuarios

Algunas de las siguientes reglas son aplicadas de manera automática a los usuarios de SED pero se deben considerar para cualquier otro ámbito que requiera el uso de contraseñas.

El personal sólo tendrá acceso a la clave del llavero LastPass proporcionada por el departamento de TI, dicha clave le permitirá gestionar el uso del llavero de credenciales de EthicsGlobal, dichas claves corresponden a los sistemas/redes/servicios a los que el usuario tiene acceso como se especifica en la Política de Control de Acceso.

Salvo la contraseña de LastPass y las contraseñas que el CISO autorice para tal motivo, queda prohibido que los usuarios guarden credenciales de acceso en cualquier otro sistema/archivo/medio o la ingresen de manera manual en los sistemas de información de EthicsGlobal. Por lo que, las credenciales de acceso de todos los sistemas de información (en donde aplique) deberán estar almacenadas en LastPass.

La contraseña de LastPass no deberá tampoco ser almacenada en ningún sistema/archivo/medio, ni podrá ser recordada por el sistema por lo que el usuario deberá teclearla al inicio de la jornada laboral.

En los sistemas/redes/servicios en los que el CISO haya requerido una autenticación doble factor, los tokens se generarán en el servicio Authy con una contraseña maestra la cual no debe ser almacenada en ningún sistema/archivo/medio. De manera que, todos los usuarios deberán tener activada la autentificación doble factor en los sistemas que aplique.

Los usuarios deben aplicar buenas prácticas de seguridad en cuanto a la elección y uso de claves:

- No se deben revelar las claves a otras personas, incluyendo la gerencia y los administradores del sistema.

- No se debe llevar un registro de las claves, a menos que un método seguro haya sido aprobado por CISO.
- Las claves generadas por el usuario no deben ser distribuidas por ningún medio (oral, escrito, electrónico, etc.); las claves deben ser cambiadas si existen indicios de que puedan estar en riesgo las mismas claves o el sistema (en ese caso, se debe informar un incidente de seguridad).
- Se deben escoger claves seguras de la siguiente forma:
    - utilizando al menos doce caracteres;
    - utilizando al menos un carácter numérico;
    - utilizando al menos un carácter alfabético en mayúscula y uno en minúscula;
    - utilizando al menos un carácter especial;
    - una clave no debe ser una palabra que se encuentre en el diccionario, en un dialecto o jerga de ningún idioma; como tampoco ninguna de estas palabras escritas hacia atrás;
    - las claves no deben estar relacionadas con datos personales (por ej., fecha de nacimiento, domicilio, nombre de un familiar, etc.);
    - no se deben usar nuevamente las últimas tres claves.
- Se deben cambiar las claves cada 3 meses.
- Se deben cambiar las claves en el primer ingreso al sistema.
- Las claves no deben ser almacenadas en un sistema de registro automatizado no autorizado por el CISO (por ej., macros o explorador).
- No se deben utilizar las mismas claves personales para fines privados y para fines comerciales.

- Se deben utilizar donde estén disponibles mecanismos de autenticación de doble factor.

4. Resguardo y divulgación de contraseñas

4.1. Procedimiento

A) Por cada área o departamento o conjunto de los mismos (si lo designa la organización), habrá un representante que será el designado para almacenar las contraseñas de acceso a sistemas, bases de datos, producción, aplicativos, etc. de EthicsGlobal; serán excluidos de este paso algunos colaboradores que serán mencionados más adelante.

B) El representante será el encargado de compartir dichos accesos haciendo uso del gestor de contraseñas Lastpass utilizando la configuración de “ocultar contraseña y bloqueo de copiado”. Sin embargo, algunos colaboradores podrán conocer y cambiar algunas contraseñas (conforme a las reglas definidas en el apartado de Obligaciones de los usuarios) dependiendo de su uso y actividades laborales, ejemplo: Microsoft Teams, Onedrive y Lasstpast.

C) El representante mencionado en los puntos anteriores no deberá tener ningún tipo de permiso o privilegio para poder crear y otorgar accesos en cualquiera de los sistemas, aplicativos, bases de datos de la Organización, únicamente se encargará de almacenar en un sitio seguro las contraseñas y compartirlos apropiadamente.

4.2. Áreas, departamentos o colaboradores que manejarán en su totalidad sus credenciales de accesos

- Dirección General
- Departamento de Administración, Contabilidad, Recursos Humanos y Capital Humano
- Dirección administrativa
- Dirección de operaciones
- Dirección de sistemas
- Departamento de Seguridad de la Información

4.3. Áreas, departamentos o colaboradores que no podrán conocer ni manejar ningún acceso

- Área de Contact Center

4.4. Representante (s) designado (s) para realizar este procedimiento

- Coordinación de Soporte técnico
- CISO

5. Validez y gestión de documentos

Este documento es válido hasta el 05-may-2022.

El propietario de este documento es el CISO, que debe verificar, y si es necesario actualizar, el documento por lo menos una vez al año.

Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:

- Cantidad de incidentes relacionados con el uso indebido de claves por personas no autorizadas.
- Cantidad de incidentes relacionados con el manejo inadecuado de claves.