Objetivo

Establecer mediante el uso de claves, la seguridad de los aplicativos, servidores, bases de datos y periféricos del Instituto.

Alcance

Este procedimiento aplica para las claves de los aplicativos, servidores de cómputo, dispositivos de red, bases de datos y periféricos. Parte de la asignación de responsables y/o titulares de las claves, seguridad en la custodia de las claves y termina con el cambio y/o actualización periódica de dichas claves.

Definiciones

Claves Sensitivas: Son aquellas que se asignan a un usuario para la administración, seguridad, parametrización y procesamiento de un sistema o aplicativo.

Siglas (si se requiere)

Normatividad

Estándar Internacional ISO/IEC 27001:2013.

Ver Normograma

Documentos relacionados en el SGI

SGI-F086 Formato Cambio de Claves de Aplicación.
SGI-F082 Formato Cambio de Claves de Servidores.
SGI-F083 Formato Cambio de Claves de activos de red.

Desarrollo

CONDICIONES GENERALES.

La contraseña debe cumplir con los cuatro requisitos:

- Caracteres en mayúsculas y minúsculas
- Extensión mínima de 12 caracteres
- Base de 10 dígitos (0 a 9)
- Caracteres no alfabéticos (Ejemplo i,$,%,&)

En caso que alguno de los responsables de manejar claves sensitivas sospeche que alguien conoce la clave, ésta debe ser cambiada inmediatamente.

Las claves sensitivas deberán ser cambiadas semestralmente en su totalidad

Las contraseñas referentes a las cuentas "predefinidas" incluidas en los sistemas o aplicaciones adquiridas deben ser desactivadas. De no ser posible su

desactivación, las contraseñas deben ser cambiadas después de la instalación del producto

Se debe concienciar y controlar a los usuarios para que apliquen buenas prácticas de seguridad en la selección, uso y protección de claves o contraseñas; las cuales constituyen un medio de validación de la identidad de un usuario y consecuentemente un medio para establecer derechos de acceso a las instalaciones, equipos o servicios tecnológicos.

Los usuarios son responsables del uso de las claves o contraseñas de acceso que se le asignen para la utilización de los equipos o servicios informáticos de la Entidad.

Ningún usuario deberá acceder a la red o a los servicios TIC del IDEAM, utilizando una cuenta de usuario o clave de otro usuario

Se debe garantizar en las plataformas de tecnología que el ingreso a la administración en lo posible, se realice con la vinculación directamente de las credenciales de los usuarios de directorio activo.

No.	Actividad	Ciclo PHVA	Responsable	Registro	Puntos de control	Tiempo de actividad
1	Asignar el titular y/o dueño de la Aplicación (Líder técnico), dueño del servidor y/o DBA, quien será el responsable del uso de las claves.	P	Jefe Oficina de Informática	Correo electrónico		
	Seguridad custodia de las bases de datos con claves sensibles					
2	Mantener en custodia una copia de la base de datos de contraseñas cifrada.	H	Jefe Oficina de Informática	Correo y/o memorando de entrega.		
3	Mantener en custodia una copia de la base de datos de	H	Oficial de Seguridad.	USB. Formato Bitácora Gestión de		

No.	Actividad	Ciclo PHVA	Responsable	Registro	Puntos de control	Tiempo de actividad
	contraseñas en un medio físico, estas cifradas con algoritmo AES-256			Servidores - Sección Gestión de Claves.		
4	Cada especialista es responsable de alimentar la base de datos con los accesos administrados La base de datos de acceso se crea y edita mediante el software de gestión de acceso Keepass v 2.47 El oficial de seguridad proporcionara una llave para realizar cifrado de la base de datos a cada especialista	H	Titular de la clave.	USB. Formato Bitácora-Gestión de Servidores - Sección Gestión de Claves.		
	CAMBIO PERÍODICO DE CLAVES POR LOS TITULARES.					
5	Enviar correo electrónico, recordando el cambio de clave a los titulares de la claves de las aplicaciones, servidores y/o bases de datos, sin perjuicio que el responsable haga el cambio de clave según se define en este procedimiento.	**H**	Oficial de Seguridad	**Correo electrónico**		

No.	Actividad	Ciclo PHVA	Responsable	Registro	Puntos de control	Tiempo de actividad
6	Solicitar la base de datos de en custodia para cambiar la clave en el aplicativo, servidor y/o base de datos correspondiente.	**H**	Titular de la clave.	Verificación del cambio de clave en los Logs del sistema.	**X**	
7	Diligenciar los formatos Cambio de Claves de Aplicación, Cambio de Claves de Servidores y/o Archivo Word para el caso de bases de datos, según corresponda. En caso que se requiera realizar un cambio de claves adicional a la planteada semestralmente	**H**	Titular de la clave.	Formato Cambio de Claves de Aplicación. Formato Cambio de Claves de Servidores. Formato Cambio de Claves de activos de red.		
8	Entregar en custodia las bases de datos, esta debe de estar cifrada con la contraseña de acceso y llave emitida por el oficial de seguridad. Registrar en el formato de la bitácora Vo.Bo. de entrega	**H**	Titular de la clave.	Formato Bitácora Gestión de Aplicaciones . Formato Gestión de Servidores - Sección Gestión de Claves -		
9	Registrar en la bitácora la fecha	**H**	Oficial de Seguridad	Formato		

No.	Actividad	Ciclo PHVA	Responsable	Registro	Puntos de control	Tiempo de actividad
	de la recepción de la base de datos de contraseñas para custodia y Vo. Bo de recibido. Relacionar el nombre del especialista.			Bitácora Gestión de Aplicaciones . Formato Bitácora Gestión de Servidores - Sección Gestión de Claves.		
10	Guarda el registro de las bases de datos de accesos que custodia. Nota: La información debe ser actualizada cada vez que se cambie una clave y/o acceso.	**V**	Oficial de Seguridad.	Formato Bitácora Gestión de Aplicaciones . Formato Bitácora Gestión de Servidores - Sección Gestión de Claves.		
	SOLICITUD DE LAS BASES DE DATOS DE LAS CLAVES POR CONTINGENCIA.					
11	El Jefe de la Oficina de Informática y/o a quien este designe deberá solicitar la base de datos de las claves del aplicativo, servidores y/o bases de datos	**H**	Jefe Oficina de Informática.	Solicitud verbal y/o por correo.		
12	Entregar la base de datos de las claves del aplicativo, servidores y/o bases de datos	**H**	Oficial de Seguridad.	Formato Bitácora Gestión de Aplicaciones .		

No.	Actividad	Ciclo PHVA	Responsable	Registro	Puntos de control	Tiempo de actividad
	requerido, a la persona designada por el Jefe de la Oficina de Informática. Notificar de dicho uso del sobre al titular de la clave.			Formato Bitácora Gestión de Servidores - Sección Gestión de Claves.		
13	Una vez se haya hecho uso de las claves, entregar la base de datos nuevamente en custodia con las claves actualizadas.	**H**	Persona que haya hecho uso del sobre.			
14	Registrar el VoBo. de recibido en los formatos de gestión de claves.	**V**	Oficial de Seguridad.	Formato Bitácora Gestión de Aplicaciones . Formato Bitácora Gestión de Servidores - Sección Gestión de Claves.		
15	Continuar con la actividad No. 5 de este procedimiento.	**H**	Titular de la clave.			

Nota: las claves deben estar cifradas en una ubicación de drive corporativo con acceso de la Coordinación de la Oficina de informática y el oficial de seguridad y una copia física de ellas en memoria extraíble tipo USB
La llave de acceso a la base de datos será custodiada en una ubicación diferente en el drive corporativo con acceso únicamente por parte de la Coordinación de la Oficina de informática y el oficial de seguridad allí reposará el archivo con las claves que se encuentren vigentes.

Control de cambios

Versión	Fecha	Descripción
01	20/11/2024	Creación del documento
02	23/11/2017	Se actualiza, versión y codificación para cumplimiento con el decreto 415.
03	10/04/2018	Actualización de documento
04	24/01/2025	Actualización medios de almacenamientos de los accesos
05	15/07/2025	Se ajusta código de E-SGI-SI-P002 a SGI-P016 y se realiza cambio de imagen del documento