MACROPROCESO: Gestión de Información y Tecnología	PROTOCOLO	Código: H5-P01-P01
PROCESO: Tecnología	PROTOCOLO SEGURIDAD FIRMAS DIGITALES	Vigente desde: 02.02.2017

CONTROL DE CAMBIOS		
FECHA	**VERSIÓN**	**DESCRIPCIÓN DEL CAMBIO**
02.02.2017	V1	Lanzamiento de Documento

1. OBJETIVO

Garantizar la seguridad de la instalación, uso y administración de las firmas digitales a cargo de los colaboradores de la Fundación Universitaria del Área Andina.

2. ALCANCE

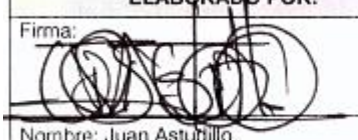
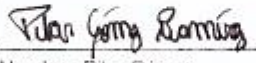
Inicia con la instalación de los elementos de hardware y software adquiridos por la institución y termina con el informe de uso y seguridad de las firmas digitales. Aplica para todas las sedes y seccional a nivel nacional.

3. DEFINICIONES

- **Firma digital:** Una firma digital (que no debe confundirse con un certificado digital) es una técnica matemática utilizada para validar la autenticidad y la integridad de un mensaje, software o documento digital.

- **Autenticación:** Es el proceso por el cual se establece que el usuario que intenta acceder a un componente tecnológico es quien dice ser; a través de diferentes mecanismos o factores de autenticación se verifica la identidad del usuario. Dentro de los diferentes factores de autenticación se tienen:

    - Algo que solamente el individuo conoce o sabe (ejemplo: contraseña).
    - Algo que una persona posee (ejemplo: una tarjeta de proximidad o token).
    - Algo que el individuo es o hace (ejemplo: huellas digitales, sensores biométricos, reconocimiento de voz, patrones de escritura, patrones en la forma de caminar).

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Firma: 	Firma: 	Firma: 
Nombre: Juan Astudillo Cargo: Coordinador de Procesos	Nombre: Pilar Gómez Cargo: Coordinador de Procesos	Nombre: José Guevara Cargo: Director Nacional de Tecnología

- **Contraseña:** Conjunto de caracteres de composición alfanumérica que permite habilitarle a un usuario el acceso a un determinado recurso o la utilización de un servicio dado.

- **Cuenta de Usuario:** La cuenta de usuario es la identificación con que el usuario va a ser reconocido dentro del sistema de Información, sistema operativo o cualquier sistema informático.

- **Bitácora de transacciones**: Registro de transacciones realizadas en un sistema de información.

- **Colaborador areandino:** Corresponde a todos aquellos administrativos de la Fundación Universitaria del Área Andina vinculados bajo cualquier modalidad de contratación.

4. MATRIZ DE RIESGOS Y CONTROLES.

Cód. Riesgo	Descripción del Riesgo	Cód. Control	Descripción del Control
R-PFD-001	El elemento de Hardware y Software es recibido por una persona que no es la responsable	C-PFD-001	Acta de entrega de elementos de hardware y software a través del formato (Acta entrega activos fijos) en el cual se responsabiliza la persona que recibe el elemento de hardware y software
R-PFD-002	Un tercero tiene acceso a las opciones de certificados digitales.	C-PFD-002-1	Aplicar las cláusulas de confidencialidad en la relación contractual con la Institución.
		C-PFD-002-2	Solicitar al proveedor la revocación temporal o permanente y solicitar nuevamente las credenciales
R-PFD-003	No se realiza la instalación oportuna por falta de	C-PFD-003	Una vez se hagan las solicitudes de compra se

Cód. Riesgo	Descripción del Riesgo	Cód. Control	Descripción del Control
	conocimiento en el proceso de dicha instalación.		envía copia a la mesa de ayuda. El técnico de mesa de ayuda debe efectuar un seguimiento y dejar evidencia de dicho seguimiento hasta el momento de la instalación correspondiente.
R-PFD-004	Falta de completitud de los datos necesarios	C-PFD-004	Aplicación del Proceso de back up por parte del área de Tecnología
R-PFD-005	Se pierde información en el proceso de depuración de los logs	C-PFD-005	Periódicamente se efectúan pruebas de recuperación de back up por parte del área de Tecnología
R-PFD-006	Existen diferencia entre el inventario de tecnología y los dispositivos físicos existentes	C-PFD-006	Realizar verificación periódica mínimo 3 (tres) veces al año del inventario por parte del área de Tecnología.

5. SISTEMAS DE INFORMACIÓN ASOCIADOS

- Sistema de Información Académico
- Software de Gestión Documental.

6. CONDICIONES Y POLÍTICAS

- El uso de la firma digital es personal e intransferible de acuerdo con la Política Específica de Seguridad de Gestión de Usuarios y Contraseñas. El colaborador areandino debe ejercer el uso de la firma digital con alto sentido de responsabilidad, teniendo en cuenta todos los factores de riesgo implícitos en su administración.

- El área de Tecnología debe garantizar que se mantengan disponibles de forma permanente las copias de seguridad de los distintos sistemas de información institucionales, que incluyan la bitácora de las transacciones con firma digital.

- El área de Tecnología y la mesa de ayuda en conjunto, serán los responsables de la correcta instalación (de ser necesario) de los elementos de hardware y software asignados a los colaboradores o cargos directivos que emitirán firmas digitales.

- La instalación de los elementos de hardware y software que acompaña el proceso de firma digital, debe hacerse en el equipo asignado al colaborador o directivo responsable. En ningún caso se hará en dos o más máquinas.

- En caso de pérdida o robo el colaborador o directivo responsable debe informar inmediatamente la novedad al proveedor de la firma digital de acuerdo con sus procedimientos y debe instaurar el denuncio correspondiente a más tardar el siguiente día hábil de la ocurrencia del hecho.

- El director de toda área que sea responsable de emitir firmas digitales, debe implementar estrategias de autocontrol para asegurar el correcto uso de las firmas y guardar la evidencia de los controles implementados.

- El elemento de hardware y software que permite la emisión de firmas digitales, debe permanecer bajo custodia del colaborador o directivo responsable.

- El área de Tecnología debe contar con planes de acción diseñados para el caso de pérdida o robo de los elementos de hardware y software asociados a la firma digital. Dichos planes de acción deben ser documentos de registro incluidos en los procedimientos institucionales dentro de los cuales se implementen firmas digitales.

- Para realizar auditoría a transacciones emitidas a través de plataformas externas, el representante legal debe solicitar al proveedor, la bitácora de transacciones realizadas según el alcance de la auditoría a realizar. Control Interno incluirá dichos registros como insumo de las auditorías administrativas o académicas según corresponda.

- La base de datos de los colaboradores que tienen firmas digitales se encuentra bajo custodia de Director Nacional de Tecnología.

7. ACTIVIDADES

7.1 Recepción e instalación de los elementos de hardware y software

NOMBRE DE LA ACTIVIDAD	DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE/CARGO	CONTROL ASOCIADO	DOCUMENTOS Y/O REGISTROS ASOCIADOS
1. Recibir los elementos de hardware y software	Se recibe por parte del colaborador o directivo, los elementos de hardware y software adquiridos por la institución, verificando que corresponda con la SOLP montada en SAP	Solicitante	C-PFD-001	
2. Solicitar Instalación	Se coloca el caso en la mesa de ayuda solicitando la asistencia técnica del área de tecnología para la instalación de los elementos de hardware y software en el PC del colaborador responsable de emitir las firmas digitales.	Solicitante	C-PFD-002-1 C-PFD-002-2	

NOMBRE DE LA ACTIVIDAD	DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE/CARGO	CONTROL ASOCIADO	DOCUMENTOS Y/O REGISTROS ASOCIADOS
3. Instalar elementos de hardware y software	Se instalan los elementos de hardware y software en el equipo asignado al solicitante	Colaborador Responsable Técnico de Mesa de Ayuda	C-PFD-003	
4. Capacitar al usuario	Se capacita al usuario por parte del proveedor o colaborador de tecnología acerca de los pormenores del uso del sistema de firma digital	Proveedor Técnico de Mesa de Ayuda		Acta de capacitación

7.2 Seguridad de la información

NOMBRE DE LA ACTIVIDAD	DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE/CARGO	CONTROL ASOCIADO	DOCUMENTOS Y/O REGISTROS ASOCIADOS
1. Generar copia de seguridad	Se genera copia de seguridad de la bitácora de transacciones para el caso de sistemas de información institucionales e información básica de acceso para sistemas de información	Automático a través de sistema	C-PFD-004 C-PFD-005	

NOMBRE DE LA ACTIVIDAD	DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE/CARGO	CONTROL ASOCIADO	DOCUMENTOS Y/O REGISTROS ASOCIADOS
	externos (Mapeo de actividades).			
2. Reportar informe de copias de seguridad realizadas	Se reporta al Vicerrector Nacional Administrativo y Financiero o a quien haga sus veces un informe semestral que incluya la información relevante de la bitácora de transacciones realizadas a través de firma digital de los distintos sistemas de información.	Director Nacional de Tecnología		Reporte copias de seguridad bitácora de firmas digitales
3. Incluir reportes en auditorias	Incluir como insumo de las auditorías administrativas o académicas los reportes de las copias de seguridad de la información asociada a las firmas digitales generadas.	Auditor Senior		Reporte copias de seguridad bitácora de firmas digitales

7.3 Pérdida o robo de los elementos de hardware y software

NOMBRE DE LA ACTIVIDAD	DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE/CARGO	CONTROL ASOCIADO	DOCUMENTOS Y/O REGISTROS ASOCIADOS
1. Notificar pérdida o robo de elementos de software o hardware asociados a la firma digital.	Se notifica al proveedor de la firma la pérdida o robo de los elementos de hardware y software asociados a la firma digital para su revocatoria.	Colaborador o directivo responsable de firma digital	C-PFD-006	
2. Instaurar denuncio por pérdida o robo de los elementos de hardware y software	Se instaura la denuncia de pérdida o robo ante la autoridad competente	Colaborador o directivo responsable de firma digital		Denuncio
H2-P02-PR02 GESTIÓN DE COMPRA				

8. NORMAS RELACIONADAS AL PROCEDIMIENTO

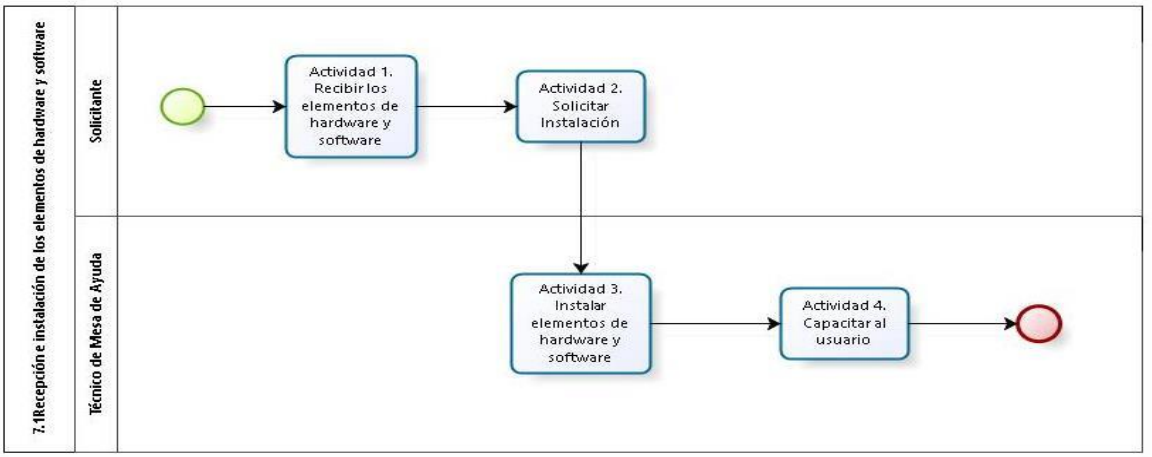
- Política específica de seguridad – Gestión de Usuarios y Contraseñas Areandina.

9. CONTROL DE DOCUMENTOS

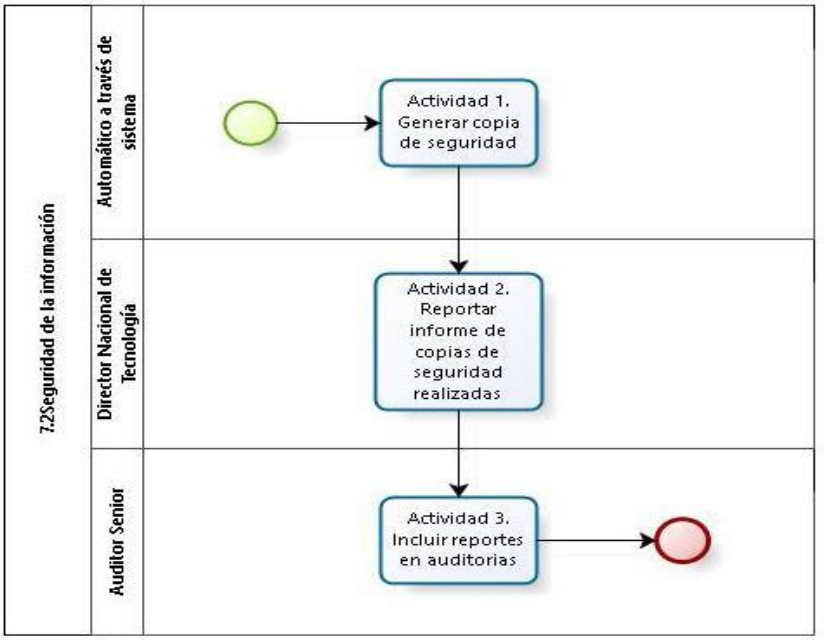
CODIGO	NOMBRE	QUIEN DILIGENCIA	COMO SE ALMACENA Y RECUPERA	TIEMPO DE RETENCIÓN	DISPOSICIÓN FINAL Y RESPONSABLE
N/A	Acta de Capacitación	Técnico Mesa de Ayuda	Físico	Un (1) año	Archivo Inactivo
N/A	Reporte copias de seguridad bitácora de firmas digitales	Generado automáticamente desde el sistema	Formato Digital	Un (1) año	Copia de Seguridad
N/A	Denuncio	Responsable de firma digital	Físico	Un (1) año	Archivo Inactivo

10. FLUJOGRAMAS

10.1 Recepción e instalación de los elementos de hardware y software.



10.2 Seguridad de la información.



10.3 Pérdida o robo de los elementos de hardware y software