

	POLÍTICA DE USO Y SEGURIDAD PARA APP MACROPROCESO DE TECNOLOGIA Y SISTEMAS DE INFORMACIÓN PROCESO DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: PL-002-TIC
		VERSIÓN: V1.0-2023

MACROPROCESO Y/O PROCESO AL CUAL PERTENECE LA POLÍTICA	TECNOLOGIA Y SISTEMAS DE INFORMACION	RESPONSABLE	ING. SEGURIDAD INFORMATICA
---	---	--------------------	----------------------------

DEFINICIONES		
No.	TÉRMINO	DEFINICIÓN
1	APP	Abreviatura de "aplicación" en inglés, y se utiliza para referirse a un software diseñado para ser utilizado en un dispositivo móvil.
2	Habeas Data	Habeas Data es un derecho fundamental que garantiza a las personas el acceso, la consulta, la actualización y la rectificación de sus datos personales, que hayan sido recolectados, almacenados y procesados por empresas, organizaciones y el Estado.
3	Responsabilidad	Refiere a la obligación de los usuarios del APP de respetar los términos y condiciones establecidos por los propietarios o desarrolladores del APP, así como de utilizarlo de manera ética y legal.

POLITICA DE USO Y SEGURIDAD PARA LA APP DE CAPITAL SALUD EPS-S S SAS

1. OBJETIVO DE LA POLITICA:

Establecer y difundir las políticas de Seguridad de la información a todos los usuarios de Capital Salud EPS-S, para que sea de su conocimiento y cumplimiento en los recursos del uso de la APP, permitiendo proteger la información, teniendo en cuenta aspectos legales, operativos, tecnológicos de la entidad.

2. DESCRIPCIÓN DE LA POLÍTICA:

2.1. POLITICA DE USO Y SEGURIDAD PARA LA APP DE CAPITAL SALUD EPS-S S SAS

Capital Salud EPS-S, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido a establecer un marco de confianza en el ejercicio de sus deberes, enmarcado en el cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para Capital Salud EPS-S, la protección de la información busca disminuir el impacto generado sobre sus activos, con objeto de velar por la integridad, confidencialidad y la disponibilidad de esta.

Esta política aplica a la Entidad según como se defina en el alcance, sus trabajadores, colaboradores y terceros, tomando como base el desarrollo de las acciones o toma de decisiones, permitiendo:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.



	POLÍTICA DE USO Y SEGURIDAD PARA APP MACROPROCESO DE TECNOLOGÍA Y SISTEMAS DE INFORMACIÓN PROCESO DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: PL-002-TIC VERSIÓN: V1.0-2023
---	---	---

- Mantener la confianza de sus clientes, socios y trabajadores.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los trabajadores, colaboradores y terceros de Capital Salud EPS-S.
- Garantizar la continuidad del negocio frente a incidentes presentados.

2.2. RESPONSABILIDADES DE LA DIRECCION DE TECNOLOGÍA

- Establecer, mantener y divulgar la política de uso a los usuarios del APP.
- Mantener la custodia de la información generada por el APP.
- Aplicar y hacer cumplir la Política de Uso y Seguridad para el APP y todo lo que esta conlleve.
- Administrar la política de acceso y los componentes tecnológicos.
- Analizar, aplicar y mantener los controles de seguridad implementados para asegurar la información y data del APP.
- Gestionar y resolver de común acuerdo con las áreas y los propietarios de la información los conflictos que se presenten por la propiedad de la información al interior de la entidad. Esto incluye los posibles medios de acceso a la información, los datos derivados del procesamiento de la información a través del APP, los datos de entrada al APP y los datos que son parte integral del apoyo de la solicitud.
- Implementar los controles necesarios para verificar el cumplimiento de la presente política.

2.3. POLÍTICA DE CONTROL DE ACCESOS

- La Entidad define las reglas para asegurar un acceso controlado, lógico, al APP informática de Capital salud EPS-S.

2.3.1. Características de las contraseñas:

Tener mínimo diez (10) caracteres alfanuméricos.

Cada vez que se cambien estas deben ser distintas por lo menos de las últimas veinticuatro anteriores.

La contraseña debe cumplir con los siguientes requisitos:

- Mínimo 1 carácter en mayúsculas
- Mínimo 1 carácter en minúsculas
- Mínimo 1 dígito en base de 10 dígitos (0 a 9)
- Mínimo 1 carácter especial no alfabéticos (Ejemplo: \$, %, &)

Uso Indebido y Prohibido

Dar a un tercero el usuario y/o contraseña de acceso al APP, el usuario es responsable del debido uso de usuario/contraseña

	POLÍTICA DE USO Y SEGURIDAD PARA APP MACROPROCESO DE TECNOLOGIA Y SISTEMAS DE INFORMACIÓN PROCESO DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: PL-002-TIC
		VERSIÓN: V1.0-2023

3. ALCANCE:

La POLÍTICA DE USO Y SEGURIDAD PARA LA APP DE CAPITAL SALUD EPS-S S SAS está dirigida a todos los usuarios que tenga legítimo acceso al APP Capital Salud EPS-S.

Todo usuario que acceda al APP de Capital Salud EPS-S es responsable por:

- Dar cumplimiento a la presente política, independiente del equipo móvil que utilice para acceder al APP

4. **ORIGEN:** Interno.

5. **PLAZO:** Largo plazo.

6. **RECURSOS NECESARIOS PARA EL DESARROLLO DE LA POLÍTICA:** Recurso Humano y Tecnológico.

7. **PERIODICIDAD:** Se realizará una revisión Anual a la política

8. REFERENCIAS

DOCUMENTOS DE REFERENCIA	
CÓDIGO (CUANDO APLIQUE)	NOMBRE DEL DOCUMENTO
CONSTITUCIÓN POLÍTICA DE COLOMBIA 1991; Artículo 15.	"Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. Disponible en Línea: http://www.constitucioncolombia.com/titulo-2/capitulo-1/articulo-15
LEY 527 DE 1999;	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. Disponible en Línea: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276
LEY 1266 DE 2008,	Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. Disponible en Línea: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34488
LEY 1273 DE 2009,	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Disponible en Línea: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

	POLÍTICA DE USO Y SEGURIDAD PARA APP MACROPROCESO DE TECNOLOGÍA Y SISTEMAS DE INFORMACIÓN PROCESO DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: PL-002-TTC VERSIÓN: V1.0-2023
---	---	---

LEY ESTATUTARIA 1581 DE 2012,	Por la cual se dictan disposiciones generales para la protección de datos personales. Congreso de la República. Disponible en Línea: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981
MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.	Modelo de Seguridad y Privacidad de la Información alineado con la Estrategia de Gobierno en línea para ser adoptado por todas las entidades estatales Disponible en Línea: https://www.mintic.gov.co/gestionti/615/articulos-5482_Modelo_de_Seguridad_Privacidad.pdf
NORMA TÉCNICA COLOMBIANA ISO27000	Contiene un conjunto de buenas prácticas para el establecimiento, implementación, mantenimiento y mejora de Sistemas de Gestión de Seguridad de la Información, Disponible en Línea: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=2ahUKEwj1h8quoKDeAhWizFMKHTspDIIQFjABegQIChAC&url=https%3A%2F%2Ftienda.icontec.org%2Fwp-content%2Fuploads%2Fpdfs%2FNTC-ISO-IEC27000.pdf&usq=AOvVaw3zcBlpFRBDilwc3ePIVYrr

9. ELABORACIÓN, REVISIÓN Y APROBACIÓN DE LA POLÍTICA:

NOMBRE RESPONSABLE DE LA ELABORACION	Juan Pablo Perez Duarte	CARGO	Ingeniero de Seguridad Informática
FECHA DE ELABORACION	15/05/2023		
NOMBRE RESPONSABLE DE LA REVISION	Jhon Alexander Cepeda Zafra	CARGO	Director de Tecnología
FECHA DE REVISIÓN	24/05/2023		
NOMBRE RESPONSABLE DE LA APROBACION	Jhon Alexander Cepeda Zafra	CARGO	Director de Tecnología
FECHA DE APROBACION	24/05/2023		

OMAR PEREZ BALLESTEROS
Gerencia General

JHON ALEXANDER CEPEDA ZAFRA
Director de Tecnología