VERSIÓN	DESCRIPCIÓN DEL CAMBIO O MODIFICACIÓN	FECHA ÚLTIMA VERSIÓN
02	Modificación del documento con alcance regional	24/07/2023
01	Actualización de documento	23/07/2021
00	Documento nuevo	04/03/2016

ELABORÓ:	**REVISÓ**:	**REVISÓ**:	**REVISO**:	**APRUEBA:**
Juan Pablo Ramírez Analista de Seguridad de Información	Denisse Del Rosario Jefe de Seguridad de la Información y Cumplimiento TI	Yesenia Yance Jefe de Seguridad Informática y Ciberseguridad	Gastón Fourcade Gerente de Tecnología	Suso Zamora Presidente Ejecutivo de Auna
FIRMA:	**FIRMA**:	**FIRMA**:	**FIRMA**:	**FIRMA**:
DocuSigned by: Juan Pablo Ramirez 00F93817A9794B3...	DocuSigned by: Denisse del Rosario 0A9812E2826C4A9...	DocuSigned by: Yesenia Yance 8595529A8343451...	DocuSigned by: Gaston Fourcade 2287C646E685481...	DocuSigned by: Suso Zamora 52A942B89243497...

- **OBJETIVO**

Establecer el marco general para la Gestión de la seguridad de la información y ciberseguridad en AUNA, proporcionando las medidas y lineamientos de seguridad de la información y ciberseguridad a cumplir por parte de los colaboradores, socios, proveedores, y terceros, con el objetivo de asegurar la integridad, confidencialidad y disponibilidad de la información.

- **ALCANCE**

Esta política aplica a todas las empresas del Grupo AUNA, sus colaboradores, socios, proveedores, y terceros abarcando los activos de información.

- **RESPONSABILIDADES**

La Política de Seguridad de la información y Ciberseguridad es de aplicación obligatoria para todo el personal de AUNA, cualquiera sea su situación contractual y el nivel de las tareas que desempeñe. Para las nuevas sociedades, es fundamental que las políticas establecidas sean cumplidas por las áreas responsables de llevar a cabo dichas funciones.

- **Alta Gerencia**
  - Asignar los recursos necesarios que garanticen la adecuada gestión de la seguridad de la información y ciberseguridad

- **Gerentes / Directores / Jefes**
  - Garantizar que el personal que labora bajo su dirección, proteja la información de acuerdo con las normas establecidas por la organización.
  - Aprobar / revisar periódicamente los accesos de los colaboradores a su cargo.
  - Determinar para sus colaboradores los niveles de acceso a la información.

- **Jefe de Seguridad de la Información y Cumplimiento TI**
  - Definir las políticas y procedimientos relacionados a la seguridad de la información, de acuerdo a las regulaciones y normativas, y velar por el cumplimiento de las mismas.
  - Documentar y evaluar los riesgos identificados de seguridad de la información y ciberseguridad, y apoyar en las medidas correctivas.
  - Informar a la alta gerencia todos los temas relacionados a la seguridad de la información.
  - Ejecutar el programa de concientización en temas de seguridad de la información y ciberseguridad dirigido a los colaboradores de AUNA.

- Velar por que la seguridad de la información se gestione adecuadamente en todo AUNA.

➢ **Jefe de Seguridad Informática y Ciberseguridad**

- Definir las políticas y procedimientos relacionados a la seguridad informática, de acuerdo con las regulaciones y normativas, y velar por el cumplimiento de las mismas.
- Garantizar la seguridad de los sistemas de información e infraestructura tecnológica, a través de la implementación de herramientas tecnológicas.
- Monitorear las plataformas de seguridad, y gestionar los incidentes de ciberseguridad.
- Velar por que la seguridad informática y ciberseguridad se gestione adecuadamente en todo AUNA.

➢ **Gerencia de Tecnología de la Información.**

- Aplicar los controles de seguridad en los sistemas de información, infraestructura tecnológica y en los proyectos de tecnología de información.
- Convocar al Jefe de Seguridad informática y ciberseguridad en los proyectos relacionados al desarrollo de infraestructura tecnológica y nuevas aplicaciones.

➢ **Gerencia de Gestión Humana**

- Notificar a todo el personal que se vincule contractualmente con AUNA, de las obligaciones respecto al cumplimiento de la Política de seguridad de la Información y Ciberseguridad, estándares, procesos y procedimientos diseñados para la seguridad de la información y ciberseguridad.
- Incluir en la inducción de nuevos colaboradores la capacitación de seguridad de la información y ciberseguridad.
- Definir las acciones disciplinarias en caso de incumplimiento de las políticas de seguridad de la información y ciberseguridad.
- Definir, notificar y hacer cumplir los compromisos de confidencialidad de la información.

➢ **Colaboradores**

- Conocer, comprender y cumplir las Políticas de Seguridad de la Información y Ciberseguridad.
- Mantener la confidencialidad de sus usuarios y contraseñas de la información a la cual tienen acceso.

- Notificar incidentes y riesgos de seguridad de la información y ciberseguridad a las Áreas encargadas.

➢ **Terceros y Proveedores de Servicios**
- Conocer y cumplir las Políticas de Seguridad de la Información y Ciberseguridad.
- Cumplir con las cláusulas de seguridad de la información y ciberseguridad incluidas en los contratos para asegurar la confidencialidad, integridad y disponibilidad de la información.

➢ **Gerencia Legal**
- Establecer un modelo de contrato para los servicios tercerizados y/o la contratación de personal, que incluyan cláusulas que obliguen a los proveedores y colaboradores a que sus servicios no afecten la confidencialidad, integridad y disponibilidad de la información.

- **POLITICA**

- **Compromisos Institucionales de la Política General de la Seguridad de la Información.**

Los compromisos generales que permiten una adecuada gestión de la Seguridad de la Información y Ciberseguridad en AUNA son:

➢ Proteger los activos de información de las amenazas originadas por parte del personal y terceros.
➢ Fortalecer la cultura de seguridad de la información y ciberseguridad en los colaboradores y terceros de AUNA.
➢ Implementar un control de acceso a la información, aplicaciones e infraestructura considerando el principio de mínimo privilegio.
➢ Establecer una adecuada seguridad en la gestión de las operaciones y comunicaciones.
➢ Proteger las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
➢ Garantizar que la seguridad sea parte integral del ciclo de vida de desarrollo de los sistemas de información.
➢ Garantizar un procedimiento de gestión de incidentes de seguridad de la información y ciberseguridad.
➢ Velar por el cumplimiento de las regulaciones legales vigentes en materia de seguridad de la información y ciberseguridad que le apliquen.
➢ El documento de Política General de Seguridad de la Información debe ser revisado por el Jefe de Seguridad de la Información y Cumplimiento TI cada que ocurra un cambio significativo.

MODELO DE APLICACIÓN DE LA POLÍTICA

El marco estratégico en Ciberseguridad se basa en 4 dominios.

- **Gobierno:** Capacidad de garantizar que la estructura organizacional y la normatividad interna, operan de forma efectiva para mantener y mejorar las capacidades preventivas y de detección.
- **Vigilante:** Capacidad para detectar aquello que se desconoce y reducir el tiempo de detección de un ataque.
- **Resiliente:** Capacidad de respuesta ante incidentes cibernéticos y recuperación de las actividades del negocio.
- **Seguro:** Capacidad de proteger a los activos que soportan la operación del negocio y la información critica ante amenazas conocidas y emergentes.

- **REFERENCIAS**

CÓDIGO	NOMBRE
ISO/IEC 27001:2022	Seguridad de la Información, Ciberseguridad y Protección de la Privacidad - Sistema de Gestión de Seguridad de la Información
Ley No 29733	Ley de Protección de Datos Personales en Perú
Ley No 1581	Ley de Protección de Datos Personales en Colombia
-	Ley Federal de Protección de Datos Personales en Posesión de los particulares
Ley SOX	Ley Sarbanes-Oxley
GA.TI.T.02	Políticas Específicas de Seguridad de la Información (Perú)
P-TI-2	Políticas Específicas de Seguridad de la Información (Colombia)

- **INDICADORES**
  No aplica