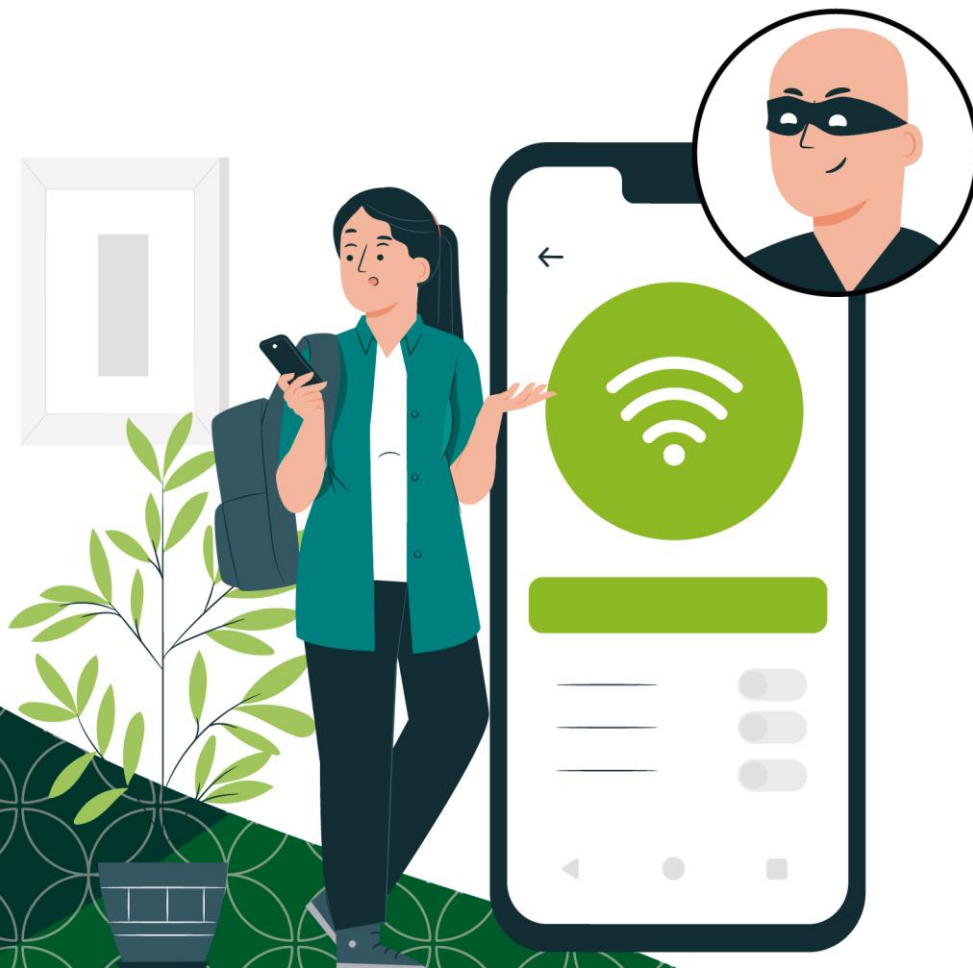




# PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2024



	<b>PLAN DE TRATAMIENTOS DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN AÑO 2024</b>		CÓDIGO:	Y-GI-03
			VERSIÓN:	5.0
			FECHA:	Ene. 22 de 2024
			PÁGINA:	1 DE 9

## TABLA DE CONTENIDO

INTRODUCCIÓN .....	2
1. OBJETIVO .....	3
2. ALCANCE .....	3
3. DEFINICIONES .....	3
4. DESCRIPCIÓN DEL PLAN .....	4
5. DOCUMENTOS DE REFERENCIA .....	8
6. NOTAS DE CAMBIO.....	9
7. APROBACIÓN.....	9

	<b>PLAN DE TRATAMIENTOS DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN AÑO 2024</b>		CÓDIGO:	Y-GI-03
			VERSIÓN:	5.0
			FECHA:	Ene. 22 de 2024
			PÁGINA:	2 DE 9


## INTRODUCCIÓN

La información es crucial para el desarrollo de las actividades misionales y administrativas en la UESVALLE, por tal razón debe ser protegida de cualquier posibilidad de ocurrencia de eventos de riesgo de seguridad y que pudiese significar un impacto indeseado generando una consecuencia negativa para el normal progreso de las actividades de la UESVALLE.

El plan de tratamiento de riesgos de Seguridad y Privacidad de la información establece y requiere el desarrollo de una cultura de carácter preventivo, de manera que, al comprender el concepto de riesgo, así como el contexto, se planean acciones que reduzcan la afectación a la entidad en caso de materialización.

Este plan busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos, dando a conocer aquellas situaciones que pueden afectar el cumplimiento de los objetivos estratégicos, a partir de la alineación al modelo de seguridad y privacidad de la información de la UESVALLE.

En cumplimiento con la política de Participación Ciudadana en la Gestión Pública contenida en la segunda dimensión de Direccionamiento Estratégico y Planeación y en la tercera dimensión Gestión con Valores para Resultados, la entidad publicó en su portal web [www.uesvalle.gov.co](http://www.uesvalle.gov.co), el borrador de este documento con el fin de brindar de que la ciudadanía en general se incluyera en su construcción dentro del ejercicio de la democracia participativa.

	<b>PLAN DE TRATAMIENTOS DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN AÑO 2024</b>	CÓDIGO:	Y-GI-03
		VERSIÓN:	5.0
		FECHA:	Ene. 22 de 2024
		PÁGINA:	3 DE 9

## 1. OBJETIVO

Establecer una metodología que permita la gestión del riesgo de seguridad de la información basado en los criterios de Confidencialidad, Integridad y Disponibilidad, que permitan la protección de los activos de información de la UESVALLE.

### 1.1 Objetivos Específicos

- Asegurar la confidencialidad, integridad y disponibilidad de los activos de información de la UESVALLE.
- Realizar la identificación y tratamiento de los riesgos para reducir el impacto ante la ocurrencia de eventos de seguridad de la información.
- Fortalecer y apropiar el conocimiento referente a la gestión de riesgos de Seguridad y Privacidad de la información.

## 2. ALCANCE

Comprende las acciones que deben tomar las diferentes áreas de la entidad en el tratamiento de riesgos de seguridad y privacidad de la información con base en los lineamientos definidos en las políticas y tiempos definidos en el Plan de Seguridad y Privacidad de la Información.

## 3. DEFINICIONES

**Amenaza.** Es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).

**Control o Medida.** Acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una entidad.

**Impacto.** Son las consecuencias que genera un riesgo una vez se materialice.

**Probabilidad.** Es la posibilidad de la amenaza aproveche la vulnerabilidad para materializar el riesgo.

**Riesgo.** Es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitando cumplir con sus objetivos.

**Vulnerabilidad.** Es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

	<b>PLAN DE TRATAMIENTOS DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN AÑO 2024</b>	CÓDIGO:	Y-GI-03
		VERSIÓN:	5.0
		FECHA:	Ene. 22 de 2024
		PÁGINA:	4 DE 9


#### 4. DESCRIPCIÓN DEL PLAN

##### 4.1 POLÍTICA DE ADMINISTRACIÓN DE RIESGOS.

La Política de Administración de Riesgos de la Unidad Ejecutora de Saneamiento del Valle del Cauca UESVALLE, establece a los servidores públicos, colaboradores, contratistas y público en general, nuestro compromiso e interés de identificar y controlar los riesgos institucionales, se debe establecer los parámetros necesarios para una adecuada gestión de los riesgos de gestión, corrupción, seguridad y privacidad de la información, seguridad digital y continuidad de los servicios de la UESVALLE, procurando que no se materialicen, atendiendo los lineamientos establecidos en la Guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP, orientando a la toma de decisiones oportunas y minimizando efectos adversos al interior de la Entidad, con el fin de dar continuidad a la gestión institucional y asegurar el cumplimiento de los compromisos con los Grupos de interés.

Las líneas de Defensa y responsabilidades de la Administración del Riesgo de la Entidad, tendrá como referencia a lo establecido en la séptima dimensión Control Interno del Modelo Integrado de Planeación y Gestión MIPG, así:

LÍNEAS DE DEFENSA	RESPONSABLE	RESPONSABILIDAD
Estratégica	Representante Legal y Comité Institucional de Coordinación de Control Interno	<ol style="list-style-type: none"> <li>1. Actualizar la Política de Administración de Riesgos y hacerlo aprobar por el Representante Legal, y supervisar su cumplimiento.</li> <li>2. Analizar los riesgos y eventos críticos y emitir directrices y mejora de los controles.</li> </ol>
Primera Línea	Responsables de Procesos	<ol style="list-style-type: none"> <li>1. Atender la Política de Administración de Riesgos.</li> <li>2. Identificar, valorar los riesgos y diseñar las acciones (controles) para evitarlos o reducir su impacto, que puedan afectar el logro de los planes y actividades a su cargo y participar en la construcción de los mapas de riesgos.</li> <li>3. Supervisar la ejecución de los controles por el equipo de trabajo en la gestión del día a día y evaluar su efectividad.</li> <li>4. Informar sobre la materialización de los riesgos y realizar el ajuste del Mapa de Riesgos.</li> <li>5. Divulgar y sensibilizar sobre los riesgos y controles en su proceso a cargo.</li> <li>6. Generar reportes periódicamente al Comité Institucional de Coordinación de Control Interno.</li> </ol>
	Profesionales Responsables de ARO.	<ol style="list-style-type: none"> <li>1. Cumplir y hacer cumplir al equipo de trabajo a su cargo en la gestión del día a día, con los controles establecidos frente a los riesgos para evitar su materialización o para la minimización del impacto.</li> <li>2. Generar reportes cuando se requiera al Comité Institucional de Coordinación de Control Interno.</li> <li>3. Ayudar con la divulgación y sensibilización sobre los riesgos y controles en el Área Operativa.</li> </ol>

	<b>PLAN DE TRATAMIENTOS DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN AÑO 2024</b>	CÓDIGO:	Y-GI-03
		VERSIÓN:	5.0
		FECHA:	Ene. 22 de 2024
		PÁGINA:	5 DE 9

LÍNEAS DE DEFENSA	RESPONSABLE	RESPONSABILIDAD
Segunda Línea	Oficina de Planeación o quien haga sus veces (Gerencia Riesgos)  Supervisores e interventores de contratos  Comités Institucionales	<ol style="list-style-type: none"> <li>1. Monitorear y asegurar que los controles y la gestión de riesgos implementados en la Primera Línea de Defensa, estén diseñados apropiadamente y funcionen como se pretende.</li> <li>2. La Oficina de Planeación en coordinación con los responsables de procesos debe consolidar el Mapa de Riesgos, generar reportes periódicamente al Comité Institucional de Coordinación de Control Interno y ayudar con la divulgación y sensibilización sobre los riesgos y controles a todos los servidores de la entidad.</li> <li>3. Los supervisores e interventores deben realizar seguimiento a los riesgos de sus respectivos contratos e informar las alertas respectivas que atenten con el cumplimiento de los objetivos.</li> <li>4. Los Comités institucionales deben realizar sus actuaciones con enfoque basado en riesgos.</li> </ol>
Tercera Línea	Oficina de Control Interno.	<ol style="list-style-type: none"> <li>1. Proporcionar información sobre la efectividad de la gestión del riesgo y controles establecidos en la Línea Estratégica y la operación de la Primera y Segunda línea de Defensa con un enfoque basado en riesgos.</li> <li>2. Comunicar al Comité Institucional de Coordinación de Control Interno sobre la evaluación del riesgo detectada en las auditorías internas.</li> <li>3. Alertar sobre la probabilidad de riesgo no identificados.</li> <li>4. Actuar como secretario del Comité Institucional de Coordinación de Control Interno</li> </ol>

## 4.2 TRATAMIENTO DE RIESGOS

El tratamiento de riesgos es la respuesta establecida por la primera línea de defensa, es decir, el líder o responsable del proceso junto con su equipo de trabajo para la mitigación de los diferentes riesgos.

El propósito del tratamiento del riesgo es seleccionar e implementar opciones para abordar el riesgo, y debe implicar un proceso iterativo de:

- Formular y seleccionar opciones para el tratamiento del riesgo.
- Planificar e implementar el tratamiento del riesgo.
- Evaluar la eficacia de ese tratamiento.
- Decidir si el riesgo residual es aceptable.
- Si no es aceptable, efectuar el tratamiento adicional.

La política de Administración de Riesgo establece las opciones para tratar los riesgos residuales ya sea fortaleciendo los actuales controles o implementado nuevos controles, para lo cual deberá tener en cuenta las siguientes opciones de manejo:

**Evitar el riesgo.** Corresponde tomar medidas encaminadas a prevenir o eliminar las causas para su materialización u ocurrencia. Es siempre la primera alternativa a considerar y se logra cuando al interior de los procesos se generan cambios sustanciales por mejoramiento, rediseño, eliminación de la actividad que causa el riesgo, y como resultado de unos adecuados controles y



	<b>PLAN DE TRATAMIENTOS DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN AÑO 2024</b>	CÓDIGO:	Y-GI-03
		VERSIÓN:	5.0
		FECHA:	Ene. 22 de 2024
		PÁGINA:	6 DE 9

acciones emprendidas. Un ejemplo de esto puede ser el control de calidad, manejo de los insumos, mantenimiento preventivo de los equipos, desarrollo tecnológico, entre otros.

**Aceptar el riesgo.** Corresponde a asumir las consecuencias del riesgo por considerar de muy baja probabilidad su ocurrencia y de leves consecuencias, o en su defecto, luego de que el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se aceptala pérdida en caso de materialización. Se elaboran planes de contingencia para su manejo.

**Reducir el riesgo.** Corresponde tomar medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención), sus impactos (medidas de protección), o ambas. La reducción del riesgo es probablemente el método más sencillo y económico para superar lasdebilidades antes de aplicar medidas más costosas y difíciles. Se consigue mediante la optimización de los procedimientos y la implementación de controles.


**Compartir el riesgo.** Se reduce su efecto a través del traspaso de las pérdidas a otras organizaciones, mediante un contrato determinado, como en el caso de los contratos de seguros, tercerización o a través de otros medios que permiten distribuir una porción del riesgo con otra entidad, como en los contratos a riesgo compartido. Es así como, por ejemplo, la información de gran importancia se puede duplicar y almacenar en un lugar distante y de ubicación segura, en vez de dejarla concentrada en un solo lugar.

#### 4.3 RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA ENTIDAD

La UESVALLE definió el documento **F-DE-13 MAPA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN**, donde se consagra todo lo relacionado a la implementación del plan de tratamiento de riesgos y privacidad de la información de la ENTIDAD.

Para la vigencia 2024, se establecen e identifican los siguientes riesgos:


Referencia	Activo de Información	Tipo de activo	Amenazas (Causa Inmediata)	Vulnerabilidades (Causa raíz)	Tipo de riesgo	Descripción del Riesgo	Clasificación riesgo
1	Equipos Informáticos	Hardware	Polvo, corrosión, congelamiento	Mantenimiento insuficiente	Daño Físico	Posibilidad de pérdida de la disponibilidad de la información debido a fallas técnicas en los dispositivos tecnológicos(hardware)	Fallas tecnológicas
2	Servidor Web Aplicativo Trámites Construcción	Entorno Web	Ataque Scripting Entre Sitios (XSS)	Configuración Incorrecta de la Seguridad	Pérdida de Confidencialidad	Posibilidad de pérdida de la integridad de la información alojada en el servidor web, debido a la configuración incorrecta de parámetros de seguridad en la aplicación lo que puede permitir ataques de XSS (Cross Site Scripting).	Fraude Externo
3	Software de gestión Administrativa y financiera	Software	Falsificación de derechos	Autenticación débil	Pérdida de integridad	Posibilidad de pérdida de integridad por la autenticación de un usuario no autorizado debido a una autenticación débil en el software, que utiliza un único factor de autenticación como es: usuario y contraseña.	Fraude interno
4	Red de Datos Locales	Red	Mal funcionamiento del software	Conexión deficiente del cableado	Pérdida de Disponibilidad de la información	Posibilidad de fallas en la comunicación entre los servidores de aplicaciones y losequipos de usuarios finales, y dificultades en el mantenimiento y accesibilidad a la estructura del cableado de datos.	Fallas tecnológicas

	<b>PLAN DE TRATAMIENTOS DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN AÑO 2024</b>	CÓDIGO:	Y-GI-03
		VERSIÓN:	5.0
		FECHA:	Ene. 22 de 2024
		PÁGINA:	7 DE 9

Se realiza la descripción de controles:

Proceso	No Control	Control Anexo A	Descripción del control
Gestión Informática	1	A.11.2.4 Mantenimiento de equipos	El responsable del proceso de gestión informática, debe garantizar el correcto funcionamiento de los equipos de cómputo
	2	A.7.1.2 Términos y condiciones del empleo	Al finalizar los contratos de prestación de servicios se debe hacer entrega de todos los bienes activos a la UESVALLE a través del formato de paz y salvo de almacén y de gestión documental. Así mismo al personal de planta se le exige dichos formatos en casos de licencias, vacaciones o renunciaciones, como requisito obligatorio por parte del proceso de gestión de contratación para continuar con el trámite de la radicación de la liquidación.
	3	A.15.2 Gestión de la prestación de servicios con los proveedores	El proceso de gestión informática cuenta con una Plataforma tecnológica: <a href="https://www.uesvalle.gov.co/feedback/192/solicitud-de-soporte-yo-servicios-informaticos">https://www.uesvalle.gov.co/feedback/192/solicitud-de-soporte-yo-servicios-informaticos</a> , para el reporte de incidencias de fallas tecnológicas, la cual permite la asignación al técnico respectivo su oportuna intervención, registrando los tiempos de gestión del incidente desde la apertura hasta su aprobación.
Gestión Informática	1	A.13.1.2 Seguridad de los servicios de red	El proveedor de la página web cuenta con el protocolo de seguridad GOOGLE CLOUD PLATFORM - Firewall. Las reglas de firewall permiten o rechaza el tráfico desde y hacia las instancias de máquina virtual (VM) según la configuración que se especifique. Las reglas de firewall de GCP se aplican al nivel de la red virtual, por lo que ofrecen protección y control de tráfico eficaces sin importar el sistema operativo que usen las instancias. Cada regla permite o rechaza el tráfico cuando se cumplen sus condiciones. Estas condiciones permiten especificar el tipo de tráfico, como puertos y protocolos, además del origen o el destino del tráfico, incluidas las direcciones IP, las subredes y las instancias.
	2	A.12.6.1 Gestión	El proveedor de la página web, realiza revisión de código de la aplicación, validación de campos de entrada, caracteres recibidos y tipos de formatos de archivos admitidos, entrega informe de seguridad como soporte de las cuentas
	3	A.12.3.1 Respaldo de información	El proveedor de la página web, dentro de sus obligaciones contractuales "Se debe realizar un Backup automático cada 48 horas como mínimo del portal web e instrucciones para reestablecer el sitio sin ningún percance". Si se materializara el riesgo, se cuenta con copia de seguridad que permite de manera oportuna ejercer la contingencia y restablecimiento total de la plataforma.



	<b>PLAN DE TRATAMIENTOS DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN AÑO 2024</b>	CÓDIGO:	Y-GI-03
		VERSIÓN:	5.0
		FECHA:	Ene. 22 de 2024
		PÁGINA:	8 DE 9

Proceso	No Control	Control Anexo A	Descripción del control
Gestión Informática	1	A.9.4.3 Sistema de gestión de contraseñas	El proceso de Gestión Informática administra la configuración de contraseñas que aplicarán sobre la plataforma tecnológica, los servicios de red y los sistemas de información de la UESVALLE; los cuales deben considerar aspectos como longitud, complejidad, cambio periódico y cambio de contraseña, especificados en documento de políticas de seguridad y privacidad de información. El sistema de información cuenta con la funcionalidad de validar los criterios de contraseñas.
	2	A.9.4.1 Restricción de acceso Información	El sistema de información cuenta con el módulo de seguridad en el cual se crean los roles o permisos requeridos de acuerdo con las actividades a realizar por el personal, donde el administrador de la aplicación asigna el roll o perfil al usuario final, para esta asignación el usuario debe diligenciar el formato de administración de usuarios con el visto bueno del responsable del proceso respectivo.
	3	A.15.1.3 Cadena de suministro de tecnología de información y comunicación	En cada uno de una de las vigencias se realiza contrato de soporte, mantenimiento y bolsa de horas de desarrollo del sistema de información, lo que permite realizar el reporte de incidencias tanto de fallas de la aplicación como ajustes requeridos para el mejoramiento de la seguridad, lo cual se realiza a la necesidad

## 5. DOCUMENTOS DE REFERENCIA


**Directiva Presidencial No. 02 de 2022** Reiteración de la Política Pública en Materia de Seguridad Digital

**Decreto 1008 de 2018.** Establece los lineamientos generales de la política de Gobierno Digital. Deroga el Decreto 2573 de 2014.

**Decreto 1078 de 2015.** Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

**NTC / ISO 27001:2013.** Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI).

**Guía No. 7.** Guía de gestión del riesgo, versión 3.0 – del Ministerio de Tecnologías de la Información y las Comunicaciones.

	<b>PLAN DE TRATAMIENTOS DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN AÑO 2024</b>	CÓDIGO:	Y-GI-03
		VERSIÓN:	5.0
		FECHA:	Ene. 22 de 2024
		PÁGINA:	9 DE 9

## 6. NOTAS DE CAMBIO

Fecha	Versión inicial	Motivo del cambio	Versión final
Ene. 01 de 2019	0.0	Versión inicial del documento	1.0
Ene. 30 de 2020	1.0	Se adiciona, términos de conceptualización, objetivos específicos, marco normativo, se adiciona nuevos puntos que ayudan a comprender la forma de darle los tratamientos a los riesgos de seguridad y privacidad de la información.	2.0
Ene. 27 de 2021	2.0	Se adiciona tabla de vulnerabilidades incluyendo el tratamiento a los riesgos que estas podrían materializar, se adiciona un nuevo objetivo específico con respecto a la optimización e implementación de controles.	3.0
Ene. 26 de 2022	3.0	Se adiciona la matriz de riesgos con la identificación de riesgos, controles y plan de acción respectivo año 2022-2023. Se adiciona la proyección del presupuesto 2022 y 2023.	4.0
Ago. 02 de 2023	4.0	Se realiza la actualización de la matriz de Riesgos	5.0
Ene. 22 de 2024	5.0	Se realiza la actualización del plan para la vigencia 2024.	6.0

## 7. APROBACIÓN

	Elaboró	Revisó	Aprobó
<b>Nombre:</b>	María Rosario Tasamá Jiménez	Julián Eduardo Montoya	Constanza Ivette Hernández Rojas
<b>Cargo:</b>	Profesional Universitario	Subdirector Administrativo	Directora General
<b>Fecha:</b>	Ene. 19 de 2024	Ene. 22 de 2024	Ene. 22 de 2024
<b>Firma:</b>	Documento original firmado	Documento original firmado	Documento original firmado