

PLAN INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO	
<b>POLÍTICA DE GESTIÓN</b>	<b>SEGURIDAD DIGITAL</b>
<b>OBJETIVO DEL PLAN</b>	Definir y adoptar buenas prácticas, tomando como referencia el Modelo de Seguridad y Privacidad de la Información, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.
<b>JUSTIFICACIÓN</b>	Su importancia radica en la necesidad de las entidades públicas de incorporar la seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y, en general, en todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos. Se encuentra alineado con el Marco de Referencia de Arquitectura TI, el Modelo Integrado de Planeación y Gestión (MIPG) y La Guía para la Administración del Riesgo y el Diseño de Controles en entidades Públicas, este modelo pertenece al habilitador transversal de Seguridad y Privacidad, de la Política de Gobierno Digital. Y Se desarrolla mediante el Documento Maestro del Modelo de Seguridad y Privacidad de la Información y sus guías de orientación. Lo debe desarrollar el líder o encargado de Seguridad de la Información con el apoyo de toda la estructura organizacional.
<b>LÍDER DE LA POLÍTICA</b>	<b>JEFE OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN</b>
<b>VERSIÓN</b>	V1 Comité de Gestión y Desempeño Institucional del 15/12/2023

Dimensión 3: Gestión con Valores para Resultados							SEGUIMIENTO A CORTE DE 30 DE SEPTIEMBRE DEL 2024				30/09/2024				EVALUACIÓN CONTROL INTERNO A 30/09/2024			
ITEM	ACTIVIDADES	PESO DE ACTIVIDAD	ACCIONES	PESO POR ACCIÓN	RESPONSABLE	DEPENDENCIAS INVOLUCRADAS EN LA IMPLEMENTACIÓN	PRODUCTO ESPERADO	FECHA DE INICIO	FECHA DE TERMINACIÓN	Evidencia	Autoevaluación	Validación OAP	% Avance real acumulado de la acción	% Avance real acumulado de la actividad	% Avance esperado acción	% Avance esperado actividad	Nivel de Cumplimiento sobre Avance Esperado	Evaluación Cualitativa -Validación Soportes
1	Fortalecer la gestión de riesgos y controles de seguridad digital asociados a servicios de nube	15%	1.1. Identificar y gestionar riesgos de seguridad digital en los servicios de nube	100%	Grupo de Seguridad de la Información	Oficina de Planeación	Matriz de riesgos actualizada	1/02/2024	30/11/2024	NA	Actividad finalizada en el segundo trimestre de la vigencia, por tanto no requiere reporte.	Ok, el cumplimiento de la acción se encuentran de acuerdo con la autoevaluación de la actividad.	100,00%	15,00%	79,87%	11,98%	<b>Nivel de Cumplimiento Alto</b> El 30 de abril de 2024, se estableció la política de administración de riesgos, junto con una matriz de riesgos de seguridad de la información y ciberseguridad, la cual fue actualizada el 24 de junio de 2024. Esta actividad se cumplió al 100% en el trimestre anterior.	
2	Vincular al CSIRT y COLCERT Gobierno, en el acompañamiento y apoyo hacia la entidad, con el fin de mejorar los procesos de seguridad de la infraestructura tecnológica y la gestión de los incidentes cibernéticos.	40%	2.1. Socializar los boletines informativos de seguridad, integrar con CSIRT de Gobierno	30%	Grupo de Seguridad de la Información		Boletines Informativos	1/03/2024	30/11/2024	NA	Durante el tercer trimestre de la vigencia, no se socializaron los boletines informativos de seguridad, integrando al CSIRT de Gobierno, puesto que se solicitó el análisis de vulnerabilidades. Por lo anterior se mantiene el % del trimestre anterior.	Ok, el cumplimiento de la acción se encuentran de acuerdo con la autoevaluación de la actividad.	70,00%		77,74%		<b>Nivel de Cumplimiento Bajo</b> De conformidad con el tiempo transcurrido y la participación establecida para esta acción (30%), el avance reportado del 70% corresponde al 21% del avance esperado del 23,33% y con respecto al peso de la actividad (40%) el avance reportado corresponde al 8,40%, es decir se logra el 90% del esperado de 9,33% de la actividad. <b>Revisión de evidencias:</b> Durante el segundo trimestre, la Oficina de Tecnologías de la Información socializó el boletín sobre phishing, smishing y recomendaciones para enfrentar amenazas digitales. Sin embargo, en el tercer trimestre no se llevó a cabo ninguna actividad adicional, por lo que el porcentaje de avance se mantiene en el 70% reportado anteriormente, reflejando un nivel de cumplimiento bajo.	
			2.2. Incluir en el procedimiento vigente de "GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN" la notificación a las autoridades pertinentes (CSIRT Gobierno, COLCERT, Centro Cibermético Policial) cuando aplique.	40%	Grupo de Seguridad de la Información	Oficina de Planeación	Procedimiento de incidentes de seguridad actualizado y publicado en Gespro	1/03/2024	30/05/2024	NA	Actividad finalizada en el segundo trimestre de la vigencia, por tanto no requiere reporte.	Ok, el cumplimiento de la acción se encuentran de acuerdo con la autoevaluación de la actividad.	100,00%		100,00%		33,31%	<b>Nivel de Cumplimiento Alto</b> Se actualiza el procedimiento DT-PR-04 Gestión de incidentes de seguridad de la información el día 17/09/2024.
			2.3. Solicitar análisis de vulnerabilidades y monitoreo de los servicios digitales de la página web	30%	Grupo de Seguridad de la Información	Oficina de Planeación	Informe de Vulnerabilidades	1/06/2024	30/11/2024	Reporte vulnerabilidades web - CSIRT	Durante el tercer trimestre de la vigencia, se reciben el 05 de agosto de 2024 los informes técnicos de los resultados del análisis de vulnerabilidades web, realizado por parte del CSIRT-Gobierno.	Las evidencias aportadas se encuentran de acuerdo con la autoevaluación de la actividad. (Adjunto)	100,00%		66,48%			<b>Nivel de Cumplimiento Alto</b> De conformidad con el tiempo transcurrido y la participación establecida para esta acción (30%), el avance reportado del 100% corresponde al 30% del avance esperado del 20% y con respecto al peso de la actividad (40%) el avance reportado corresponde al 12%, es decir se logra el 150% del esperado de 8% de la actividad. <b>Revisión de evidencias:</b> El 2 de agosto de 2024, la Oficina de Tecnologías de la Información solicitó al CSIRT Gobierno un análisis de vulnerabilidades en 15 sitios web. Como resultado, se identificaron 172 vulnerabilidades críticas, 0 de alto riesgo, 420 de riesgo medio y 559 de riesgo bajo.
3	Realizar seguimiento a posibles eventos de riesgos y vulnerabilidades	15%	3.1. Realizar seguimiento semestral a los informes de eventos y vulnerabilidades asociados a SGSI	100%	Grupo de Seguridad de la Información	Oficina de Planeación	Informe Semestral de seguimiento	1/02/2024	30/11/2024	Informe Incidentes Seguridad de la Información trim III 01 jul 30 sept Estado Remediación Vulnerabilidades ANLA 2024	Durante el tercer trimestre de la vigencia, se realiza seguimiento a los planes de remediación de las vulnerabilidades identificadas y se realiza informe de incidentes de seguridad de la información. En total durante la vigencia se realizaron 3 informes. Por lo anterior se finaliza la actividad	Las evidencias aportadas se encuentran de acuerdo con la autoevaluación de la actividad	100,00%	15,00%	79,87%	11,98%	<b>Nivel de Cumplimiento Alto</b> De conformidad con el tiempo transcurrido y la participación establecida para esta acción (100%), el avance reportado del 100% corresponde al 100% del avance esperado del 80% y con respecto al peso de la actividad (15%) el avance reportado corresponde al 15%, es decir se logra el 125% del esperado de 12% de la actividad. <b>Revisión de evidencias:</b> La Oficina de Tecnologías de la Información, presenta el informe de monitoreo y seguimiento de eventos de incidentes de seguridad de la información entre el 01 de julio al 30 de septiembre de 2024.	
4	Mantener la disponibilidad continua de servicios esenciales de Tecnologías de la información	15%	Realizar cuatro (4) pruebas de los planes de recuperación ante desastres al año a partir de los sistemas críticos identificados bajo la estructura metodológica.	100%	Grupo de Seguridad de la Información	Oficina de Tecnología de Información	Cuatro (4) informes de pruebas	1/02/2024	30/11/2024	Informe Pruebas Switch_2024 Prueba DRP Active Directory Prueba DRP Virtualización Nutanix	Durante el tercer trimestre de la vigencia se realiza prueba de recuperación ante desastres para Virtualización Nutanix; adicionalmente se realiza prueba de recuperación ante desastres para Active Directory y se realiza prueba de alta disponibilidad en switch. Se encuentra pendiente la elaboración de 2 informes de las pruebas realizadas.	Las evidencias aportadas se encuentran de acuerdo con la autoevaluación de la actividad	90,00%	13,50%	79,87%	11,98%	<b>Nivel de Cumplimiento Bajo</b> De conformidad con el tiempo transcurrido y la participación establecida para esta acción (100%), el avance reportado del 90% corresponde al 90% del avance esperado del 80% y con respecto al peso de la actividad (15%) el avance reportado corresponde al 13,50%, es decir se logra el 112% del esperado de 12% de la actividad. <b>Revisión de evidencias:</b> La OTI, reporta un avance del 90%, sin embargo, solo se ha reportado 2 informes de los 4 programados. Teniendo en cuenta lo anterior, el cumplimiento sería del 50% reflejando un nivel de cumplimiento bajo.	
5	Habilitar un entorno lógico separado de los back up de información	15%	Habilitar un entorno lógico separado e independiente a la red de servidores y computadores de los back up	100%	Infraestructura tecnológica	Grupo de Seguridad de la Información	Entornos de entorno lógico separado	1/02/2024	30/04/2024	Separacion_Ambientes	Se realiza una actualización del Avance Servidores		100,00%	15,00%	100,00%	15,00%	<b>Nivel de Cumplimiento Alto</b> Según las evidencias presentadas por la OTI en el trimestre anterior, se confirma que los ambientes de producción, integración, QA y capacitación están completamente separados. Por lo tanto, se considera que la acción se ha cumplido al 100%.	
													94,90%	94,90%	84,25%	84,25%		

Seguimiento OCI  
Fecha: 25/09/2024  
Elaboró: Diana Elizabeth Peñaflo Saboal  
Revisó: Luz Dary Amaya Peña  
Aprobó: Richard Eduardo Lopes Torres



0 a 74,9  
75 a 89,9  
90 a 100

